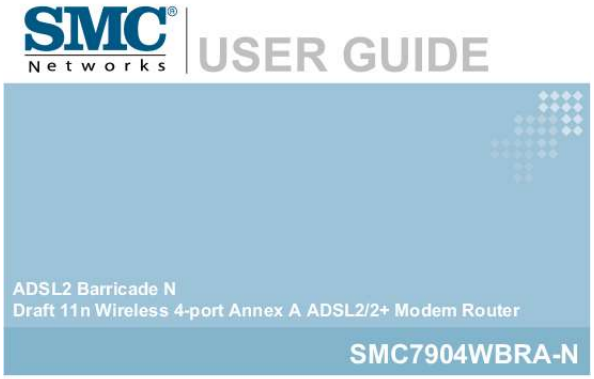
Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for SMC 7904WBRA-N. You'll find the answers to all your questions on the SMC 7904WBRA-N in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual SMC 7904WBRA-N
User guide SMC 7904WBRA-N
Operating instructions SMC 7904WBRA-N
Instructions for use SMC 7904WBRA-N
Instruction manual SMC 7904WBRA-N



You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

Manual abstract:

20 Mason 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. 20 Mason 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 This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

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

This equipment should be installed and operated with minimum distance 20cm between the radiator & 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. SMC contact for these products in US is: SMC Networks North America 20 Mason Irvine, CA 92618. USA Tel 800-762-4968 Tony Stramandinoli · · · iii COMPLIANCES FCC - Part 68 This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA.

On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: ACYDL01B7904WBRAN. If requested, this number must be provided to the telephone company. The REN is useful to determine the quantity of devices you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to you line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area. If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC.

Your telephone company may make changes in it is facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service. If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning. This equipment may not be used on coin service provided by the telephone company.

Connection to party lines is subject to state tariffs. iv COMPLIANCES CE Mark Declaration of Conformance for EMI and Safety (EEC) This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following references have been applied in order to prove presumption of compliance with the R&TTE Directive 1999/5/EC: · · · EN 300 328 EN 301 489 EN 60950-1 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. 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 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. v COMPLIANCES 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 Härmed intygar SMC Networks att 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. viii TABLE OF CONTENTS 1 Introduction . . . . . .

. . . . .

. . . . .

. . . . . .

1-1 About the Barricade . . . . . .

. . . . .

. . . . .

. . . . . .

. . . . . .

. 1-1 Features and Benefits . . . .

. . . . .

. . . . . .

. . . . . .

. . . . .

. . . . .

. 1-2 Applications . . . . . .

. . . . . .

. . . . .

. . . . .

. . . . . .

. . . . . 1-3 2 Installation . .

. . . . .

You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

affecting outside access to your network. 1-3 INTRODUCTION · 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. · Point-to-Point Tunneling Protocol -- Provides a secure tunnel for remote client access to a PPTP security gateway.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

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 Barricade N (SMC7904WBRA-N) Power adapter One CAT-5 Ethernet cable (RJ-45) One Telephone patch cables (RJ-11) Documentation CD One Warranty information card 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 2.4 GHz 802.11n draft wireless adapter or 2.

4 GHz 802.11b/g wireless adapter installed on each PC. Alternatively an Ethernet adapter can be used. Internet Explorer 5.5 or above, Netscape 4.

7 or above, Mozilla 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. Data rates up to 300 Mbps are possible with the 802.11n function enabled. 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 LED Indicators The power and port LED indicators and the WPS button on the top panel are illustrated in the following figure and table. Figure 2-1. Top View Item Power Status On Off ADSL Sync On Flashing Off ADSL Data WLAN Blinking Off On Blinking Description The Barricade is receiving power. Normal operation. Power off or failure. ADSL connection is functioning correctly. The Barricade is establishing an ADSL link. ADSL connection is not established. ADSL port is sending/receiving data. No data is being transferred. Wireless link established.

Data is been transmitted via wireless link. 2-3 INSTALLATION Item WLAN WPS Status Off On Fast Flash Slow Flash Off LAN (4 LEDs) On Flashing Off WPS button Description No wireless link. Successful WPS connection. WPS connection failed. The Barricade is establishing WPS connection.

WPS function is off. Ethernet connection is established. The indicated LAN port is sending or receiving data. There is no LAN connection on the port. This button is located on the top panel, press this button for at least 4 seconds when activating the WPS function. Note: with successful WPS connection, the WPS LED indicator will be off after 300 seconds. 2-4 HARDWARE DESCRIPTION Rear Panel SMC7904BRA-N contains the following ports on the rear panel: Figure 2-2. Rear Panel Item ADSL Port LAN1 to LAN4 Reset Button Power Inlet Power On/Off switch 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 4-78. Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage the Barricade. Use this switch to turn on/off the power. 2-5 INSTALLATION 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 SMC7904WBRA-N is RJ-11.

2-6 CONNECT THE SYSTEM 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.

You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide

http://yourpdfguides.com/dref/3456744

2-7 INSTALLATION Connection Illustration The connection diagram shows how to connect the Barricade. 2-8 CHAPTER 3 CONFIGURING CLIENT PC After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade.

See: "Windows 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 Barricade" 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 CHAPTER 4 CONFIGURING THE BARRICADE 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 in your web browser: http://192.168.2.
1. Enter the default password: "smcadmin", and click LOGIN. Note: Password is case sensitive. 4-1 CONFIGURING THE BARRICADE Navigating the Management Interface 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 4-3 for details. For configuration details of the 13 menu items, refer to "Configuration parameters" on page 4-17. 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.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

" 4-2 SETUP WIZARD 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. 4-3 CONFIGURING THE BARRICADE Wireless Settings Configure the wireless settings on this screen. Parameter SSID SSID Broadcast Description This is the Service Set ID. The SSID must be the same on the router and all of its wireless clients. Select to enable/disable the brocasting of SSID, turning off the brocasting of SSID increases your network security.

This device supports 11n, 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. SMC recommend using "Mixed 802.11n, 802.11g and 802.11b" to provide compatibility with 11n, 11g and 11b wireless clients. Wireless Mode 4-4 SETUP WIZARD Parameter Channel Description The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the router and all of its wireless clients. The router will automatically assign itself a radio channel, or you may select one manually. Bandwidth Select the bandwidth: ·20 MHz: Sets the operation bandwidth as 20 MHz.

when 20 MHz is selected, there would be no extension channel available. ·20/40 MHz: Allows automatic detection of the operation bandwidth between 20 and 40 MHz. Choosing this mode allows you to use the extension channel. Extension Channel This is the optional channel for use. Setting the Bandwith to 20/40 MHz allows you to use this extension channel as the secondary channel for doubling the bandwith of your wireless network.

Note: (1). When the main or primary channel is set to 1, channel 5 will be used as the extension channel. If the main channel is set to 9, channel 5, or channel 13 can be used as the extension channel. (2). The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

The firmware setting is not accessible by the end user. 4-5 CONFIGURING THE BARRICADE ADSL Settings 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 4-7 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.

4-6 SETUP WIZARD 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. 4-7 CONFIGURING THE BARRICADE PPPoE Parameter VPI/VCI Encapsulation Username Password Confirm Password Description Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. 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 "Summary" on page 4-15 in the manual for details about the settings. 4-8 SETUP WIZARD PPPoA Parameter VPI/VCI Encapsulation Username Password Confirm Password Description Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. 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 "Summary" on page 4-15 in the manual for details about the settings. 4-9 CONFIGURING THE BARRICADE 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. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by 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 "Summary" on page 4-15 in the manual for details about the setting. 4-10 SETUP WIZARD 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. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied 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 "Summary" on page 4-15 in the manual for details about the settings. 4-11 CONFIGURING THE BARRICADE 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. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. Select the encapsulation used by ISP from the drop down menu. Click NEXT to continue to the "Confirm" settings screen. Go to "Summary" on page 4-15 in the manual for details about the settings.

4-12 SETUP WIZARD 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.

Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

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 "Summary" on page 4-15 in the manual for details about the settings. 4-13 CONFIGURING THE BARRICADE 1483 Routing (DHCP) Parameter DNS Server VPI/VCI Encapsulation Description Enter the DNS Server IP address provided by your ISP.

Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. Select the encapsulation used by ISP from the drop down menu. Click NEXT to continue to the "Confirm" settings screen. Go to "Summary" on page 4-15 in the manual for details about the settings. 4-14 SETUP WIZARD Summary The summary screen shows values of the configuration parameters. Check ADSL operation mode (WAN), Network Layer Parameters (WAN) and ISP parameters are correct. Parameter Wireless Parameters SSID SSID Broadcast Description Service Set ID, SSID must be the same on the Router, and all it's wireless clients. Enable SSID broadcasting on the wireless network for easy connection for the wireless clients. Disable SSID broadcast for increased security. The Router supports 11n, 11g, and 11b wireless networks.

This is the radio channel used for wireless communication. This is the time zone that you have selected. Enable or disable of the Network time protocol. The IP address of the time server. The IP address of the time server. Wireless mode Channel Time Zone Parameters Time Zone NTP Primary server Secondary server 4-15 CONFIGURING THE BARRICADE Parameter ISP Protocol VPI/VCI Description The name of the ISP you have selected from list. The WAN protocol of your ISP. If you are unsure if the selected protocol is correct check with your ISP. Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). If you are unsure the VPI/VCI values are correct check with your ISP.

ADSL Operation Mode (WAN) AAL5 Encapsulation Shows the packet encapsulation type. If you are unsure the selected Encapsulation is correct check with your ISP. Go to page 4-21 for a detailed description. Network Layer Parameters (WAN) IP Address Subnet Mask Default Gateway DNS Server WAN IP address (only displayed if you have static IP). WAN subnet mask (only displayed if you have static IP).

WAN gateway (only displayed if you have static IP). The IP address of the DNS server. If the DNS address field was left blank in previous steps the address will be displayed as 0.0.0.

0. The ISP assigned user name. The password (hidden). ISP Parameters Username Password If the parameters are correct, click FINISH to save these settings. Your Barricade is now set up. @@@@Configures the Internet connection settings. @@Configure the wireless parameters. 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. Sets the ADSL operation type and shows the ADSL status. @@@@@@@@@Select your time zone from the drop down menu. @@@@@@@@The default password is "smcadmin". @@@@@@@@@@@@@@@@@@Click the VC to set the detailed parameters. The Barricade can support up to 8 Virtual Circuits (VC's). @@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. 4-23 CONFIGURING THE BARRICADE 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 VPI/VCI Encapsulation QoS Class PCR/SCR/MBS Description Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied 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 (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) are configurable. 4-24 CONFIGURATION PARAMETERS PPPoA Parameter VPI/VCI Encapsulation QoS Class PCR/SCR/MBS IP assigned by ISP IP Address Subnet Mask Connect Type Description Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied 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. 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 4-25 CONFIGURING THE BARRICADE 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. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied 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. 4-26 CONFIGURATION PARAMETERS PPPoE Parameter VPI/VCI Encapsulation QoS Class PCR/SCR/MBS IP assigned by ISP IP Address Subnet Mask Connect Type Description Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. Select the encapsulation used by ISP from the drop-down menu.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

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 4-27 CONFIGURING THE BARRICADE 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. Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied 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. 4-28 CONFIGURATION PARAMETERS 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. 4-29 CONFIGURING THE BARRICADE 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.
4-30 CONFIGURATION PARAMETERS LAN The LAN settings menu allows you to change the default IP address of the Barricade, modify the DHCP server settings. Parameter LAN IP IP Address IP Subnet Mask DHCP Server Lease Time 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.
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/end 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.

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 4-31 CONFIGURING THE BARRICADE Wireless The router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the domain identifier, and the security options. · Enable or disable Wireless module function: select to enable or disable the wireless function. 4-32 CONFIGURATION PARAMETERS Channel and SSID You must specify a common radio channel and SSID (Service Set ID) to be used by the router and all of its wireless clients. Be sure you configure all of its clients to the same values. Parameter SSID SSID Broadcast Description This is the Service Set ID. The SSID must be the same on the router and all of its wireless clients. Select to enable/disable the brocasting of SSID.
Enable this function for easy connection for the clients. Disable this function for increased security. The Router supports 11n, 11g, and 11b wireless networks. SMC recommend using "Mixed 802.11n, 802.
11g and 802.11b" to provide compatibility with 11n, 11g and 11b wireless clients. Wireless Mode Channel This is the radio channel used for wireless communication. 4-33 CONFIGURING THE BARRICADE Parameter Bandwidth Description Select the bandwidth: ·20 MHz: Sets the operation bandwidth as 20 MHz. when 20 MHz is selected, there would be no extension channel available.
·20/40 MHz: Allows automatic detection of the operation bandwidth between 20 and 40 MHz. Choosing this mode allows you to use the extension channel. Extension Channel This is the optional channel for use. Setting the Bandwith to 20/40 MHz allows you to use this extension channel as the secondary channel for doubling the bandwith of your wireless network. In most situations, best performance is achieved with Protected Mode turning Off. If you are operating in an environment with heavy 802.11b traffic or interference, best performance may be achieved with Protected Mode turning On. Select to turn on/turn off the QoS function. Protected Mode 802.11e/WMM QoS Note: (1).

When bandwidth is set to 20 MHz, there would be no extension channel that can be selected. The extension channel is based on the main or primary channel. When the main channel is set to channel 1, channel 5 will be used as the extension channel. When the main channel is set to 9, the extension channel can be channel 5 or 13. (2). The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user. 4-34 CONFIGURATION PARAMETERS Access Control Using the Access Control functionality, you can restrict access based on MAC address. Each PC has a unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, the computers whose MAC address you have listed in the filtering table will be able to connect (or will be denied access) to the router.
· · Enable MAC Filtering: select to enable or disable this function. Access Rule for registered MAC address: select to allow/deny access for the registered MAC addresses. Selecting Allow means only MAC addresses registered here will be able to connect to the router. Selecting Deny means only the MAC addresses registered here will be denied access to the router. Wireless DHCP Client List: use the drop down list to quickly copy the current entry to the table. MAC Filtering Table: you can enter up to 32 stations to the table.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744

· · 4-35 CONFIGURING THE BARRICADE Security To make your wireless network safe, you should turn on the security function. Allowed Client Type: · · · No WEP, No WPA - this means no security mechanism will be used on your wireless network. WEP only - this menas only WEP will be used for your wireless communication. WPA only - this means only WPA will be used for the wireless network.

4-36 CONFIGURATION PARAMETERS WEP Parameter WEP Mode Key Entry Method Key Provisioning Description Select 64 bit, or 128 bit. Select Hex, or ASCII. Select Static, or Dynamic. If you select Static, you will need to configure the Static WEP Key Setting section. If you choose Dynamic, then 802.1X authentication should be enabled. To automatically generate encryption keys using the passphrase function, when Key Entry Method is set to Hex, enter a string into the passphrase field, then click Generate. Select the Default Key ID from the drop-down menu and click SAVE SETTINGS. To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. Note: A hexadecimal digit is a number or letter in the range 0-9 or A-F.

The passphrase can consist of up to 32 alphanumeric characters. 4-37 CONFIGURING THE BARRICADE WPA Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service. The router supports both WPA and WPA2. Parameter WPA mode Cypher suite Authentication Description Select WPA, WPA2 or mixed mode. Select the encryption cypher for use. Choose 802.1X or Pre-shared Key to use as the authentication method.

· 802.1X: for the enterprise network with a RADIUS server. · Pre-shared key: for the SOHO network environment without an authentication server. Pre-shared key type Pre-shared Key Group Key Re_Keying Select the key type to be used in the Pre-shared Key. Enter the key string here.

Define the time period for re-obtain the key. 4-38 CONFIGURATION PARAMETERS 802.1X If 802.1X is used in your network, then you should enable this function for the router. Parameter 802.

1X authentication Session Idle Timeout Re-Authentication Period Quiet Period Server Type RADIUS Server Parameters Server IP Server Port Description Choose to enable or disable this function. Defines a maximum period of time for which the connection is maintained during inactivity. Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client. Defines a maximum period of time for which the router will wait between failed authentications. Select RADIUS. Enter the authentication server IP address. Enter the port number. 4-39 CONFIGURING THE BARRICADE Parameter Secret Key NAS-ID Description The secret key shared between the authentication server and its clients. Defines the request identifier of the Network Access Server. WPS (Wi-Fi Protected Setup) The Barricade was implemented with the ease-of-use Wi-Fi Protected Setup (WPS).

WPS makes a secure wireless network much easier to achieve by using a PIN number and the Push Button Control (PBC). · · · Enable or disable WPS features: select to enable or disable. Generate New PIN: click this button to create a new PIN. Restore Default PIN: click this button to restore the PIN. 4-40 CONFIGURATION PARAMETERS Note: If you are using WEP encryption on the SMC Barricade and Windows Zero Configuration (WZC) service to configure the wireless settings on your PC you may experience problems connecting to the SMC Barricade. Refer to the "Troubleshooting" section for further details. PIN Enter the PIN of the client device and click Start PIN. Then start WPS on the client device from it's wireless utility or WPS application within 2 minutes. Take the following steps for easy network security settings. 1.

Power on your client device supporting WPS PIN code method. 2. Start WPS PIN process on client device. For instructions on how to do this refer to the client devices user manual. 3.

Enter the PIN code of client device. Note: The PIN code is generally printed on the bottom of the unit or displayed in the utility. 4. Click the Start PIN button on the screen. 4-41 CONFIGURING THE BARRICADE PBC (Push Button Configuration) To achieve successful WPS connection, you can use one of the following ways: (1) push and hold the WPS button on this router for 4 seconds or (2) click the Start PBC button on this screen.

Now click the WPS button on the client device which you are connecting. Make sure the client device is powered on. Note: This connection procedure must be done within 2 minutes after pressing the WPS button on the router. 4-42 CONFIGURATION PARAMETERS Manual For client devices without the WPS function, you should manually configure the client device with the settings on this screen. 4-43 CONFIGURING THE BARRICADE NAT Network Address Translation (NAT) allows multiple users to access the Internet sharing one public IP. · Enable or disable NAT module function: select to enable or disable this function. 4-44 CONFIGURATION PARAMETERS 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.

4-45 CONFIGURING THE BARRICADE 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. 4-46 CONFIGURATION PARAMETERS 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.


You're reading an excerpt. Click here to read official SMC 7904WBRA-N user guide
http://yourpdfguides.com/dref/3456744