




USER GUIDE



ADSL2 Barricade N
Draft 11n Wireless 4-port Annex A ADSL2/2+ Modem Router

SMC7904WBRA-N



Router with built-in ADSL2/2+ Modem

From SMC's line of award-winning connectivity solutions

SMC[®]

Networks

20 Mason

Irvine, CA 92618

Phone: (949) 679-8000

August 2007

R.01 F/W 0.11

Information furnished is believed to be accurate and reliable. However, no responsibility is assumed by our company for its use, nor for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of our company. We reserve the right to change specifications at any time without notice.

Copyright © 2007 by
SMC Networks, Inc.
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.

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, NEGLIGENCE, 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

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.

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

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 used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: ACYDL01B7904WBRAN. The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

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 its 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.

Company: SMC Networks North America
Address: 20 Mason, Irvine, CA 92618. USA
Telephone number: 800-762-4968

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.

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.
Finnish	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.
Dutch	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
Swedish	Härmed intygar SMC Networks att denna Radio LAN device står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede SMC Networks erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF
German	Hiermit erklärt SMC Networks, dass sich dieser/diese/dieses Radio LAN device in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMWi) Hiermit erklärt SMC Networks die Übereinstimmung des Gerätes Radio LAN device mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
Greek	Με την παρουσία smc networks δηλώνει ότι radio LAN device συμμορφώνεται προς τις ουσιαστικές απαιτήσεις και τις λοιπές σχετικές διατάξεις της οδηγίας 1999/5/εκ
Italian	Con la presente SMC Networks dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Spanish	Por medio de la presente SMC Networks declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE
Portuguese	SMC Networks declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

NCC Statement

- (1) 經審驗合格之射頻電信終端設備，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- (2) 射頻電信終端設備之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。所謂合法通信，係指依電信法規定作業之無線電信。
- (3) 輸入、製造射頻電信終端設備之公司、商號或其使用者違反本辦法規定，擅自使用或變更無線電頻率，電功率者，除依電信法規定處罰外，電信總局並得撤銷其審驗合格證明。
- (4) 本機限在不干擾合法電台與不受被干擾保障條件下於室內使用。
- (5) 為減少電磁波干擾，請妥適使用。

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 Netzanschlusßsteckdose 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 Netzanschlusßleitung 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 autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. 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.

TABLE OF CONTENTS

Introduction	1-1
About the Barricade	1-1
Features and Benefits	1-2
Applications	1-3
Installation	2-1
Package Contents	2-1
System Requirements	2-2
Hardware Description	2-2
LED Indicators	2-3
Rear Panel	2-5
ISP Settings	2-6
Connect the System	2-6
Connect the ADSL Line	2-6
Attach to Your Network Using Ethernet Cabling	2-7
Connect the Power Adapter	2-7
Connection Illustration	2-8
Configuring Client PC	3-1
TCP/IP Configuration	3-1
Windows 2000	3-2
Disable HTTP Proxy	3-3
Obtain IP Settings from Your Barricade	3-3
Windows XP	3-5
Disable HTTP Proxy	3-5
Obtain IP Settings from Your Barricade	3-6
Configuring Your Macintosh Computer	3-7
Disable HTTP Proxy	3-8

Configuring the Barricade	4-1
Navigating the Management Interface	4-2
Making Configuration Changes	4-2
Setup Wizard	4-3
Time Zone	4-3
Wireless Settings	4-4
ADSL Settings	4-6
Parameter Setting - Country or ISP Not Listed	4-7
Summary	4-15
Configuration parameters	4-17
System	4-19
WAN	4-22
LAN	4-31
Wireless	4-32
NAT	4-44
Routing	4-49
Firewall	4-53
SNMP	4-66
UPnP	4-69
ADSL	4-70
DDNS	4-73
Tools	4-74
Status	4-79
Finding the MAC address of a Network Card	4-82
Windows 2000/XP	4-82
Macintosh	4-82
Linux	4-82

Troubleshooting A-1

Cables B-1

 Ethernet Cable B-1

 Specifications B-1

 Wiring Conventions B-1

 RJ-45 Port Connection B-2

 Pin Assignments B-3

 ADSL Cable B-5

 Specifications B-5

 Wiring Conventions B-5

Specifications C-1

CHAPTER 1

INTRODUCTION

Congratulations on your purchase of the 802.11n ADSL2 Barricade™, hereafter referred to as the “Barricade”. We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, this router provides a convenient and powerful solution.

About the Barricade

The Barricade provides Internet access to multiple users by sharing a single-user account. It is simple to configure and can be up and running in minutes.

The Barricade is compliant with the next generation IEEE 802.11n draft v2.0 specification while maintaining full backwards compatibility with the current 802.11b/g standards.

802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughputs for up to 300 Mbps.

This provides sufficient bandwidth to stream HD video, listen to digital music, play online games, transfer large files, make VoIP calls and surf the Internet simultaneously.

Features and Benefits

- Intergrated ADSL modem for connecting to ADSL line
- Fully backward compatible with 802.11 g/802.11 b networks
- Wireless speeds up to 300 Mbps.
- Increased speed and coverage - up to 5 times the speed of 802.11g
- 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 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 and Wireless LAN**

The Barricade provides connectivity to 10/100 Mbps devices, and wireless connection speed up to 300 Mbps. This router is fully compliant with specifications defined in IEEE 802.11b, IEEE 802.11g and IEEE 802.11n draft v2.0 standards, 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 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.

- **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.

- 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.

CHAPTER 2

INSTALLATION

Before installing the Barricade™, verify that you have all the items listed under the Package Contents list. If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Barricade. After installing the Barricade, refer to Configuring the Barricade™ on page 4-1.

Package Contents

After unpacking, 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.

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.

LED Indicators

The power and port LED indicators and the WPS button on the top panel are illustrated in the following figure and table.

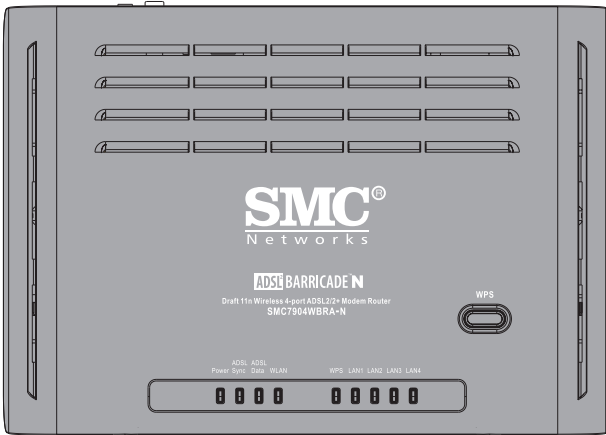


Figure 2-1. Top View

Item	Status	Description
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
ADSL Sync	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL Data	Blinking	ADSL port is sending/receiving data.
	Off	No data is being transferred.
WLAN	On	Wireless link established.
	Blinking	Data is been transmitted via wireless link.

Item	Status	Description
WLAN	Off	No wireless link.
WPS	On	Successful WPS connection.
	Fast Flash	WPS connection failed.
	Slow Flash	The Barricade is establishing WPS connection.
	Off	WPS function is off.
LAN (4 LEDs)	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.
WPS button		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.

Rear Panel

SMC7904BRA-N contains the following ports on the rear panel:

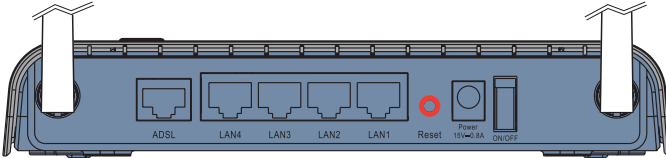


Figure 2-2. Rear Panel

Item	Description
ADSL Port	Connect your ADSL line to this port (RJ-11 port).
LAN1 to LAN4	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).
Reset Button	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.
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage the Barricade.
Power On/Off switch	Use this switch to turn on/off the power.

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.

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

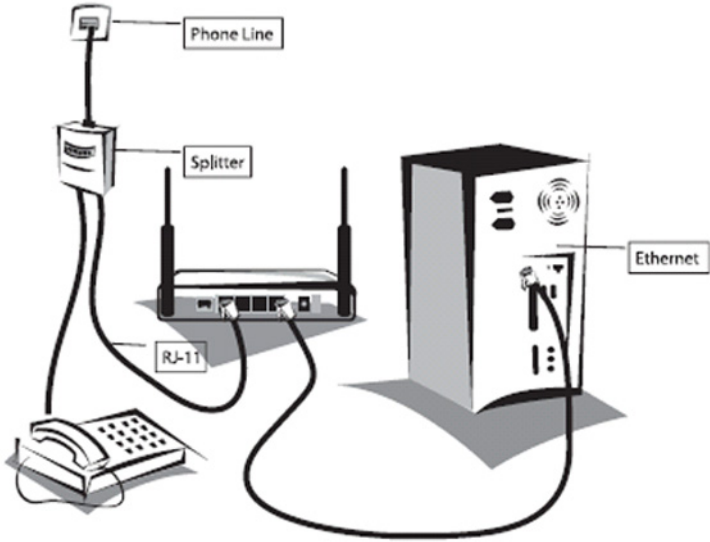
Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet.

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.

Connection Illustration

The connection diagram shows how to connect the Barricade.



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:

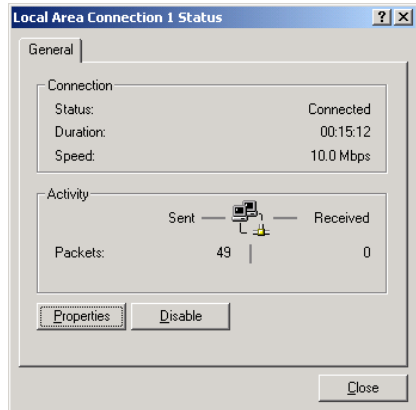
IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

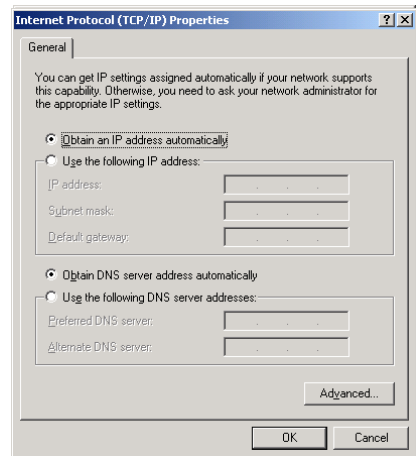
Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade’s web configuration interface in order to make the required changes. (See “Configuring the Barricade” on page 4-1 for instruction on configuring the Barricade.)

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.



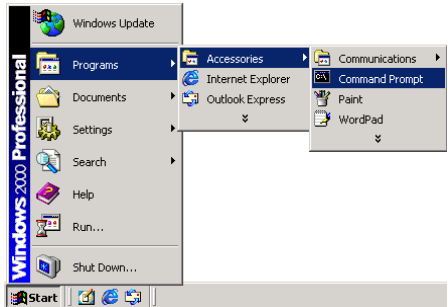
Disable HTTP Proxy

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**.

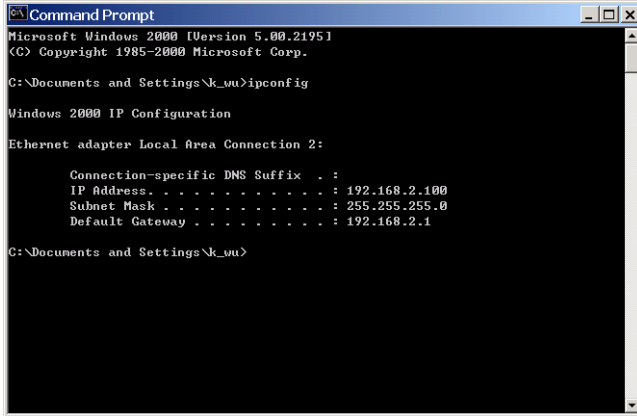


2. In the Command Prompt window, type “**IPCONFIG /RELEASE**” and press the ENTER key.

```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>IPCONFIG /RELEASE
Windows 2000 IP Configuration
IP address successfully released for adapter "Local Area Connection 1"
C:\>_
```

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.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\k_wu>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\Documents and Settings\k_wu>
```

4. Close the Command Prompt window.

Your computer is now configured to connect to the Barricade.

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.

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.

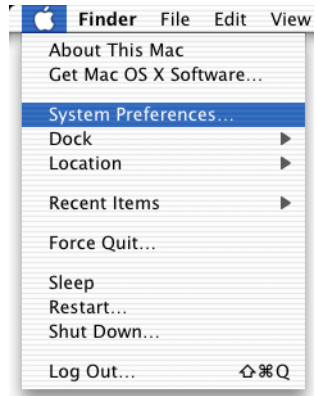
Your computer is now configured to connect to the Barricade.

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:

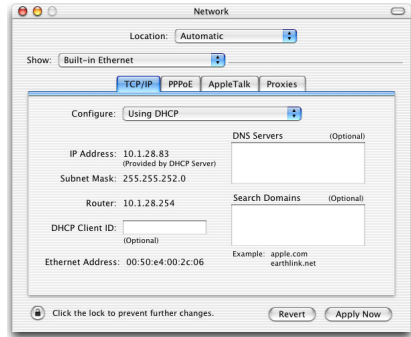
1. Pull down the Apple Menu . Click **System Preferences**.



2. Double-click the **Network** icon in the Systems Preferences window.



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.

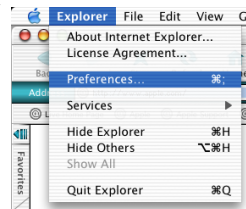
Now your computer is configured to connect to the Barricade.

Disable HTTP Proxy

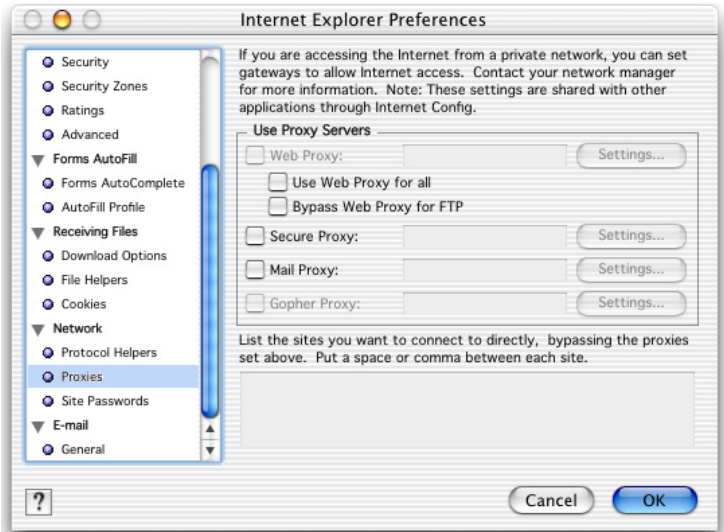
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

1. Open Internet Explorer and click **Explorer/Preferences**.
2. In the Internet Explorer Preferences window, under Network, select **Proxies**.



3. Uncheck all check boxes and click OK.



CHAPTER 4

CONFIGURING THE

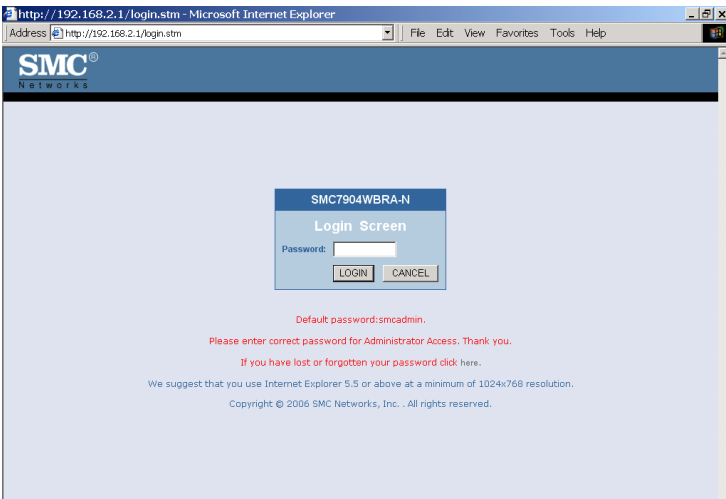
BARRICADE

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`.

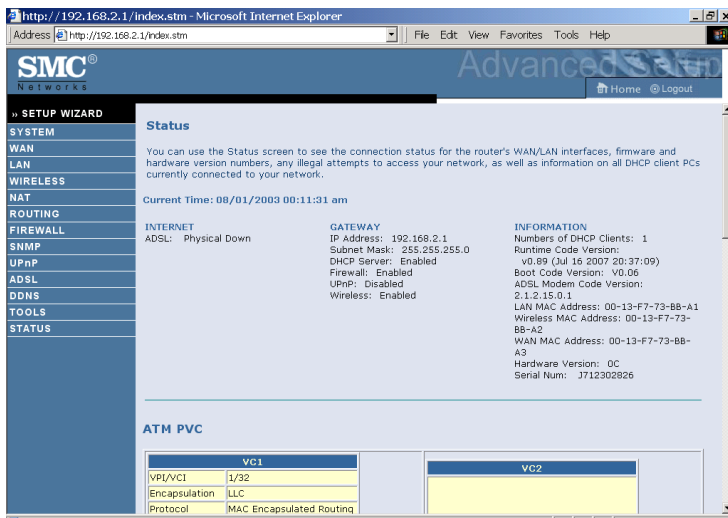
Enter the default password: "smcadmin", and click **LOGIN**.

Note: Password is case sensitive.



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

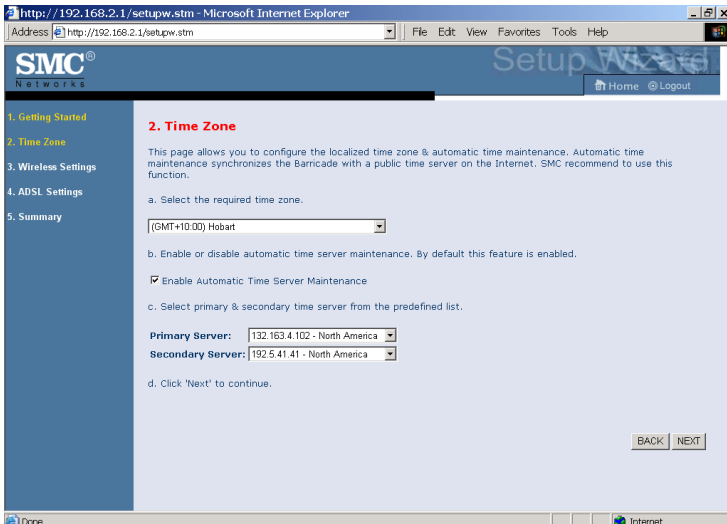
Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click the **APPLY** or **SAVE SETTINGS** or **NEXT** button at the bottom of the screen to enable the new setting.

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.”

SETUP WIZARD

Time Zone

Click on **SETUP WIZARD** and **NEXT**, you will see the time zone screen.



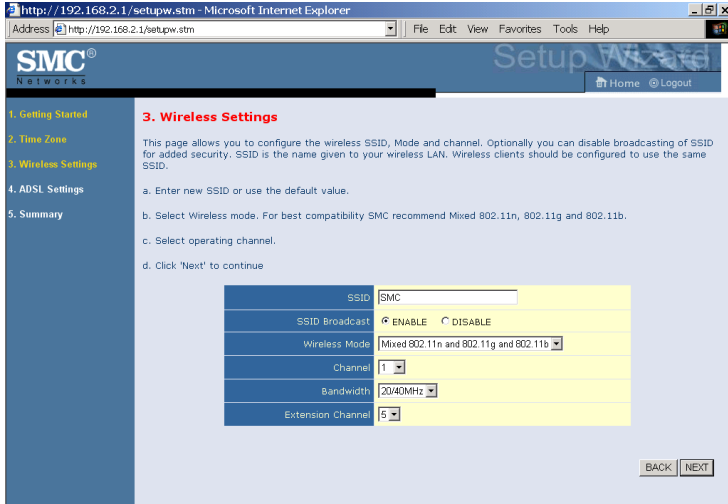
Select your local time zone from the drop down menu. This information is used for log entries and client filtering.

If you want to automatically synchronize the ADSL router with a public time server, check the **Enable Automatic Time Server Maintenance** box. Select the desired servers from the drop down menu.

Click **NEXT** to continue.

Wireless Settings

Configure the wireless settings on this screen.



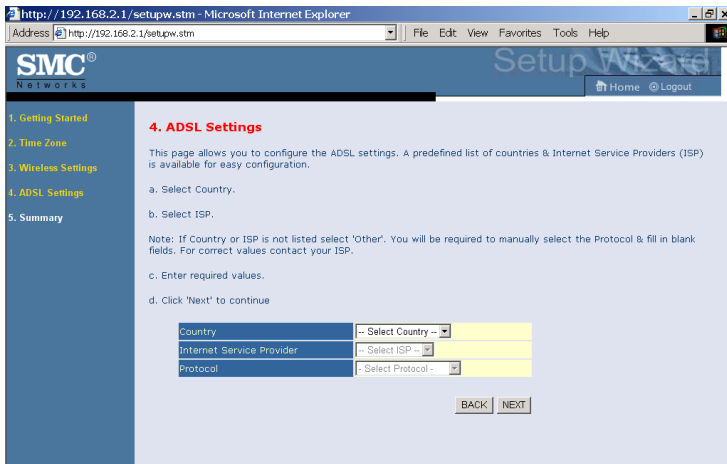
Parameter	Description
SSID	This is the Service Set ID. The SSID must be the same on the router and all of its wireless clients.
SSID Broadcast	Select to enable/disable the brocasting of SSID, turning off the brocasting of SSID increases your network security.
Wireless Mode	This device supports 11n, 11g 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.

Parameter	Description
Channel	<p>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.</p> <p>The router will automatically assign itself a radio channel, or you may select one manually.</p>
Bandwidth	<p>Select the bandwidth:</p> <ul style="list-style-type: none"> •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	<p>This is the optional channel for use. Setting the Bandwidth to 20/40 MHz allows you to use this extension channel as the secondary channel for doubling the bandwidth of your wireless network.</p>

- Notes:**
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.

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.



The screenshot shows a web browser window titled "http://192.168.2.1/setup.stm - Microsoft Internet Explorer". The address bar shows "http://192.168.2.1/setup.stm". The page header includes the SMC Networks logo and "Setup Wizard" text. A navigation menu on the left lists: 1. Getting Started, 2. Time Zone, 3. Wireless Settings, 4. ADSL Settings (highlighted), and 5. Summary. The main content area is titled "4. ADSL Settings" and contains the following text: "This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration." Below this are instructions: "a. Select Country.", "b. Select ISP.", "c. Enter required values.", and "d. Click 'Next' to continue." A note states: "Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP." The form includes three dropdown menus: "Country" (with "-- Select Country --"), "Internet Service Provider" (with "-- Select ISP --"), and "Protocol" (with "-- Select Protocol --"). At the bottom right are "BACK" and "NEXT" buttons.

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.

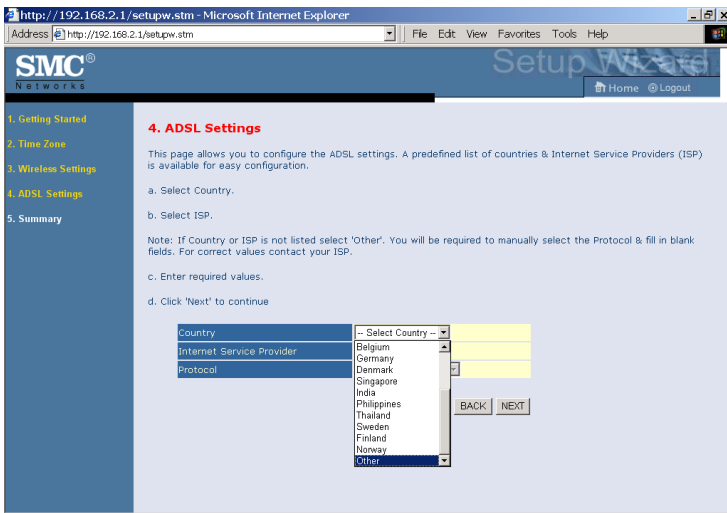
Parameter Setting - Country or ISP Not Listed

If your Country or Internet Service Provider is not listed, select **Other**.

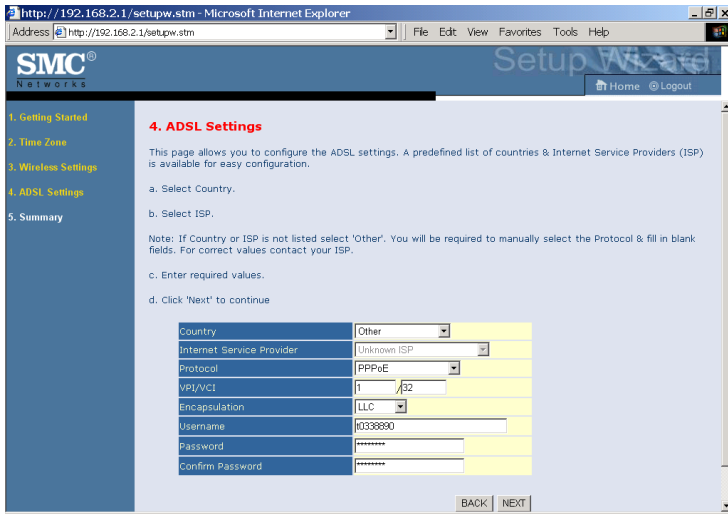
This will allow you to manually configure your ISP settings.

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.



PPPoE

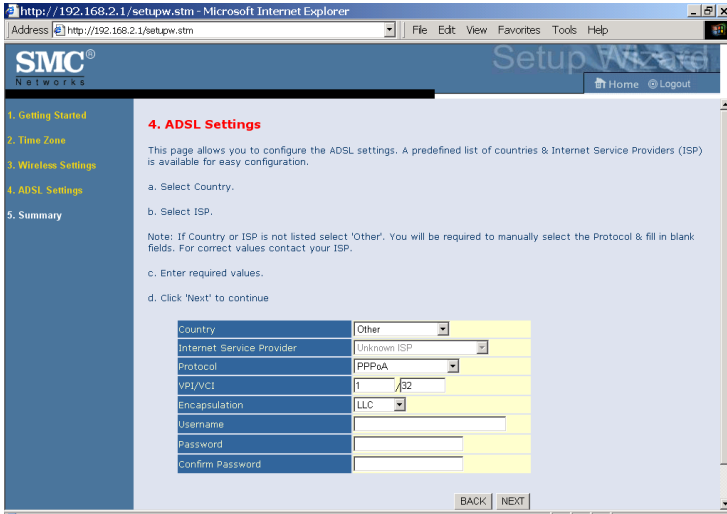


Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down menu.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.
Confirm Password	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.

PPPoA

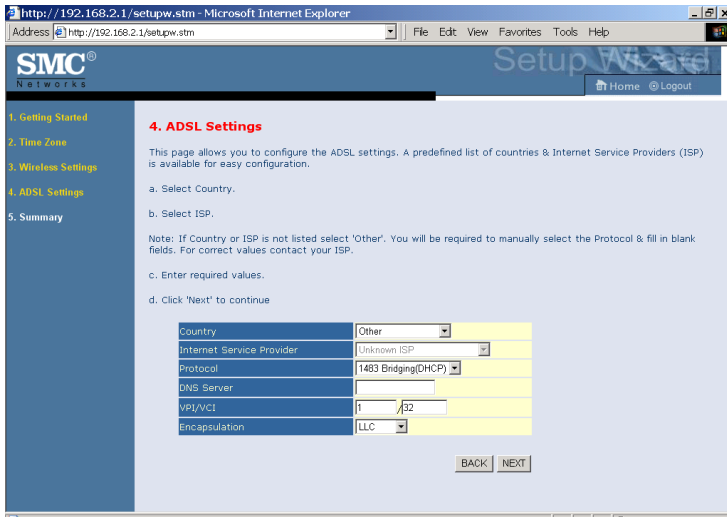


Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.
Confirm Password	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.

1483 Bridging (DHCP)

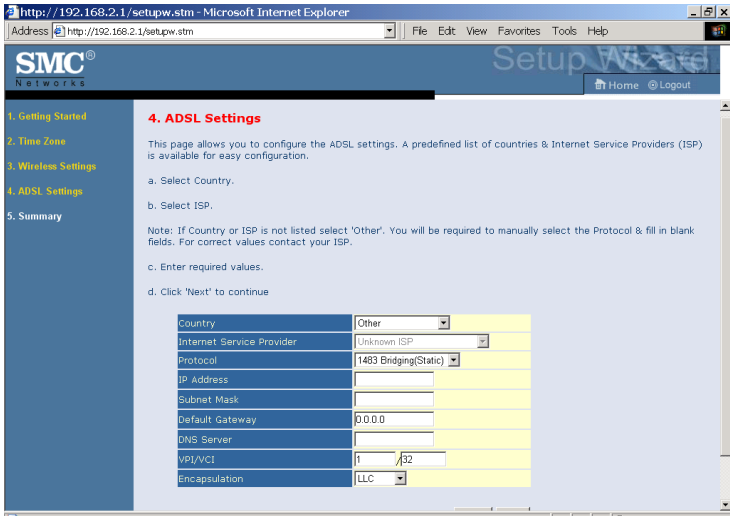


Parameter	Description
DNS Server	Enter the DNS Server IP address provided by your ISP. If your ISP has not provided you with a DNS address, leave this field blank. The Barricade will automatically obtain the DNS address from your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	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 setting.

1483 Bridging (Static)

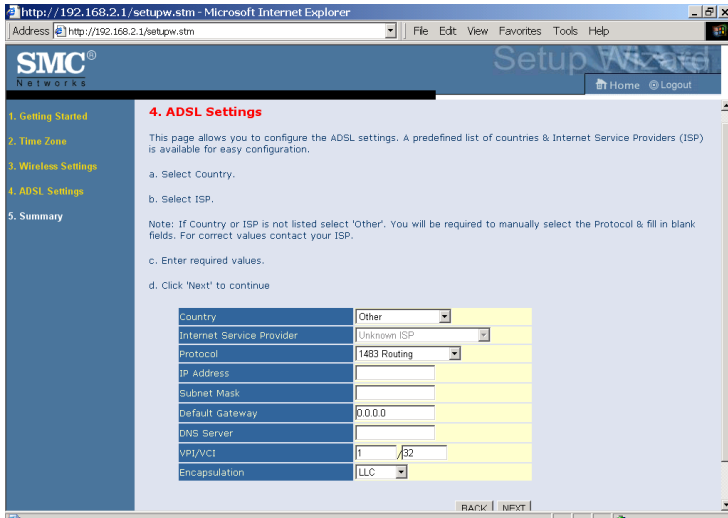


Parameter	Description
IP Address	Enter your ISP supplied static IP address here
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	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.

1483 Routing

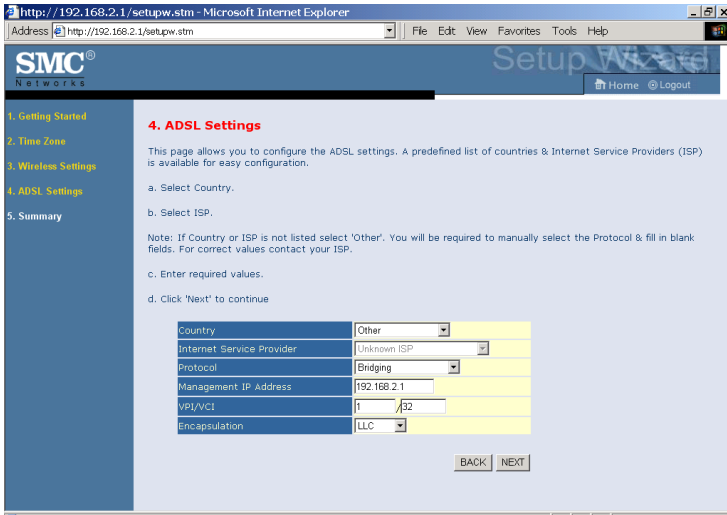


Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	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.

Bridging

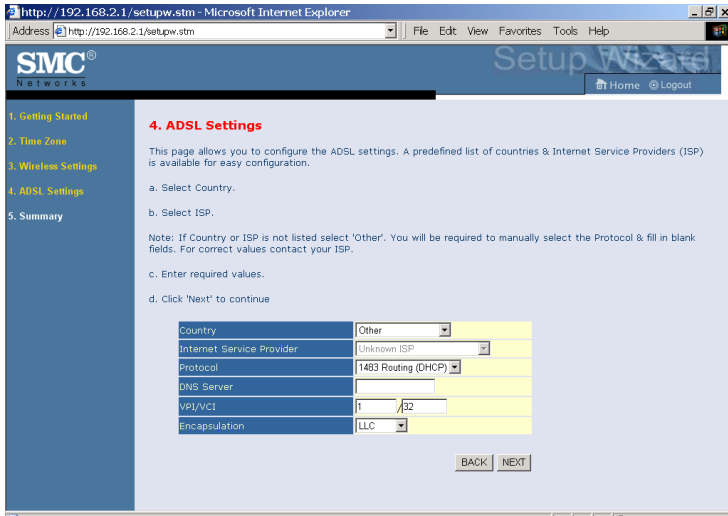


Parameter	Description
Management IP Address	Management IP address of the Barricade (Default:192.168.2.1). When configured in "Bridging" mode you will be able to manage the Barricade using this IP address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	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.

1483 Routing (DHCP)



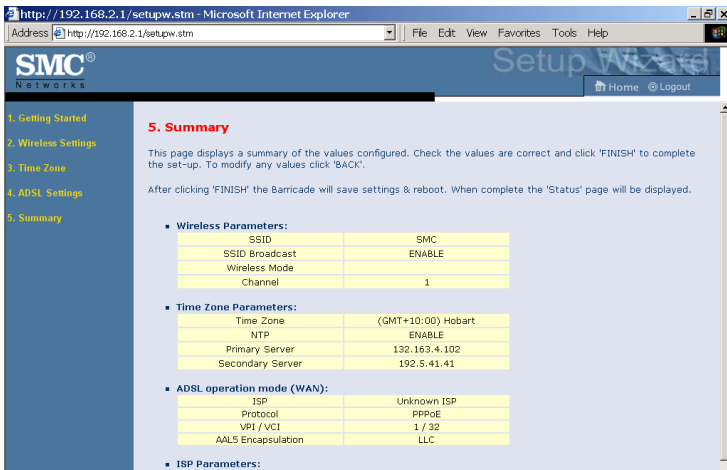
Parameter	Description
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down menu.

Click **NEXT** to continue to the “Confirm” settings screen.

Go to “Summary” on page 4-15 in the manual for details about the settings.

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	Description
-----------	-------------

Wireless Parameters

SSID	Service Set ID, SSID must be the same on the Router, and all its wireless clients.
SSID Broadcast	Enable SSID broadcasting on the wireless network for easy connection for the wireless clients. Disable SSID broadcast for increased security.
Wireless mode	The Router supports 11n, 11g, and 11b wireless networks.
Channel	This is the radio channel used for wireless communication.

Time Zone Parameters

Time Zone	This is the time zone that you have selected.
NTP	Enable or disable of the Network time protocol.
Primary server	The IP address of the time server.
Secondary server	The IP address of the time server.

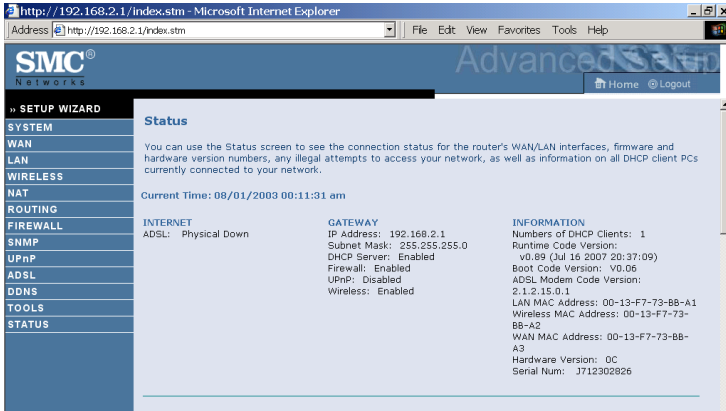
Parameter	Description
ADSL Operation Mode (WAN)	
ISP	The name of the ISP you have selected from list.
Protocol	The WAN protocol of your ISP. If you are unsure if the selected protocol is correct check with your ISP.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). If you are unsure the VPI/VCI values are correct check with your ISP.
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	WAN IP address (only displayed if you have static IP).
Subnet Mask	WAN subnet mask (only displayed if you have static IP).
Default Gateway	WAN gateway (only displayed if you have static IP).
DNS Server	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.
ISP Parameters	
Username	The ISP assigned user name.
Password	The password (hidden).

If the parameters are correct, click **FINISH** to save these settings.

Your Barricade is now set up. Go to “Troubleshooting” on page A-1 if you cannot make a connection to the Internet.

Configuration parameters

There are 13 main menu items located on the left side of the screen. Each main menu item is described in the following table.



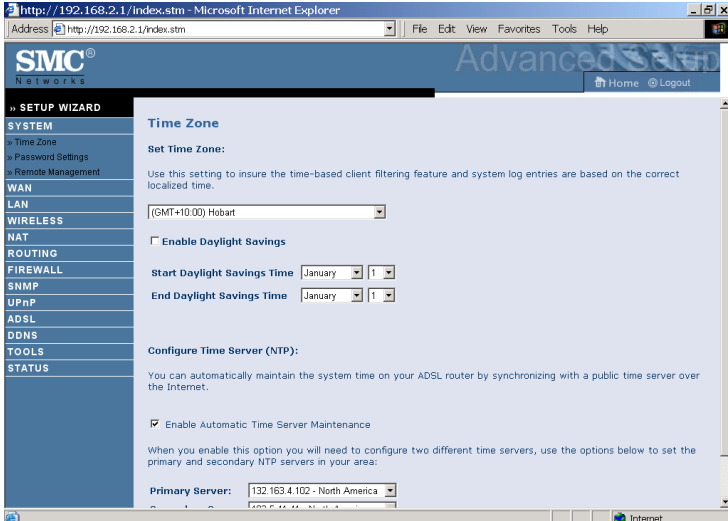
Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.
WAN	Configures the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.
Wireless	Configure the wireless parameters.
NAT	Configures Address Mapping, virtual server and special applications.
Routing	Sets the routing parameters and displays the current routing table.
Firewall	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection, and DMZ.
SNMP	Community string and trap server settings.
UPnP	Enable/disable the Universal Plug and Play function.
ADSL	Sets the ADSL operation type and shows the ADSL status.
DDNS	Configures Dynamic DNS function.

Menu	Description
Tools	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.
Status	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log.

System

Time Zone

Select your local time zone from the drop down menu. This information is used for log entries and client filtering.



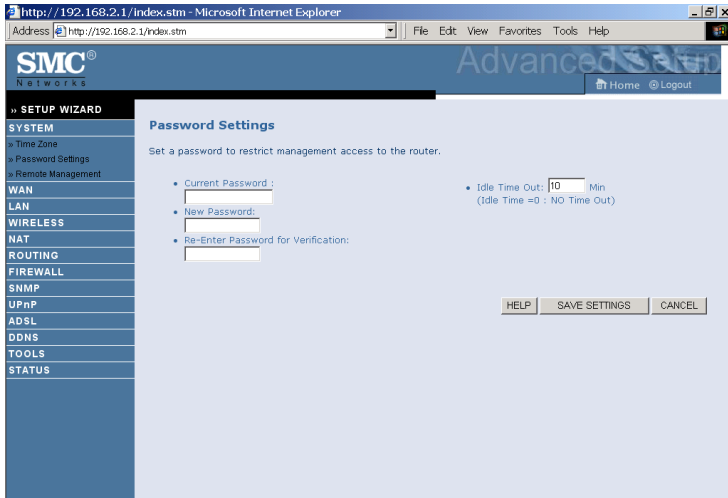
For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down menu.

If daylight savings is used in your area, check the box to enable the function, and select the start/end dates.

If you want to automatically synchronize the ADSL router with a public time server, check the **Enable Automatic Time Server Maintenance** box. Select the desired servers from the drop down menu.

Password Settings

Use this screen to change the password for accessing the management interface.



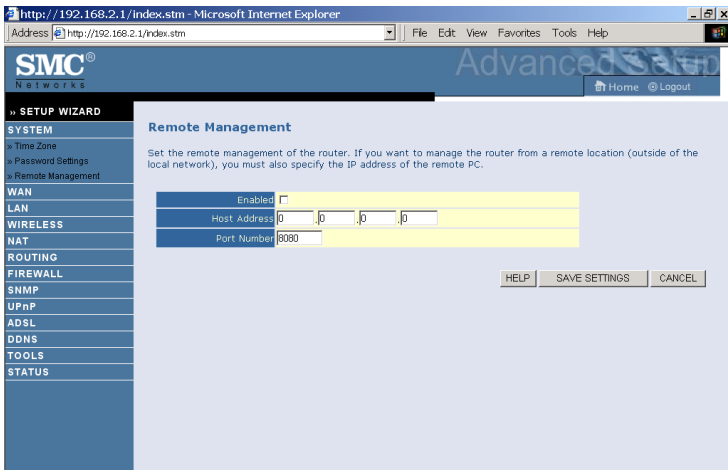
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

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)

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 enable this function 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.

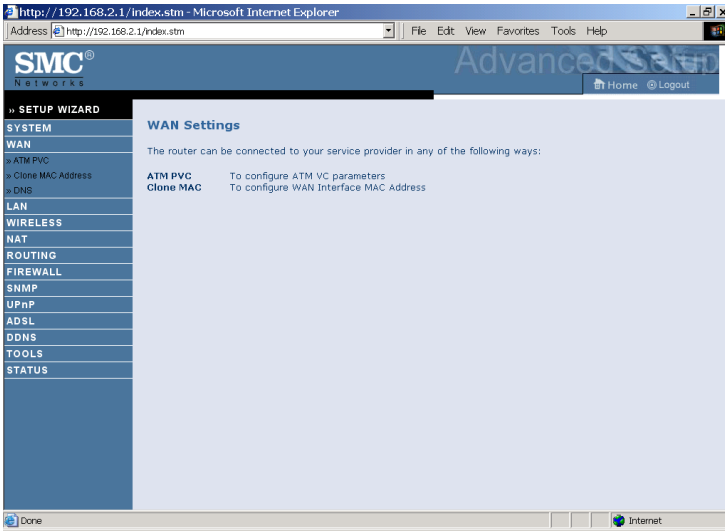


WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

The following three items are configurable:

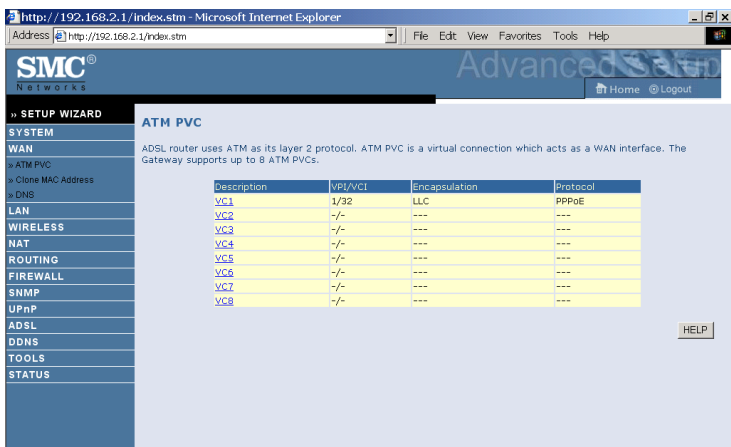
- ATM PVC
- Clone MAC
- DNS



ATM PVC

To configure your Internet Connection settings, select **ATM PVC**, then **VC1**. Click the VC to set the detailed parameters. 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	Description
VC1 to VC8	Click on the desired VC to configure the connection parameters.
VPI/VCI	Displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for the corresponding VC.
Encapsulation	Displays the Encapsulation configured for the corresponding VC. Encapsulation specifies how to handle multiple protocols at the ATM transport layer. <ul style="list-style-type: none"> 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.

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.

ATM1	
Protocol	1483 Bridging
VPI/VCI	1 / 32
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10

Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR
PCR/SCR/MBS	QoS Parameters - PCR (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) are configurable.

PPPoA

ATM1	
Protocol	PPPoA
VPI/VCI	1 / 32
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Auto - Triggered by traffic
Idle Time (Minute)	20
Username	
Password	
Confirm Password	
MTU	1492

Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
IP assigned by ISP	Select Yes if the IP address was provided by your ISP
IP Address	Enter the IP address provided by your ISP. For dynamic IP leave this field blank.
Subnet Mask	Enter the subnet mask address provided by your ISP. For dynamic IP leave this field blank.
Connect Type	Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.
Idle Time (Minute)	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.
Username	Enter user name.
Password	Enter password.