SMC® Networks

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

May 2008
R.02 F/W 0.11

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.

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.

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 AUSTRALIA is:

SMC Networks Australia
1 / 14 Wellington Street
ACACIA RIDGE, QLD 4110

Tel 1300 725 323

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.

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 παρουσα smc networks δηλωνει οτι radio LAN device συμμορφωνεται προσ τισ ουσιωδεισ απαιτησεισ και τισ λοιπεσ σχετικεσ διαταξεισ τησ οδηγιασ 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) 爲減少電磁波干擾， 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 Netzanschlu ßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. 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

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.

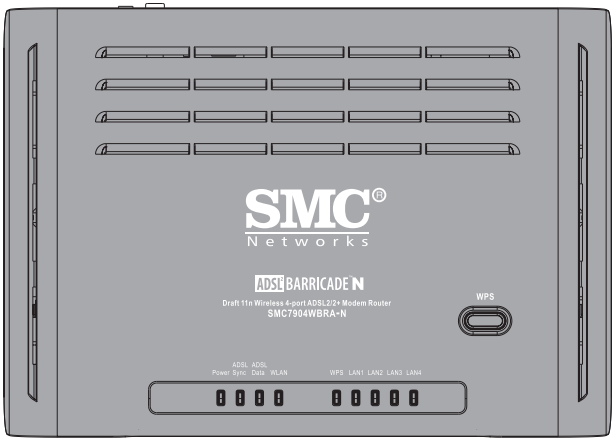


Figure 2-1. Top View

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:

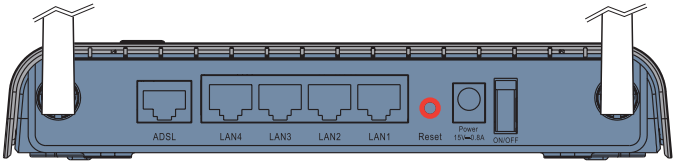


Figure 2-2. Rear Panel

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

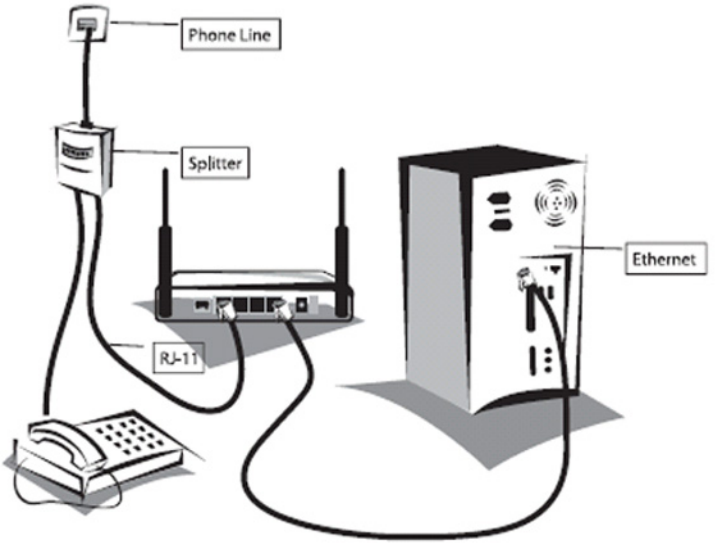
Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet.

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

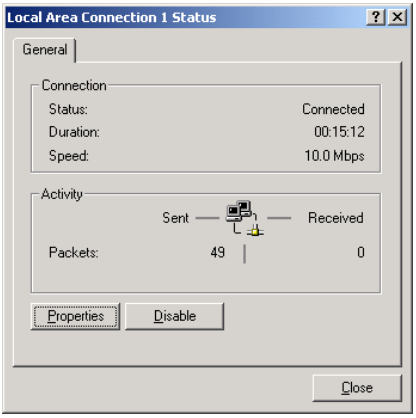
Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade's web configuration interface in order to make the required changes. (See "Configuring the Barricade" on page 4-1 for instruction on configuring the Barricade.)

Windows 2000

1. On the Windows desktop, click **Start/Settings/Network** and **Dial-Up Connections**.

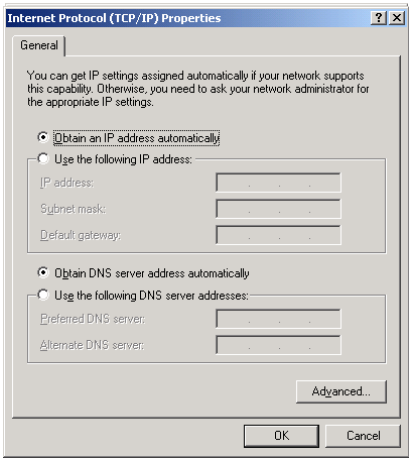
2. Click the icon that corresponds to the connection to your Barricade.

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.



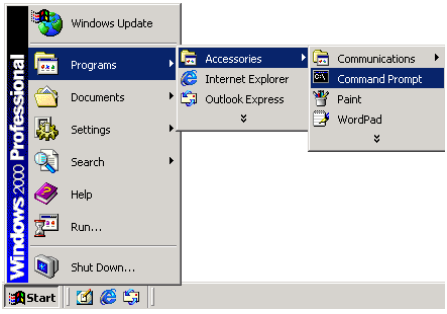
Disable HTTP Proxy

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.

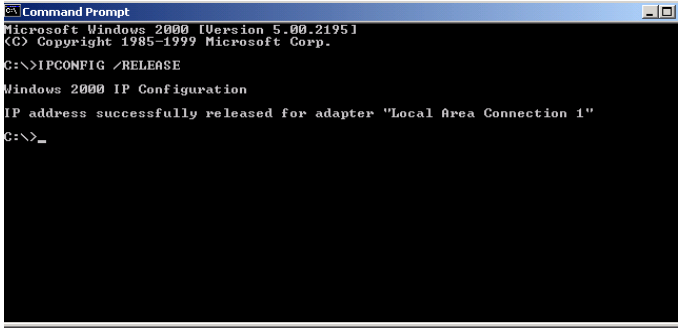
Obtain IP Settings from Your Barricade

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.

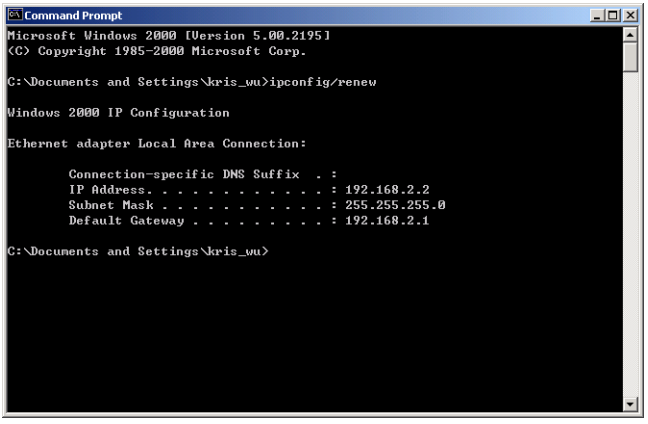
1. On the Windows desktop, click **Start/Programs/ Accessories/ Command Prompt**.



2. In the Command Prompt window, type **ipconfig /release** and press the **Enter** key.



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.

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.

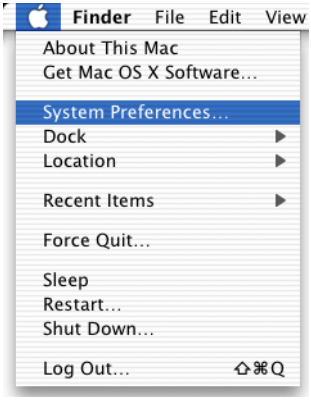
Your computer is now configured to connect to the Barricade.

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.

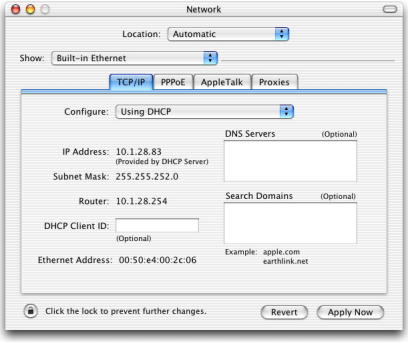
Follow these instructions:

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.

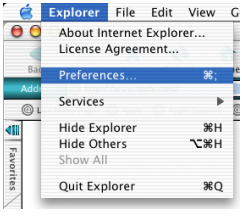
Disable HTTP Proxy

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.

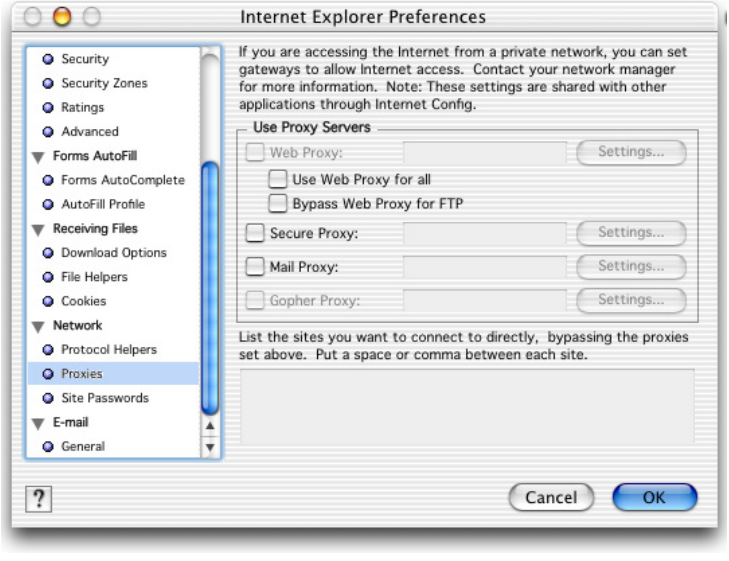
Internet Explorer

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**.

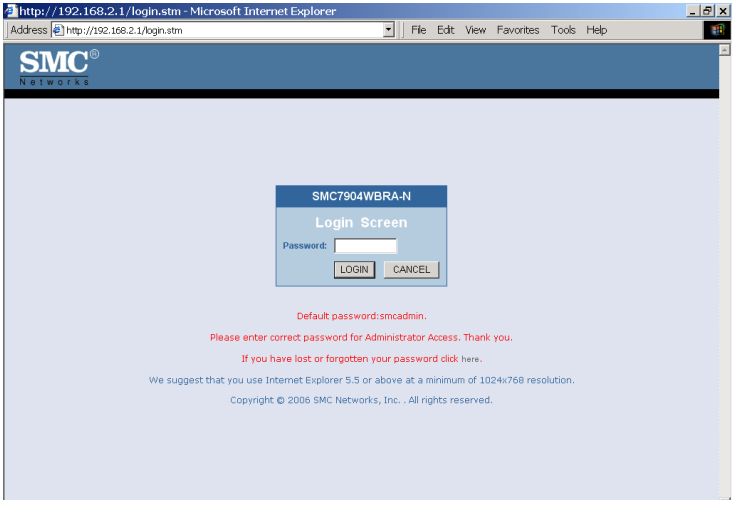


CHAPTER 4
CONFIGURING THE BARRICADE

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

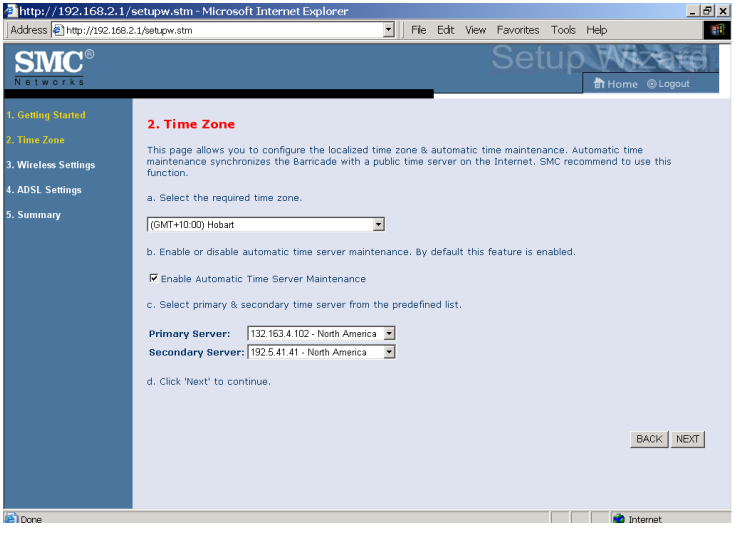
Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click the **APPLY** or **SAVE SETTINGS** or **NEXT** button at the bottom of the screen to enable the new setting.

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.



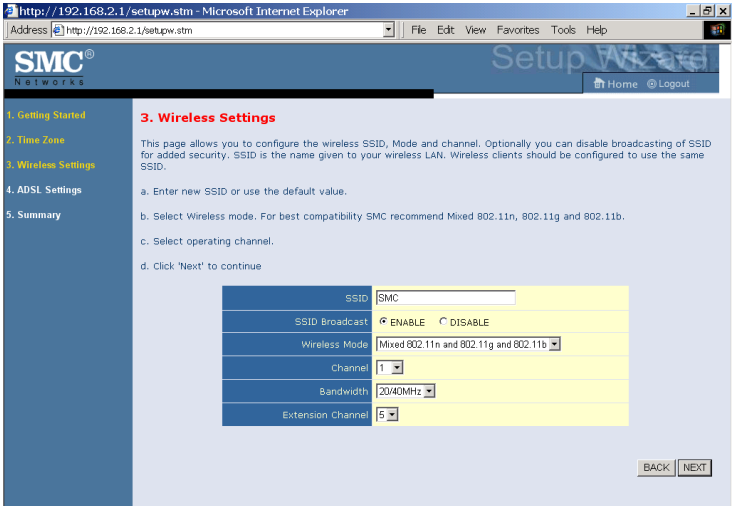
Select your local time zone from the drop down menu. This information is used for log entries and client filtering.

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.

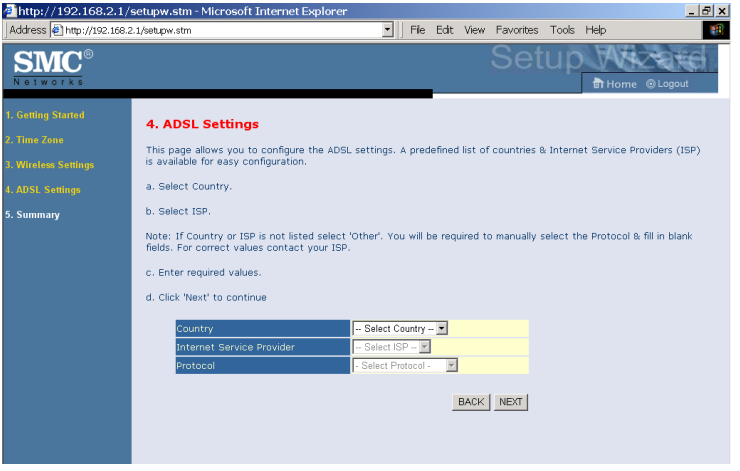
Parameter	Description
Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the router and all of its wireless clients. The router will automatically assign itself a radio channel, or you may select one manually.
Bandwidth	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.

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.

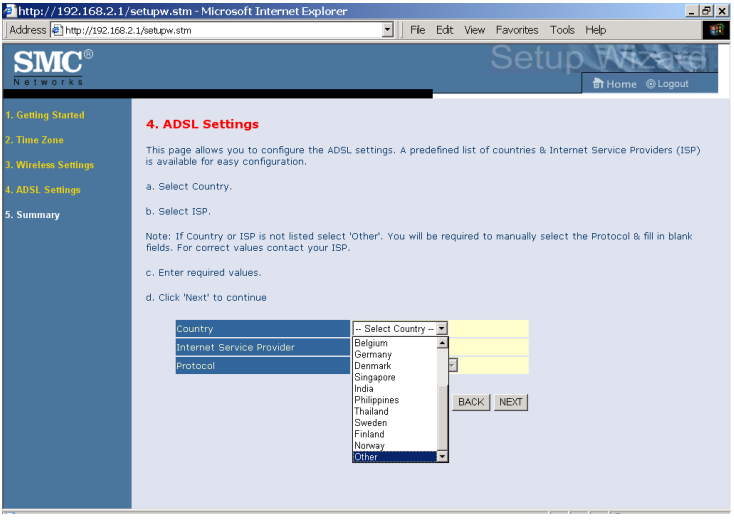
Click **NEXT** to continue.

Parameter Setting - Country or ISP Not Listed

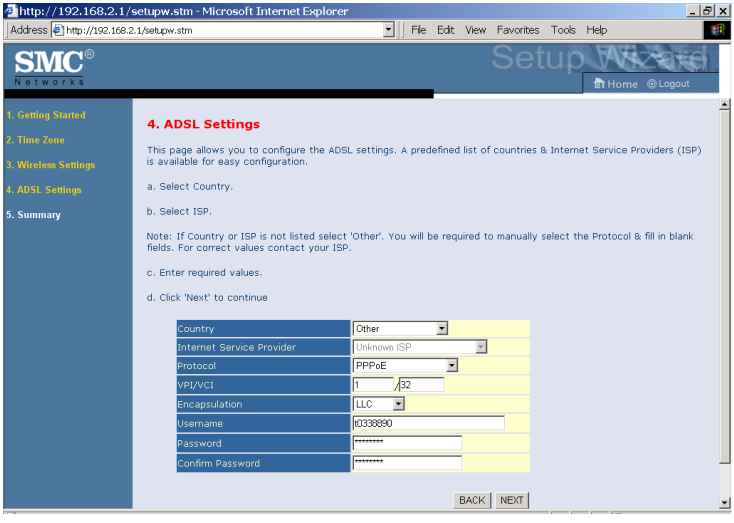
If your Country or Internet Service Provider is not listed, select **Other**. This will allow you to manually configure your ISP settings.

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

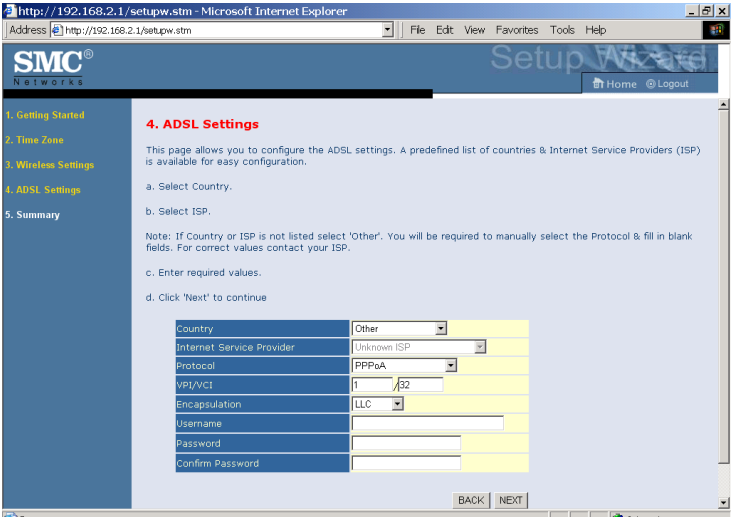


Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down menu.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.
Confirm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

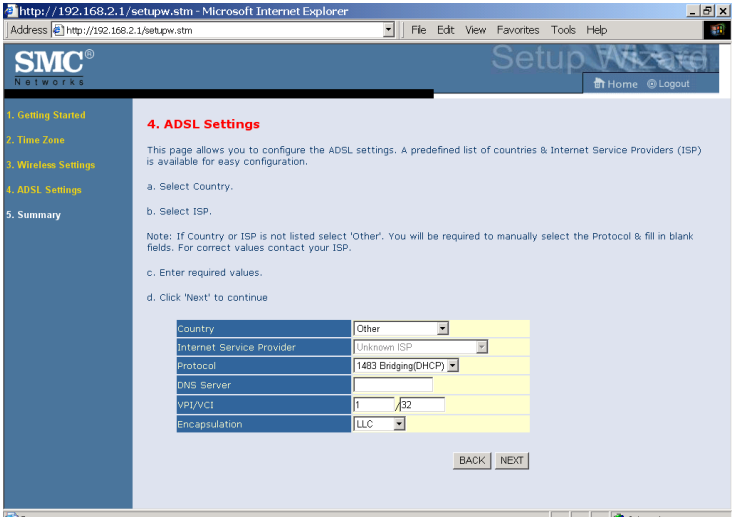


Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down list.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.
Confirm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

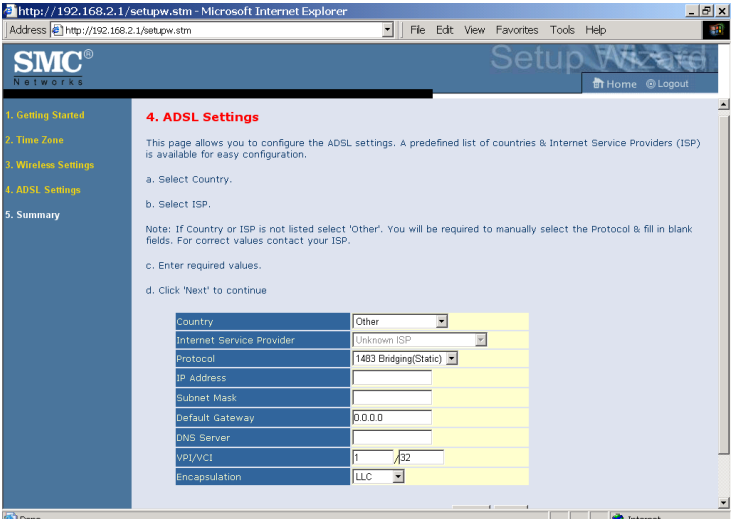


Parameter	Description
DNS Server	Enter the DNS Server IP address provided by your ISP. If your ISP has not provided you with a DNS address, leave this field blank. The Barricade will automatically obtain the DNS address from your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit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

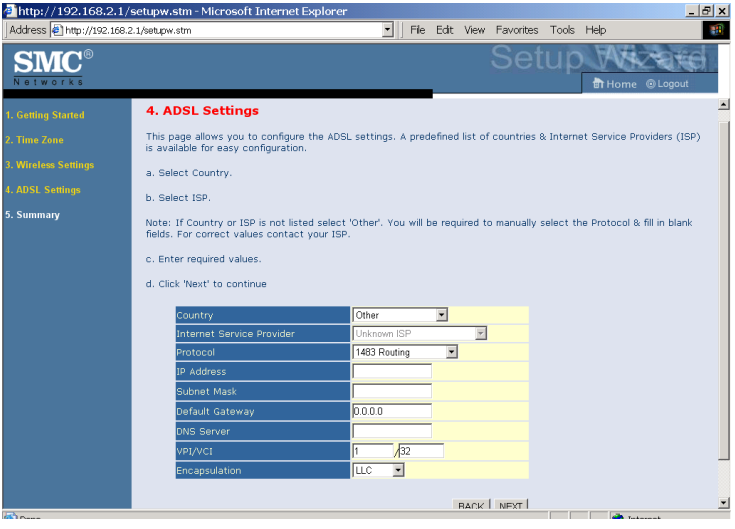


Parameter	Description
IP Address	Enter your ISP supplied static IP address here
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path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

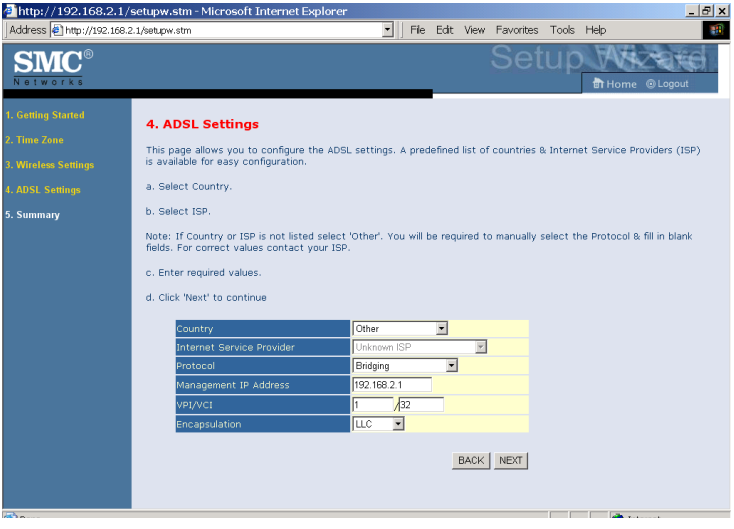


Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier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

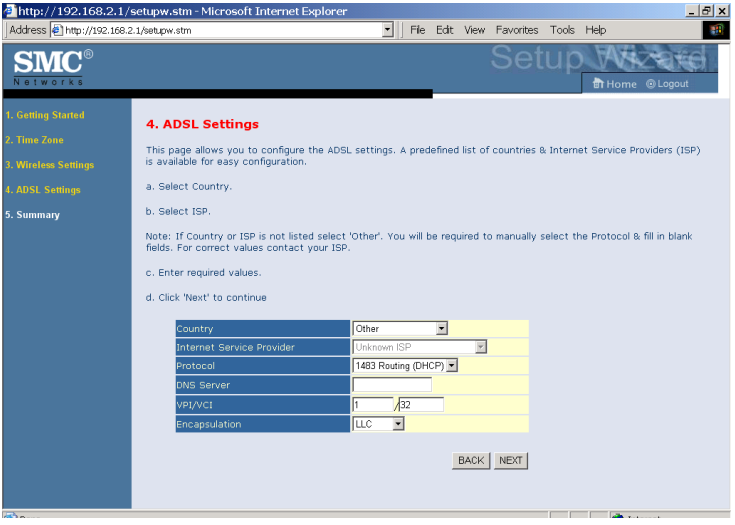


Parameter	Description
Management IP Address	Management IP address of the Barricade (Default:192.168.2.1). When configured in "Bridging" mode you will be able to manage the Barricade using this IP address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by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



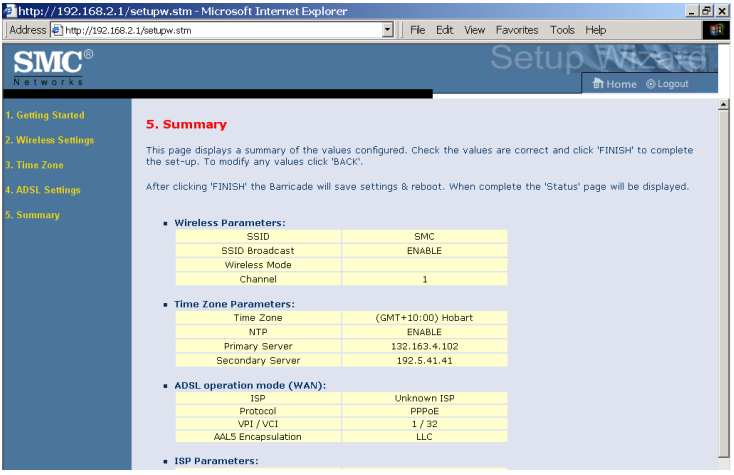
Parameter	Description
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down menu.

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 it's 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.

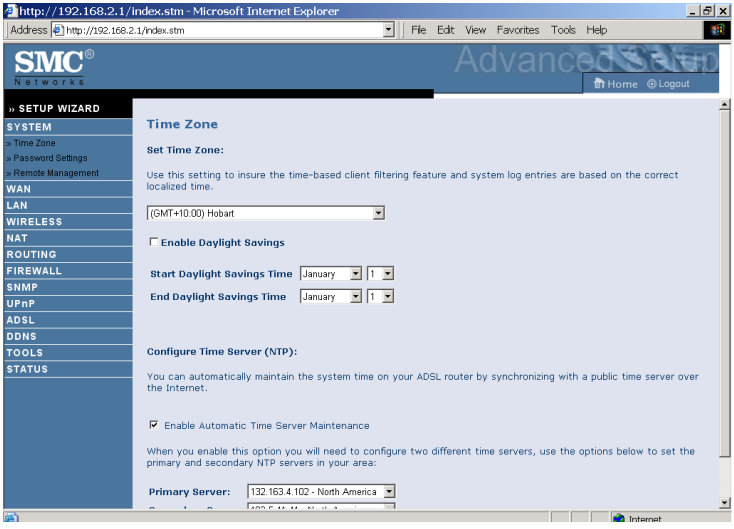
Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.
WAN	Configures the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.
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.



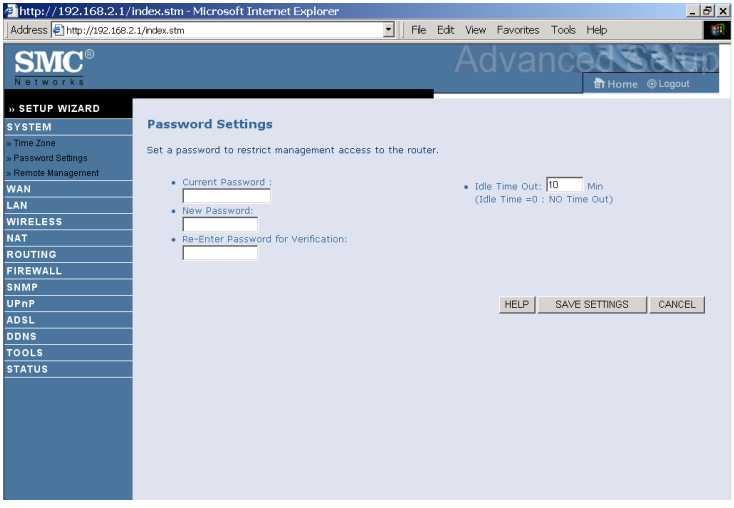
For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down menu.

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.



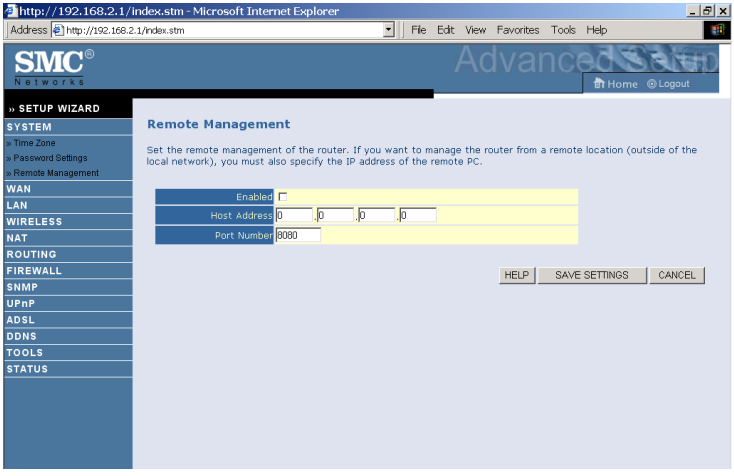
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

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)

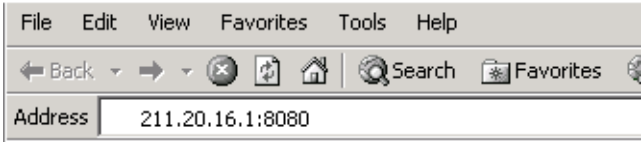
Remote Management

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.

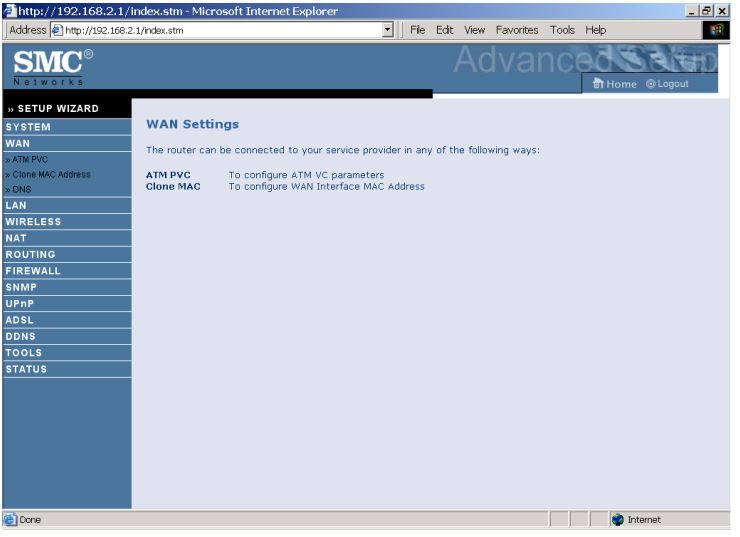


WAN

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

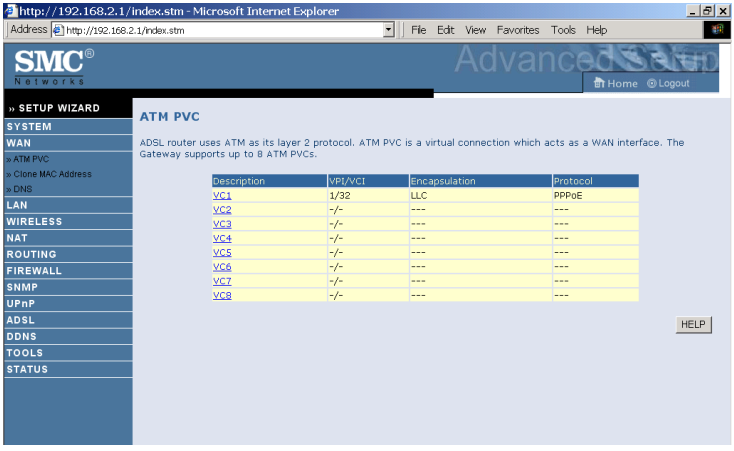
The following three items are configurable:

- 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.

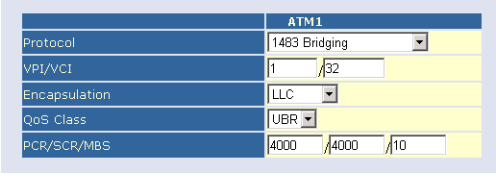


Parameter	Description
VC1 to VC8	Click on the desired VC to configure the connection parameters.
VPI/VCI	Displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for the corresponding VC.
Encapsulation	Displays the Encapsulation configured for the corresponding VC. Encapsulation specifies how to handle multiple protocols at the ATM transport layer. • 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

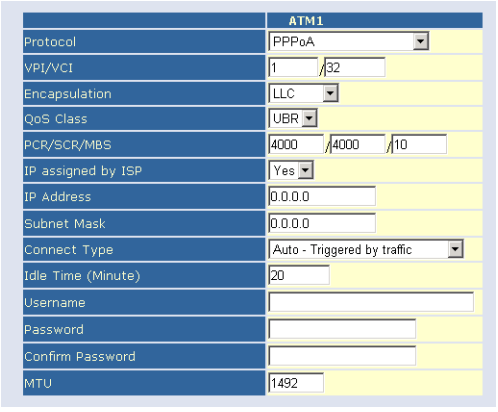
1483 Bridging

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.



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.

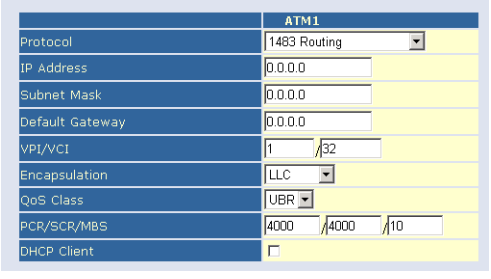
PPPoA



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.

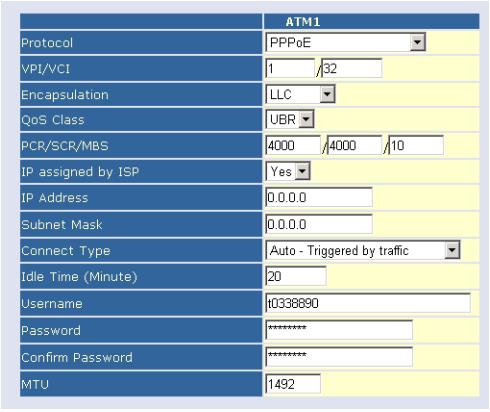
Parameter	Description
Confirm Password	Confirm password
MTU	Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP

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.
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.
QoS Class	ATM QoS classes including CBR, UBR and VBR
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
DHCP Client	Check the box if your ISP assigns an IP address dynamically.

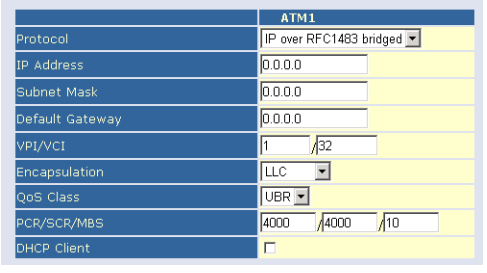
PPPoE



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.
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 your ISP assigns IP address dynamically.
IP Address	If you have selected "No" in the previous field, type in the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
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.

Parameter	Description
Confirm Password	Confirm password
MTU	Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP.

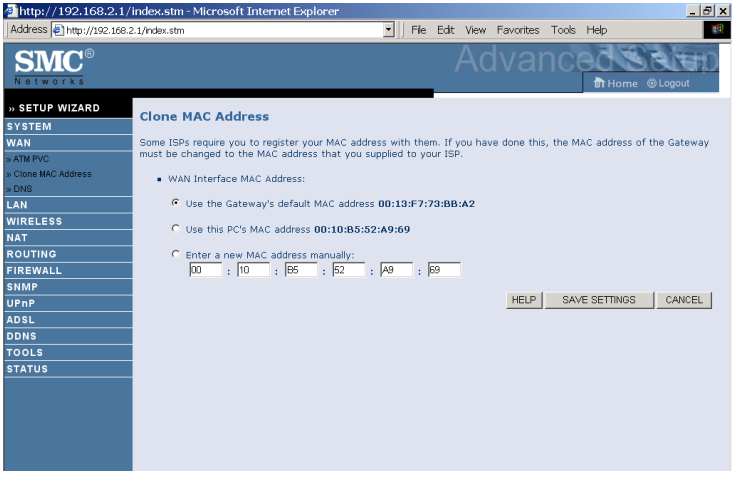
IP Over RFC1483 bridged



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.
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.
DHCP Client	Check the box if your ISP assigns an IP address dynamically.

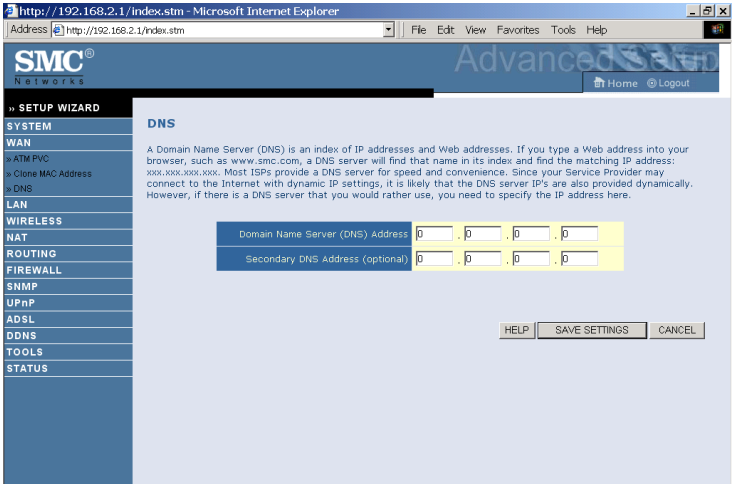
Clone MAC Address

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.



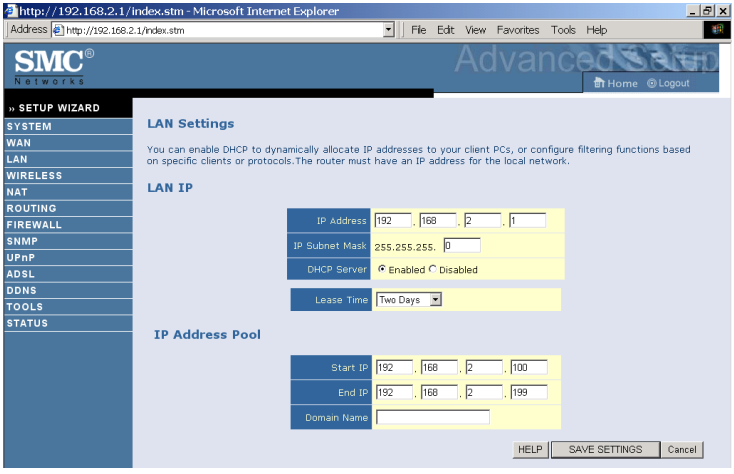
DNS

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.



LAN

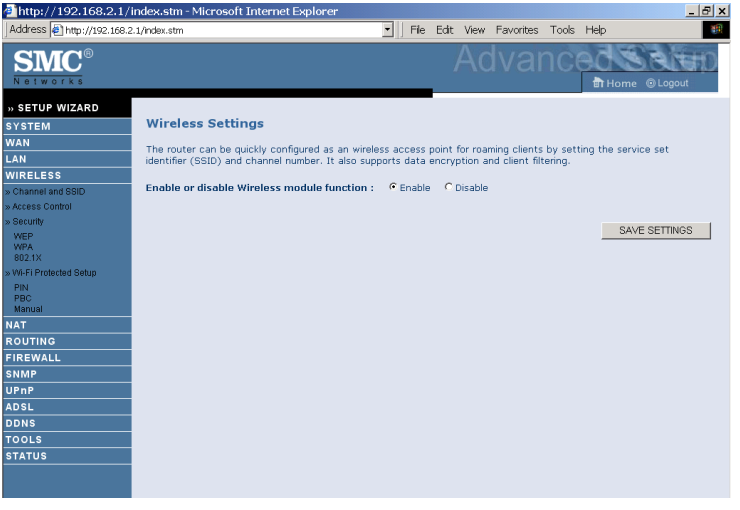
The LAN settings menu allows you to change the default IP address of the Barricade, modify the DHCP server settings.



Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	The subnet mask of the Barricade.
DHCP Server	This option allows you to enable or disable the DHCP server function. By default DHCP is enabled.
Lease Time	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.
IP Address Pool	
Start IP Address/ End IP address	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.
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.

Wireless

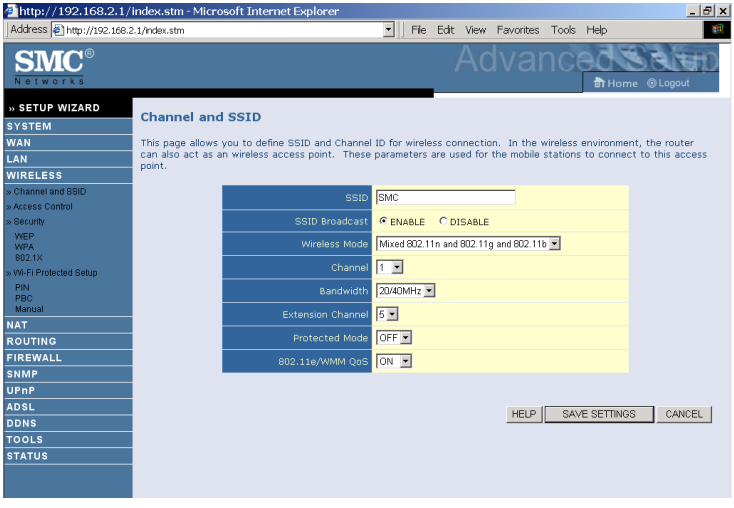
The router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the domain identifier, and the security options.



- Enable or disable Wireless module function: select to enable or disable the wireless function.

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	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. Enable this function for easy connection for the clients. Disable this function for increased security.
Wireless Mode	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.
Channel	This is the radio channel used for wireless communication.

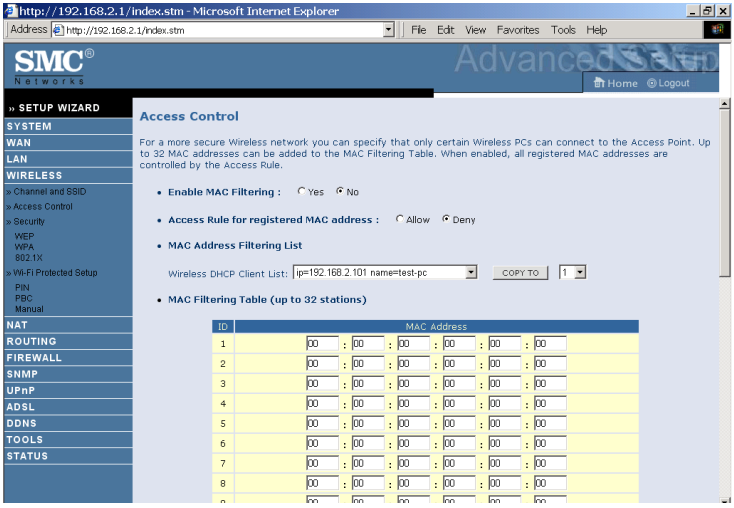
Parameter	Description
Bandwidth	Select the bandwidth: •20 MHz: Sets the operation bandwidth as 20 MHz. when 20 MHz is selected, there would be no extension channel available. •20/40 MHz: Allows automatic detection of the operation bandwidth between 20 and 40 MHz. Choosing this mode allows you to use 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.
Protected Mode	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.
802.11e/WMM QoS	Select to turn on/turn off the QoS function.

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.

Access Control

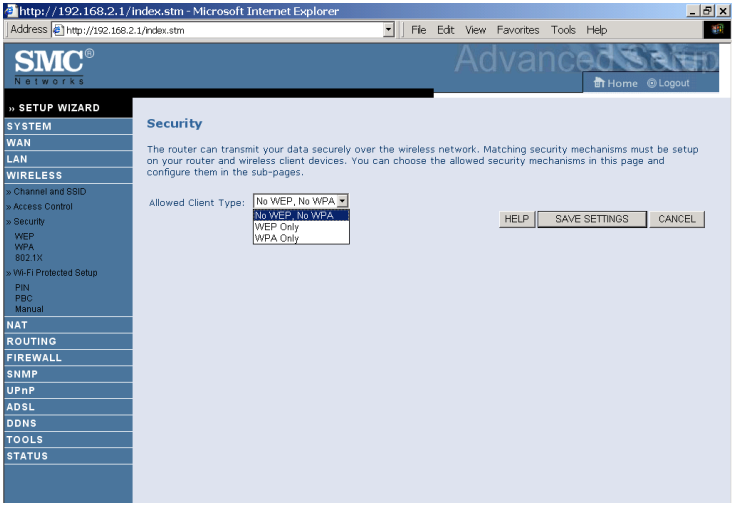
Using the Access Control functionality, you can restrict access based on MAC address. Each PC has a unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, the computers whose MAC address you have listed in the filtering table will be able to connect (or will be 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.

Security

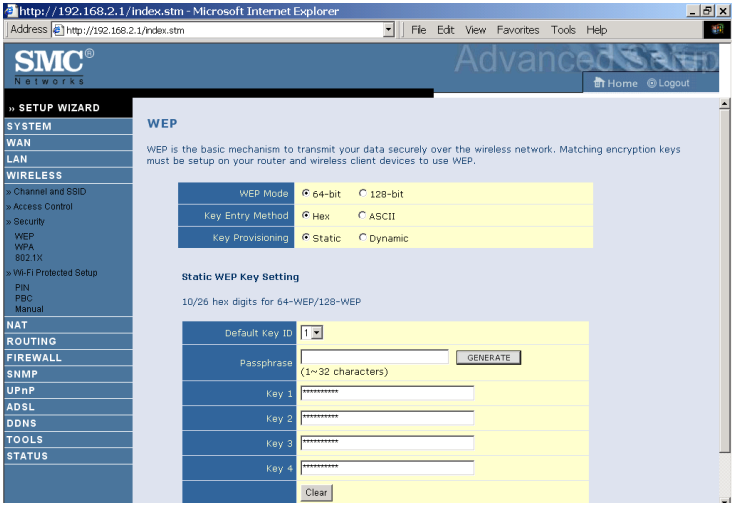
To make your wireless network safe, you should turn on the security function.



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.

WEP



Parameter	Description
WEP Mode	Select 64 bit, or 128 bit.
Key Entry Method	Select Hex, or ASCII.
Key Provisioning	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.

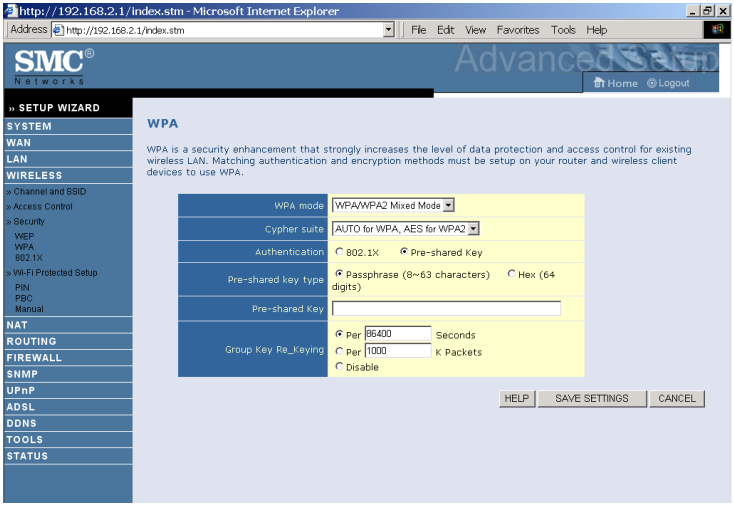
To automatically generate encryption keys using the passphrase function, when Key Entry Method is set to **Hex**, enter a string into the passphrase field, then click **Generate**. Select the **Default Key ID** from the drop-down menu and click **SAVE SETTINGS**.

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.

WPA

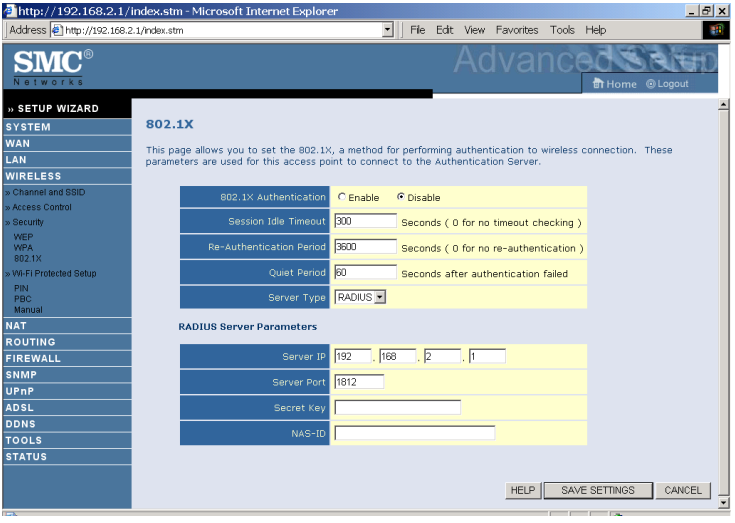
Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service. The router supports both WPA and WPA2.



Parameter	Description
WPA mode	Select WPA, WPA2 or mixed mode.
Cypher suite	Select the encryption cypher for use.
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. • Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Enter the key string here.
Group Key Re_Keying	Define the time period for re-obtain the key.

802.1X

If 802.1X is used in your network, then you should enable this function for the router.

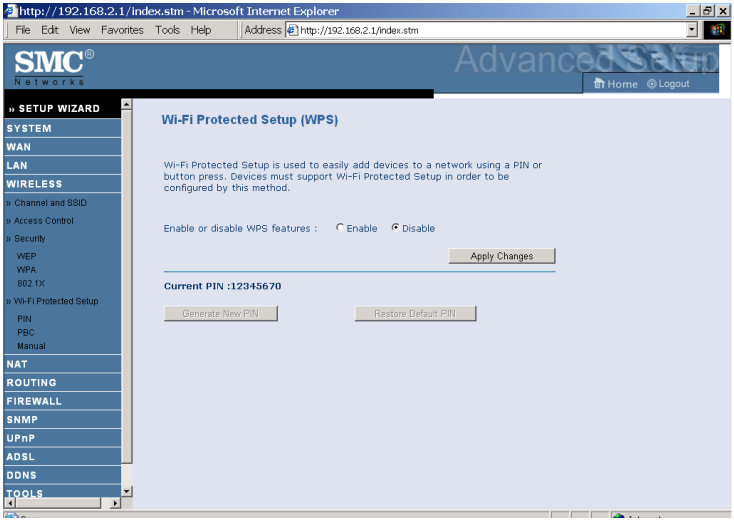


Parameter	Description
802.1X authentication	Choose to enable or disable this function.
Session Idle Timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re-Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the router will wait between failed authentications.
Server Type	Select RADIUS.
RADIUS Server Parameters	
Server IP	Enter the authentication server IP address.
Server Port	Enter the port number.

Parameter	Description
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	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).

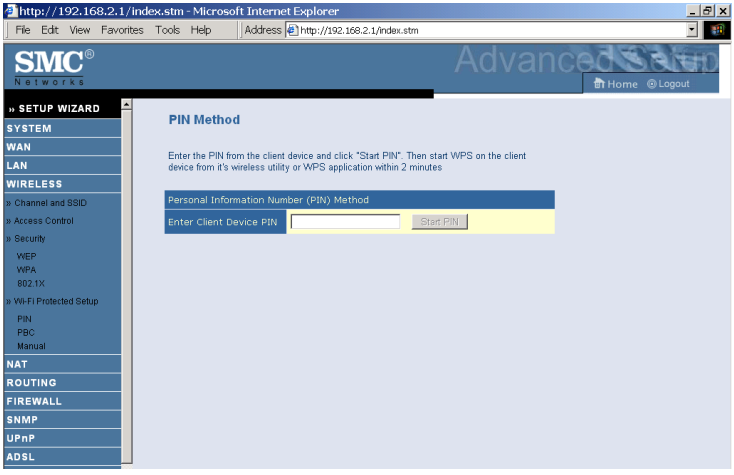


- Enable or disable WPS features: select to enable or disable.
- Generate New PIN: click this button to create a new PIN.
- Restore Default PIN: click this button to restore the PIN.

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.

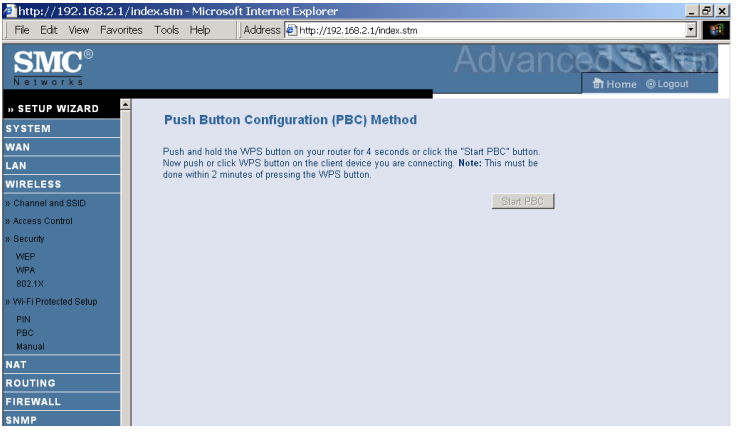


Take the following steps for easy network security settings.

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.

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

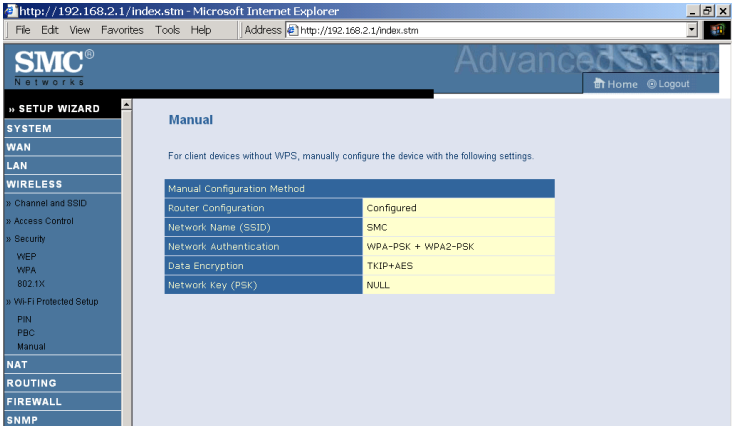
(2) click the **Start PBC** button on this screen.

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.

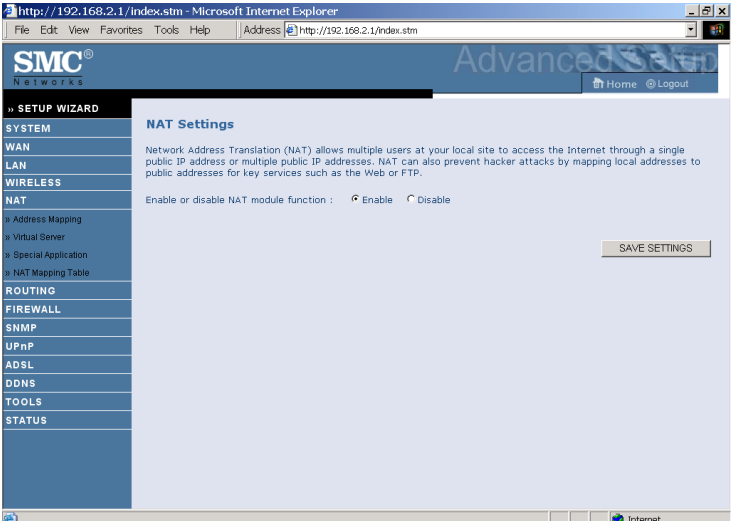
Manual

For client devices without the WPS function, you should manually configure the client device with the settings on this screen.



NAT

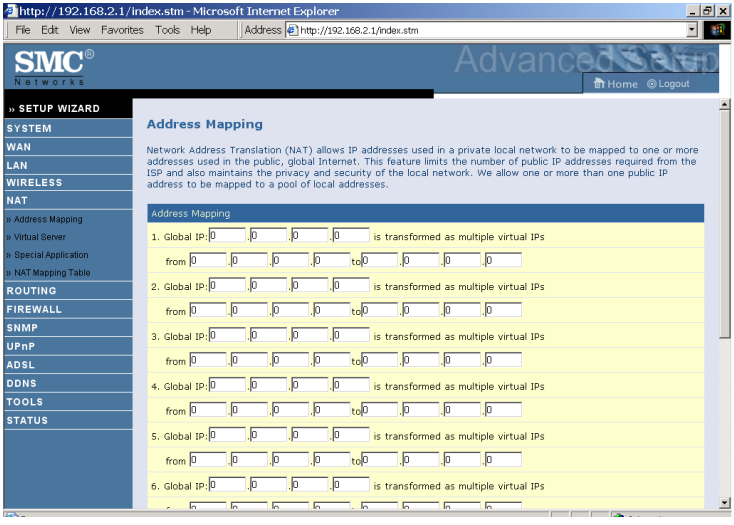
Network Address Translation (NAT) allows multiple users to access the Internet sharing one public IP.



- Enable or disable NAT module function: select to enable or disable this function.

Address Mapping

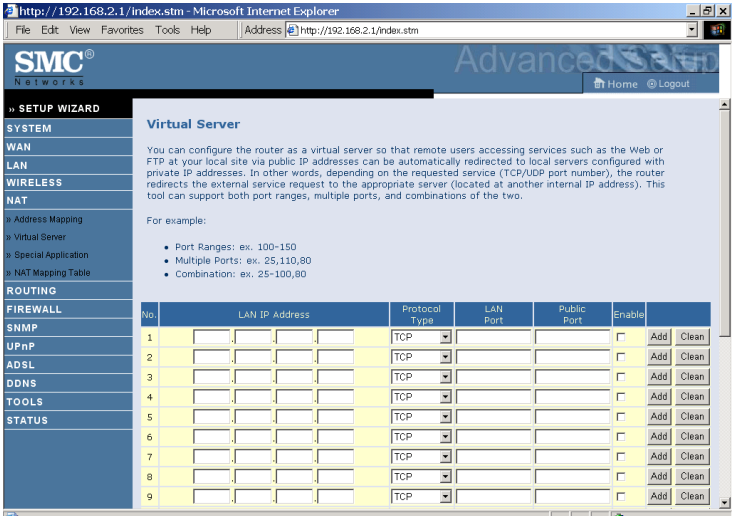
Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security.



- 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.

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).



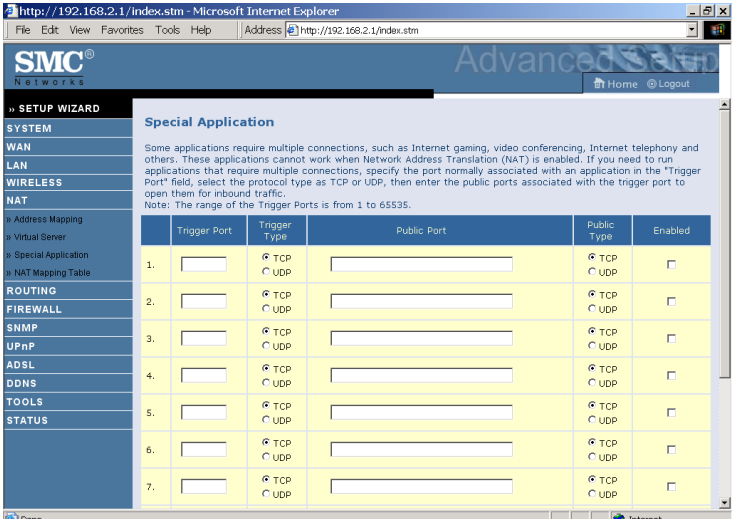
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they 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.

Special Application

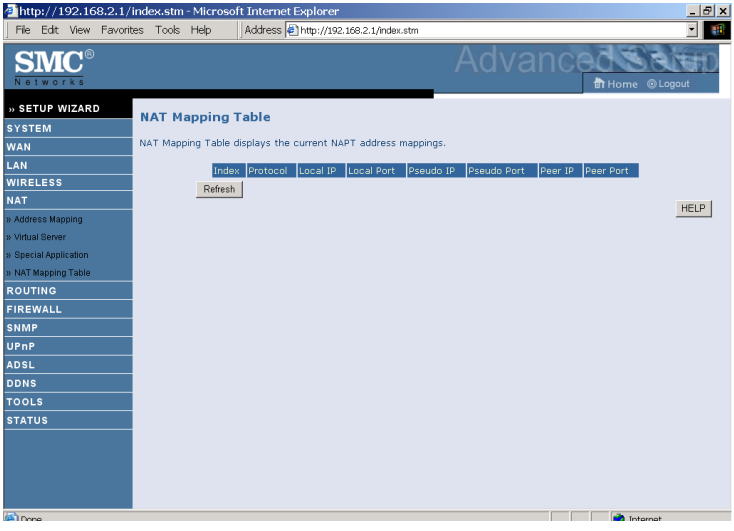
Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these screens to specify the additional public ports to be opened for each application.



- Use the Popular applications drop down menu to quickly copy the entry to the table.

NAT Mapping Table

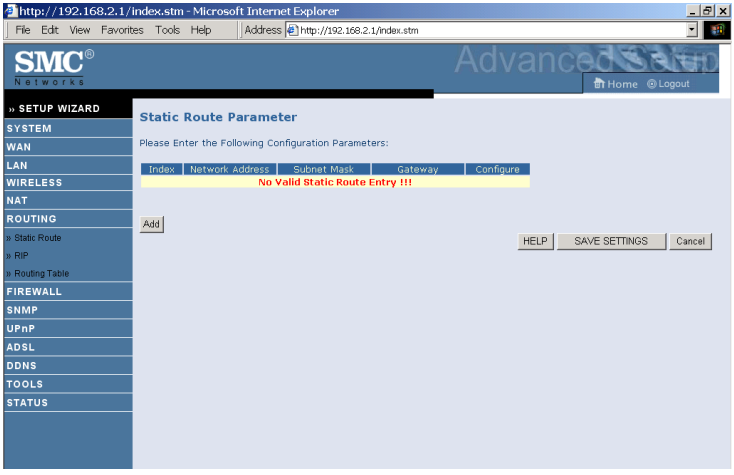
This screen displays the current NAPT (Network Address Port Translation) address mappings. Click **Refresh** to update the table.



Routing

These screens define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

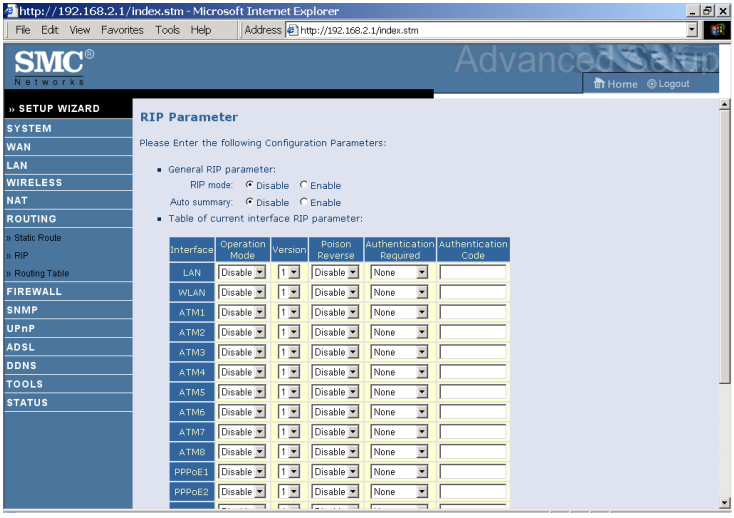
Static Route



Parameter	Description
Index	Check the box of the route you wish to delete or modify.
Network Address	Enter the IP address of the remote computer for which to set a static route.
Subnet Mask	Enter the subnet mask of the remote network for which to set a static route.
Gateway	Enter the WAN IP address of the gateway to the remote network.

Click **Add** to add a new static route to the list, or check the box of an already entered route and click **Modify**. Clicking **Delete** will remove an entry from the list.

RIP

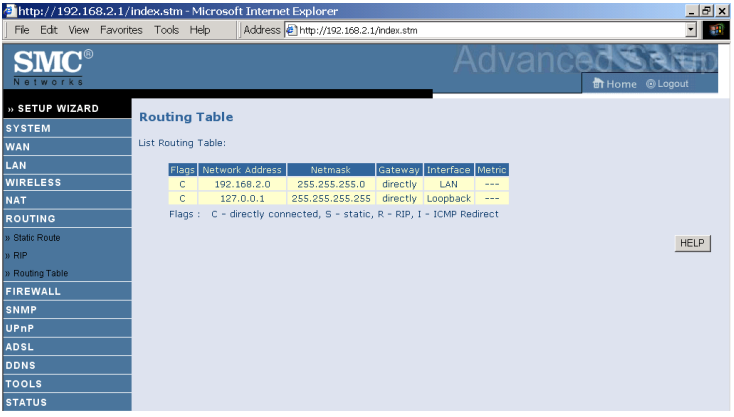


Parameter	Description
General RIP Parameters	
RIP mode	Globally enables or disables RIP.
Auto summary	If Auto summary is disabled, then RIP packets will include sub-network information from all sub-networks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all sub-networks.
Table of current Interface RIP parameter	
Interface	The WAN interface to be configured.
Operation Mode	Disable: RIP disabled on this interface. Enable: RIP enabled on this interface. Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.
Version	Sets the RIP (Routing Information Protocol) version to use on this interface.

Parameter	Description
Poison Reverse	A method for preventing loops that would cause endless retransmission of data traffic.
Authentication Required	• None: No authentication. • Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets. • MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.
Authentication Code	Password or MD5 Authentication key.

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

Routing Table



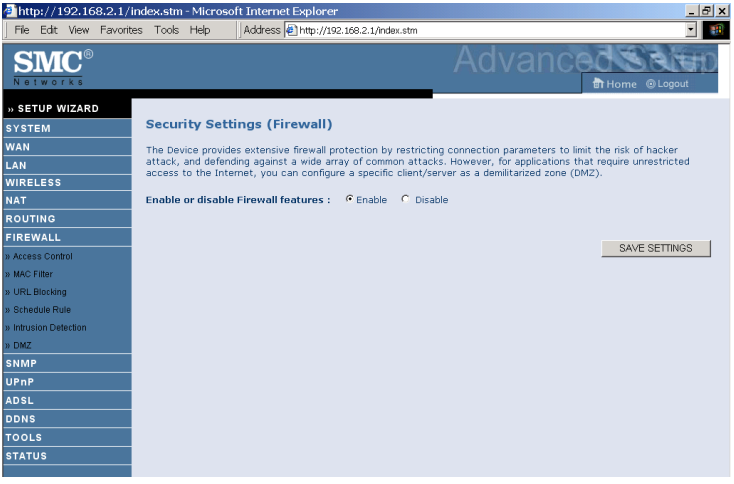
Parameter	Description
Flags	Indicates the route status: C = Direct connection on the same subnet. S = Static route. R = RIP (Routing Information Protocol) assigned route. I = ICMP (Internet Control Message Protocol) Redirect route.
Network Address	Destination IP address.
Netmask	The subnetwork associated with the destination. This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the subnet mask number; each bit that corresponds to "0" is part of the host number.
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

Firewall

The Barricade Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
(For details see page 4-60.)

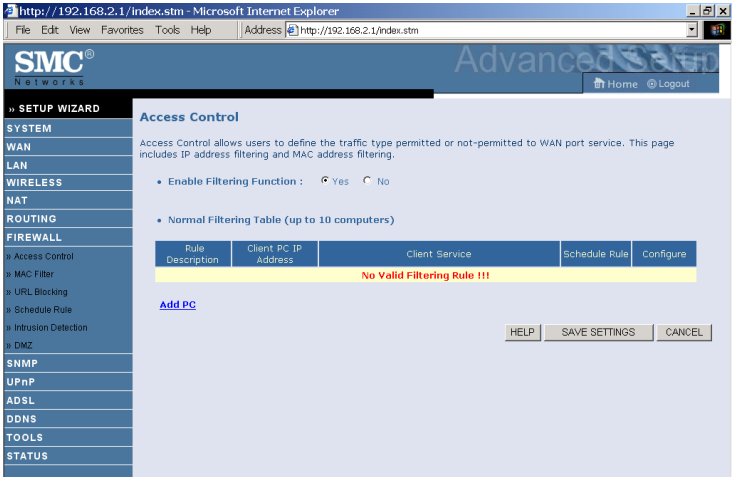


The firewall does not significantly affect system performance, so we advise enabling the function to protect your network.

Select **Enable** and click the **SAVE SETTINGS** button.

Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.



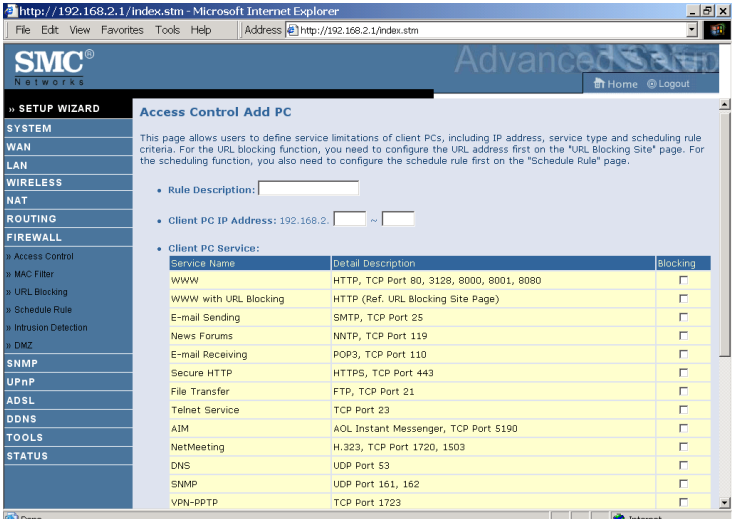
Parameter	Description
Enable Filtering Function	Enable or Disable Access control function.
Normal Filtering Table	Displays descriptive list of filtering rules defined.

To create a new access control rule:

1. Click **Add PC** on the Access Control screen. The Access Control Add PC screen will appear.

2. Define the appropriate rule settings for client PC services.

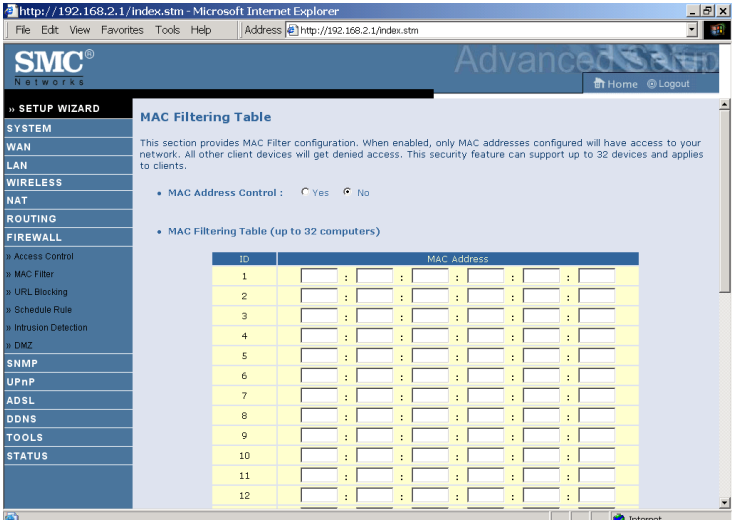
3. Click **OK** and then click **SAVE SETTINGS** to save your settings.



MAC Filter

The MAC Filter allows you to define what client PC's can access the Internet. When filtering function is enabled only the MAC addresses defined in the MAC Filtering table will have access to the Internet. All other client devices will be denied access.

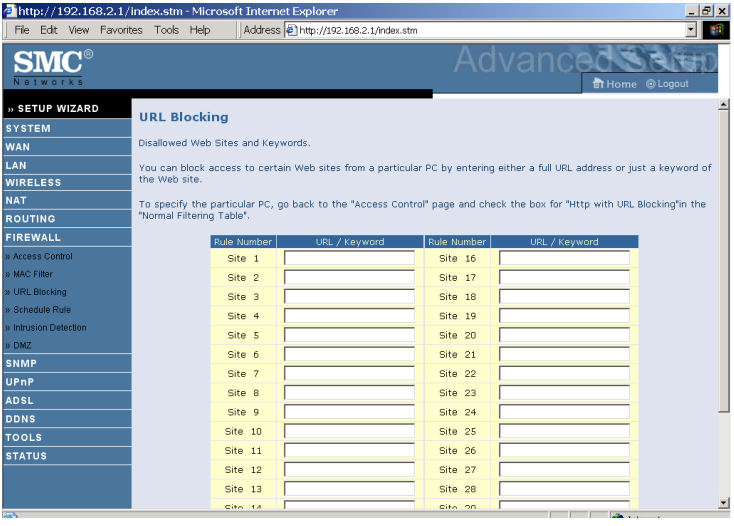
You can enter up to 32 MAC addresses in this table.



- MAC Address Control: select enable or disable.
- MAC Filtering Table: enter the MAC address in the space provided.

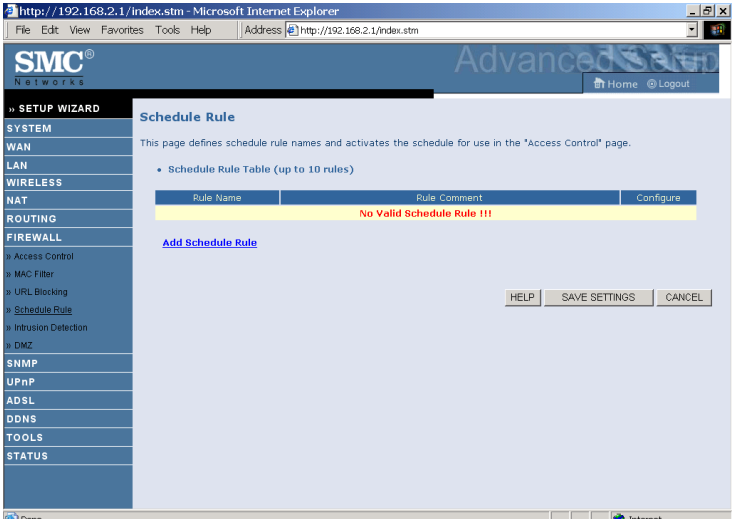
URL Blocking

The Barricade allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites. You can define up to 30 sites here.



Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule screen, and apply the rule on the Access Control screen.

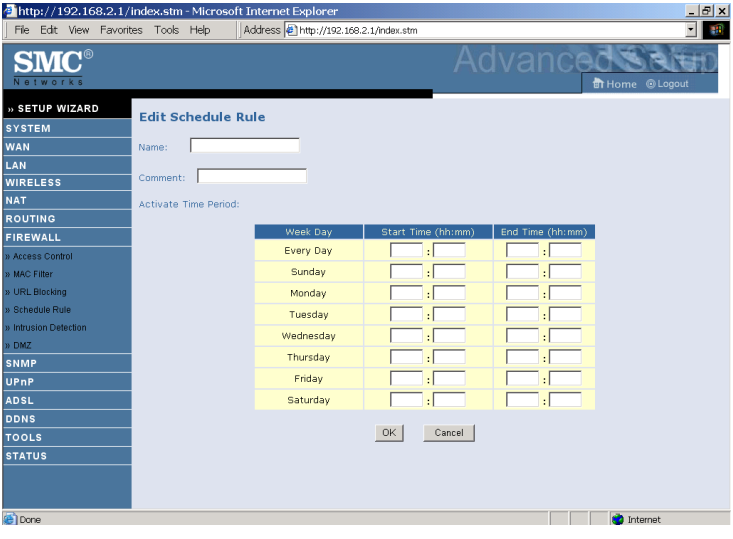


Follow these steps to add a schedule rule:

1. Click **Add Schedule Rule** on the Schedule Rule screen. The Edit Schedule Rule screen will appear.

2. Define the appropriate settings for a schedule rule.

3. Click **OK** and then click **SAVE SETTINGS** to save your settings.



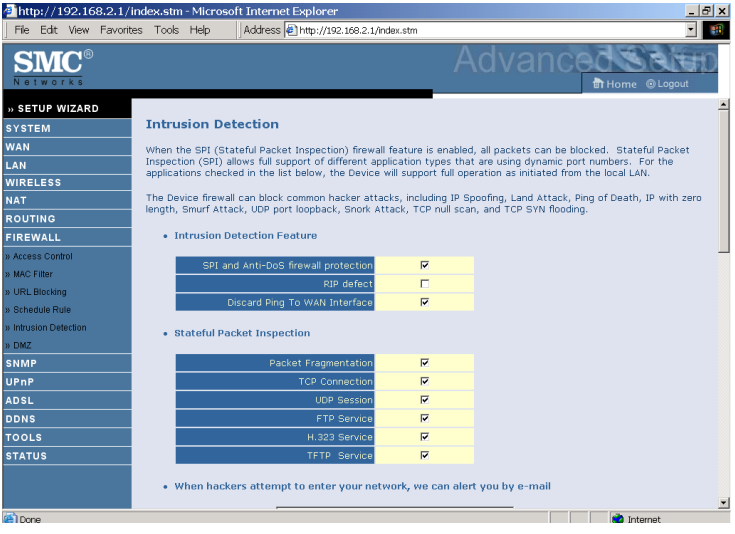
Intrusion Detection

- **Intrusion Detection Feature**

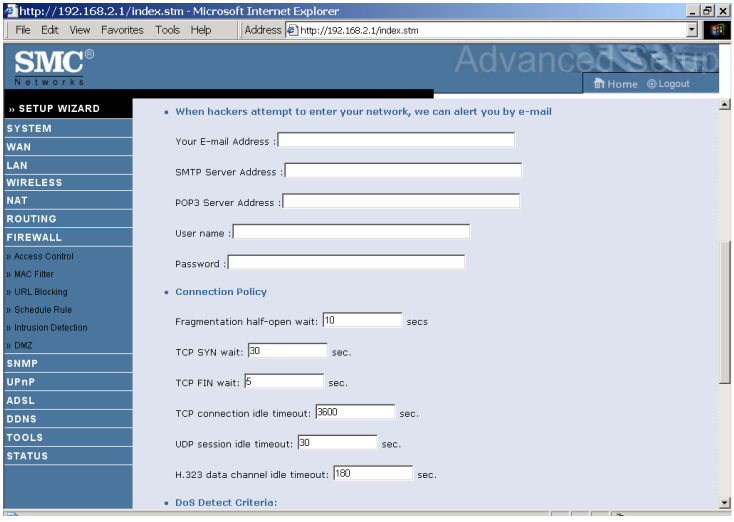
Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) — The Intrusion Detection Feature of the Barricade Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

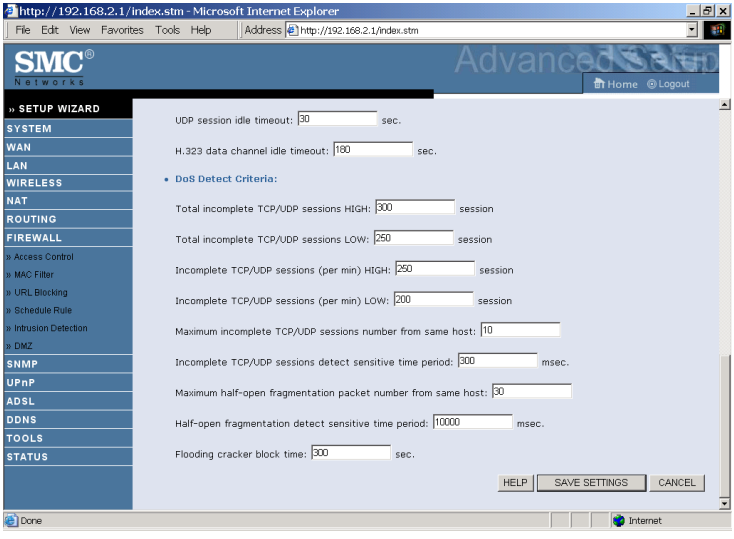
RIP Defect (Default: Enabled) — If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

Discard Ping to WAN (Default: Disabled) — Prevent a ping on the Barricade's WAN port from being routed to the network.



Scroll down to view more information.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.1/index.stm
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
UPnP
ADSL
DDNS
TOOLS
STATUS
When hackers attempt to enter your network, we can alert you by e-mail
Your E-mail Address :
SMTP Server Address :
POP3 Server Address :
User name :
Password :
Connection Policy
Fragmentation half-open wait: 10 secs
TCP SYN wait: 30 sec.
TCP FIN wait: 5 sec.
TCP connection idle timeout: 3600 sec.
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.
DoS Detect Criteria:


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.1/index.stm
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
UPnP
ADSL
DDNS
TOOLS
STATUS
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.
DoS Detect Criteria:
Total incomplete TCP/UDP sessions HIGH: 300 session
Total incomplete TCP/UDP sessions LOW: 250 session
Incomplete TCP/UDP sessions (per min) HIGH: 250 session
Incomplete TCP/UDP sessions (per min) LOW: 200 session
Maximum incomplete TCP/UDP sessions number from same host: 10
Incomplete TCP/UDP sessions detect sensitive time period: 300 msec.
Maximum half-open fragmentation packet number from same host: 30
Half-open fragmentation detect sensitive time period: 10000 msec.
Flooding cracker block time: 300 sec.
HELP
SAVE SETTINGS
CANCEL
Done
Internet

- **Stateful Packet Inspection**

This is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks "FTP Service" in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.

- **When hackers attempt to enter your network, we can alert you by e-mail**

Enter your email address. Specify your SMTP and POP3 servers, user name, and password.

- **Connection Policy**

Enter the appropriate values for TCP/UDP sessions as described in the following table.

Parameter	Defaults	Description
Fragmentation half-open wait	10 sec	Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet.
TCP SYN wait	30 sec	Defines how long the software will wait for a TCP session to synchronize before dropping the session.
TCP FIN wait	5 sec	Specifies how long a TCP session will be maintained after the firewall detects a FIN packet.
TCP connection idle timeout	3600 seconds (1 hour)	The length of time for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 sec	The length of time for which a UDP session will be managed if there is no activity.
H.323 data channel idle timeout	180 sec	The length of time for which an H.323 session will be managed if there is no activity.

- **DoS Criteria and Port Scan Criteria**

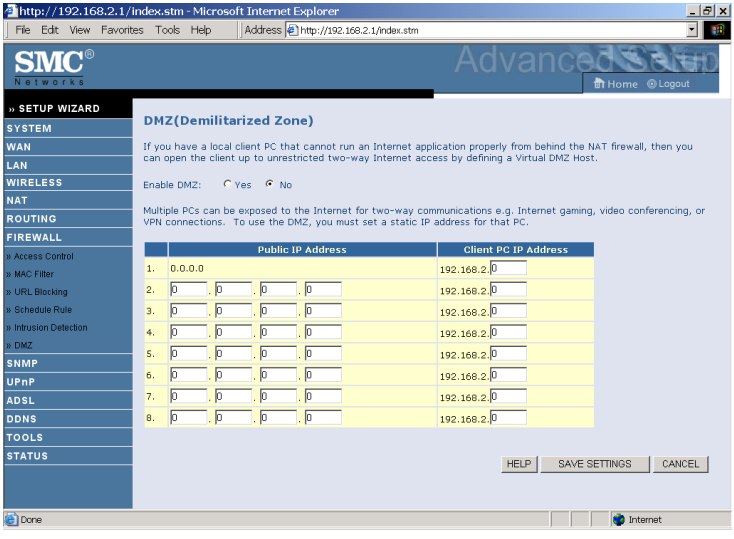
Set up DoS and port scan criteria in the spaces provided (as shown below).

Parameter	Defaults	Description
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of new unestablished sessions that will cause the software to *start* deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to *stop* deleting half-open sessions.
Incomplete TCP/UDP sessions (per min) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute.
Maximum incomplete TCP/UDP sessions number from same host	10	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	10000 msec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 second	Length of time from detecting a flood attack to blocking the attack.

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

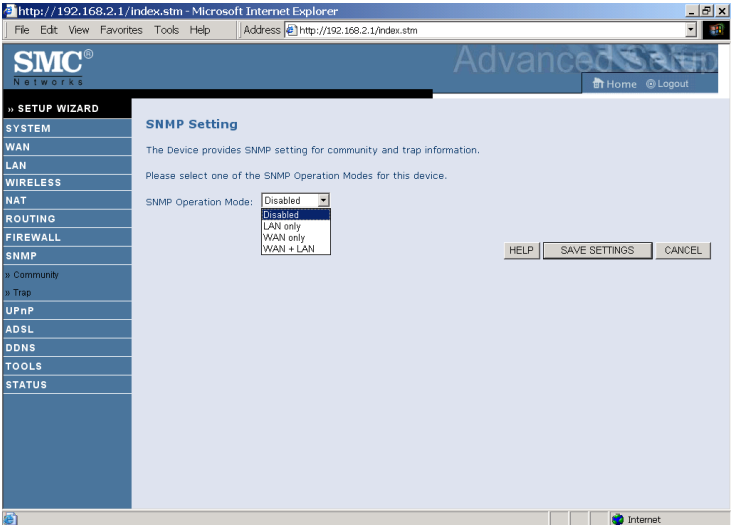
DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.



SNMP

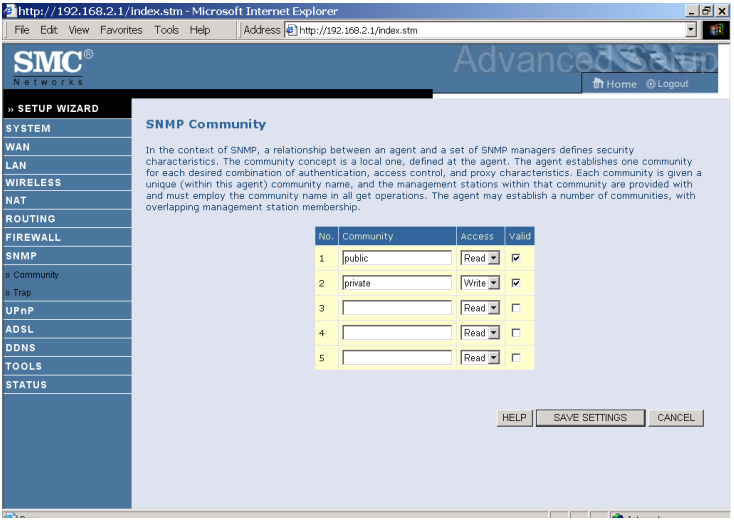
Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP).



- Select the SNMP Operation mode from the drop down menu.

Community

A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication.

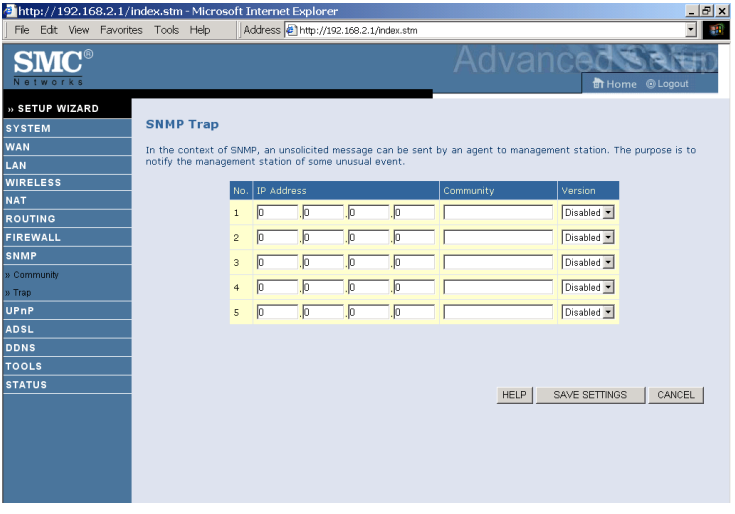


Parameter	Description
Community	A community name authorized for management access.
Access	Management access is restricted to Read Only (Read) or Read/Write (Write).
Valid	Enables/disables the entry.

Note: Up to five community names may be entered.

Trap

Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver.

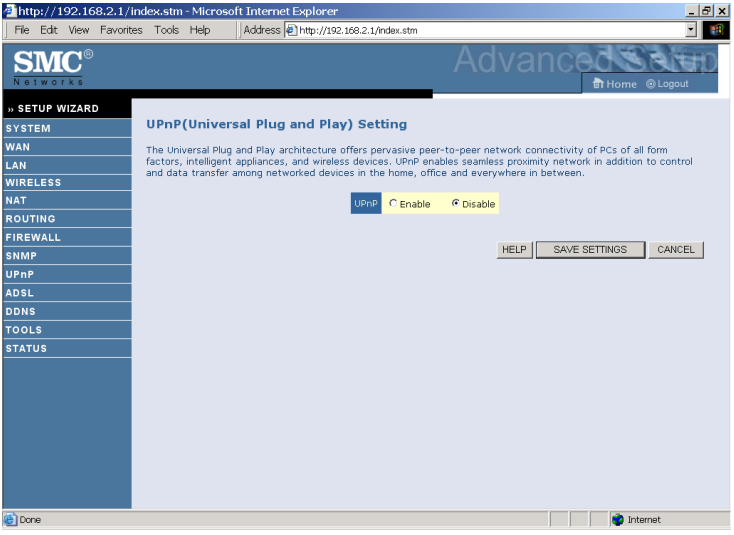


Parameter	Description
IP Address	Traps are sent to this address when errors or specific events occur on the network.
Community	A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information on your system.
Version	Sets the trap status to disabled, or enabled with V1 or V2c. The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station.

UPnP

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.

UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the office, home and everywhere within your network.



UPnP allows the device to automatically:

- join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices.

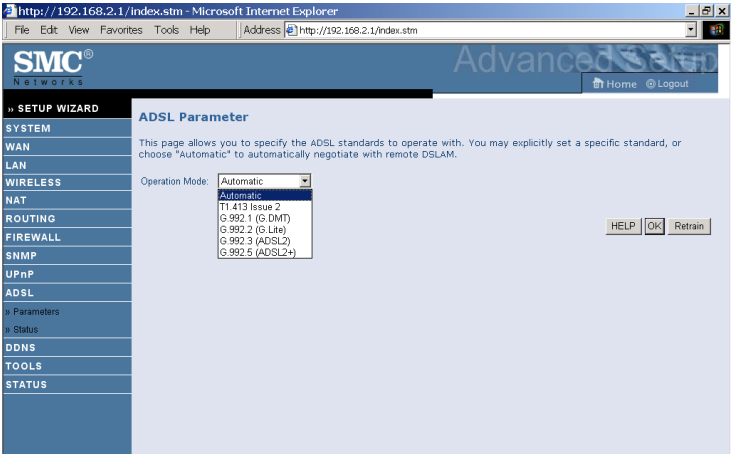
Check **Enable** to activate this function.

ADSL

ADSL (Asymmetric Digital Subscriber Line) is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. This section is used to configure the ADSL operation type and shows the ADSL status.

ADSL Parameters

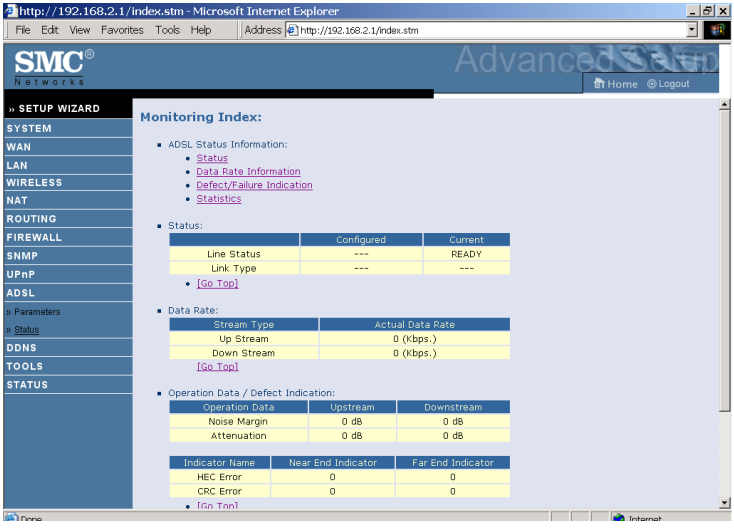
This screen is designed for the engineer to test the ADSL loop condition. Therefore, it is advised that users should not change the settings here at all.



Parameter	Description
Operation Mode	• Automatic • T1.413 Issue 2 • G.992.1 (G.DMT) • G.992.2 (G.Lite) • G.992.3 ADSl2 • G.992.5 ADSL2+

ADSL Status

The Status screen displays information on connection line status, data rate, operation data and defect indication, and statistics.

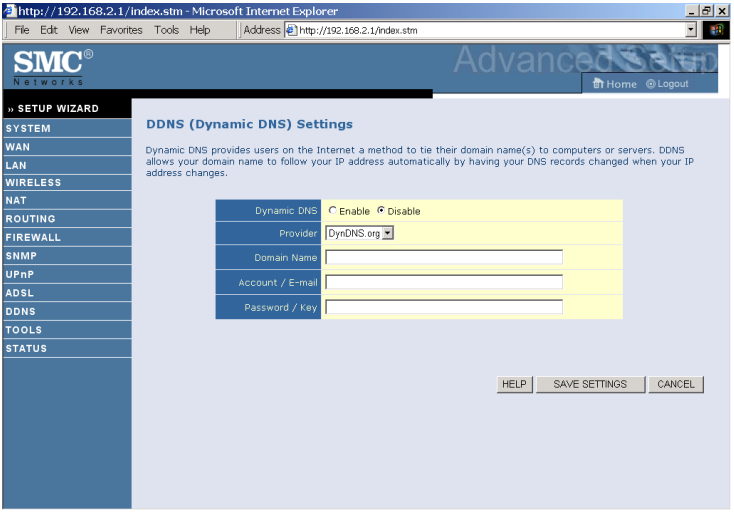


Parameter	Description
Status	
Line Status	Shows the current status of the ADSL line connection.
Data Rate	
Upstream	Maximum upstream data rate.
Downstream	Maximum downstream data rate.
Operation Data/Defect Indication	
Noise Margin	Maximum upstream and downstream noise margin.
Output Power	Maximum fluctuation in the output power.
Attenuation	Maximum reduction in the strength of the upstream and downstream signal.

Parameter	Description
Fast Path FEC Correction	There are two latency paths that may be used: fast and interleaved. For either path, a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC.
Interleaved Path FEC Correction	An interleaver is basically a buffer used to introduce a delay, allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real-time signals such as video transmission.
Fast Path CRC Error	The number of Fast Path Cyclic Redundancy Check errors.
Interleaved Path CRC Error	The number of Interleaved Path Cyclic Redundancy Check errors.
Loss of Signal Defect	Momentary signal discontinuities.
Loss of Frame Defect	Failures due to loss of frames.
Loss of Power Defect	Failures due to loss of power.
Fast Path HEC Error	Fast Path Header Error Concealment errors.
Interleaved Path HEC Error	Interleaved Path Header Error Concealment errors.
Statistics	
Received Cells	Number of cells received.
Transmitted Cells	Number of cells transmitted.

DDNS

Dynamic Domain Name Service (DDNS) provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes. This DNS feature is powered by DynDNS.org or NO-IP.com or TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

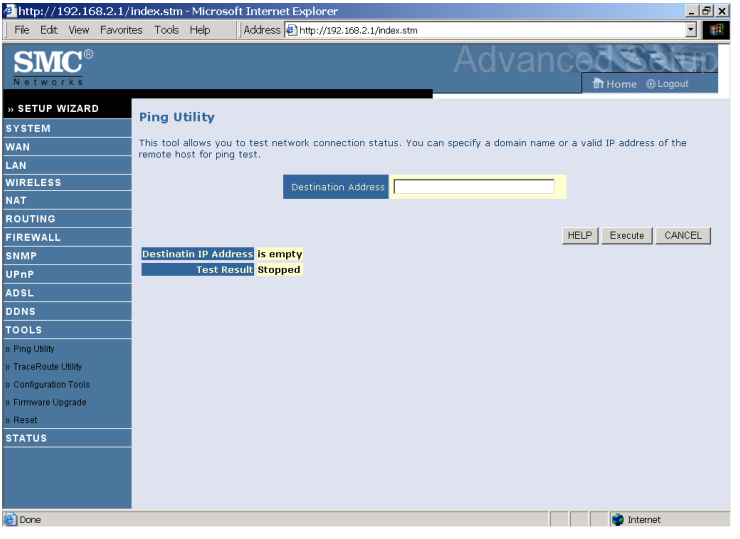


Tools

Use the Tools menu to ping, trace route, backup the current configuration, restore a previously saved configuration, update firmware, and reset the Barricade.

Ping Utility

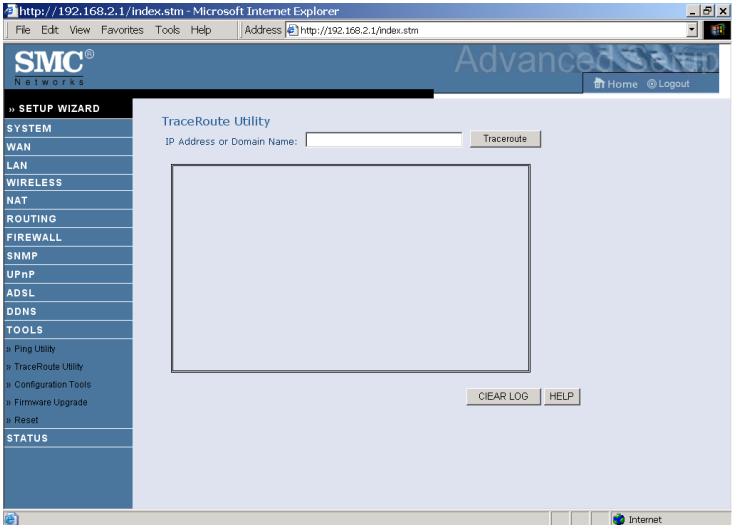
This tool allows you to test your network connection. You can specify a domain name or a valid IP address of the remote host for ping test.



- Enter the address in the Destination address field, then click **Execute**. The result will show in the Test Result area.

Trace Route Utility

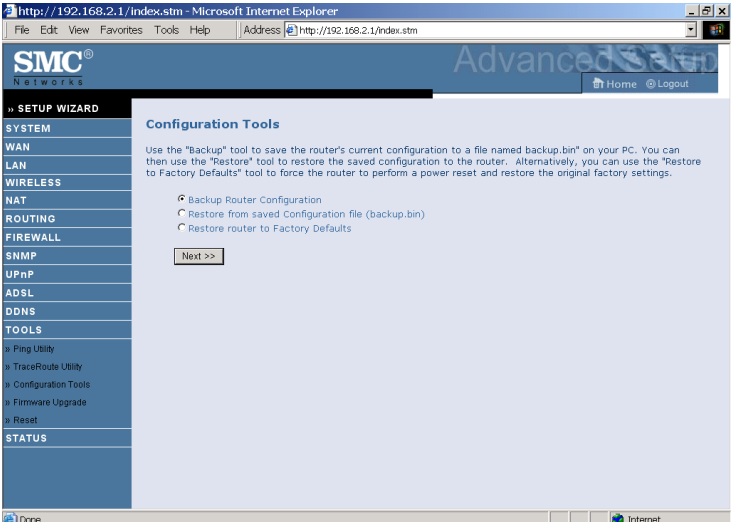
Traceroute is a TCP/IP utility which allows the user to determine the route packets take to reach a particular host.



- Enter the information in the IP Address or Domain Name field, and click the **Traceroute** button.

Configuration Tools

Choose a function and click **Next**.



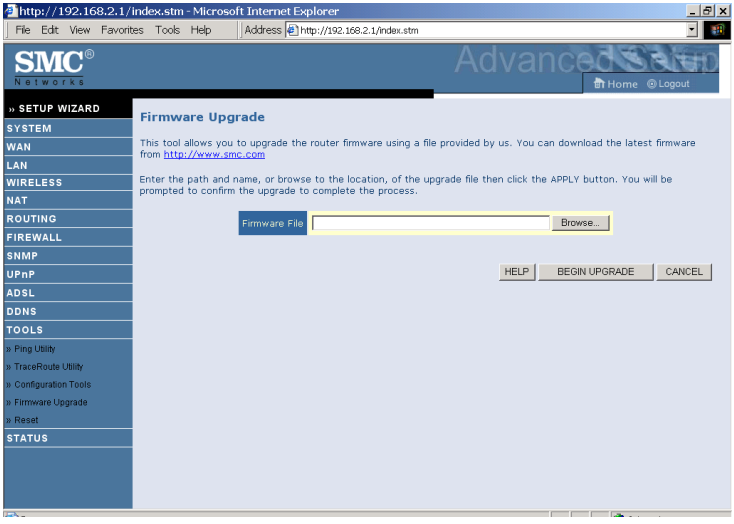
- Backup Router Configuration: this allows you to save the Barricade's configuration to a file.
- Restore from saved Configuration file: this function is used to restore the previously saved backup configuration file.
- Restore router to Factory Defaults: this resets the Barricade back to the original default settings.

Firmware Upgrade

Use this screen to update the firmware or user interface to the latest versions.

1. Download the upgrade file from the SMC web site first, and save it to your hard drive.

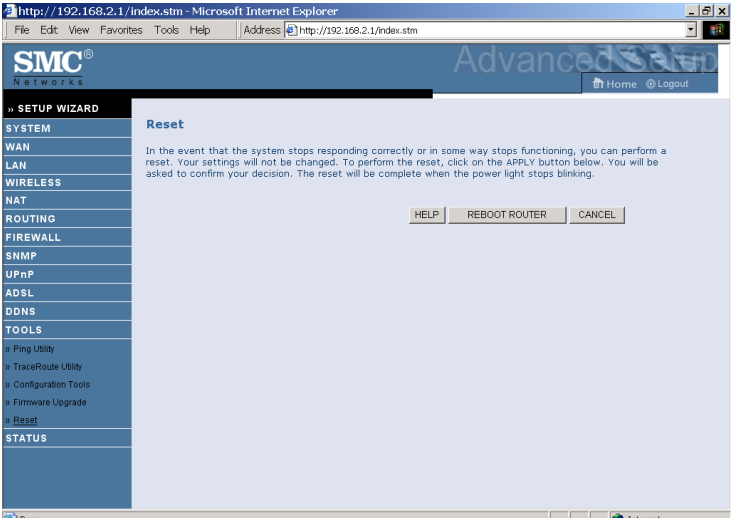
2. Then click **Browse...** to look for the downloaded file. Click **BEGIN UPGRADE**.



Check the Status screen Information section to confirm that the upgrade process was successful.

Reset

Click **REBOOT ROUTER** to reset the Barricade. The reset will be complete when the power LED stops blinking.



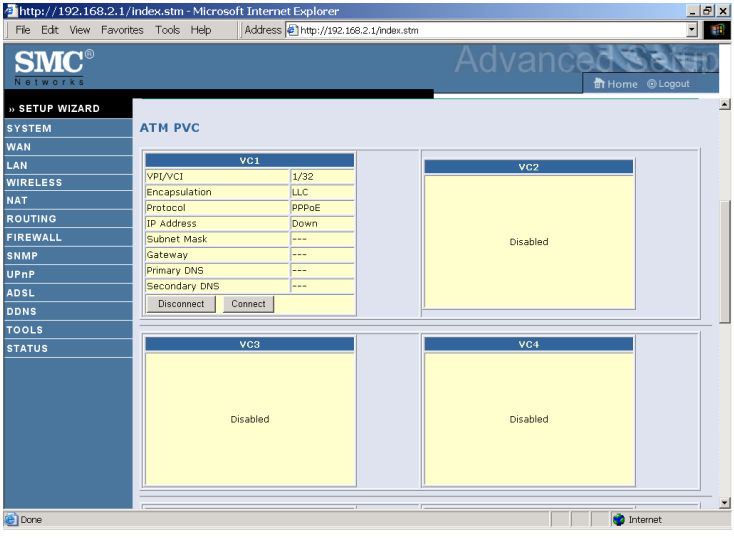
If you perform a reset from this screen, the configurations will not be changed back to the factory default settings.

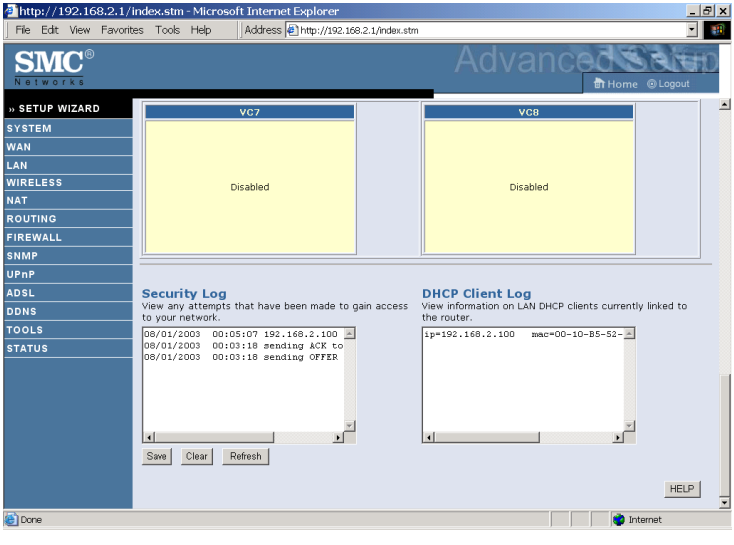
Note: If you use the Reset button on the back panel, the Barricade performs a power reset. If the button is pressed for over 10 seconds, all the LEDs will illuminate and the factory default settings will be restored.

Status

The Status screen displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking **Save** and choosing a location.

Scroll down to view more information on the Status screen.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.1/index.stm
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
SNMP
UPnP
ADSL
DDNS
TOOLS
STATUS
ATM PVC
VC1
VPI/VCI 1/32
Encapsulation LLC
Protocol PPPoE
IP Address Down
Subnet Mask ---
Gateway ---
Primary DNS ---
Secondary DNS ---
Disconnect
Connect
VC2
Disabled
VC3
Disabled
VC4
Disabled
Done
Internet


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.2.1/index.stm
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
SNMP
UPnP
ADSL
DDNS
TOOLS
STATUS
VC7
Disabled
VC8
Disabled
Security Log
View any attempts that have been made to gain access to your network.
08/01/2003 00:05:07 192.168.2.100
08/01/2003 00:03:18 sending ACK to
08/01/2003 00:03:18 sending OFFER
DHCP Client Log
View information on LAN DHCP clients currently linked to the router.
ip=192.168.2.100 mac=00-10-B5-52-
Save
Clear
Refresh
HELP
Done
Internet

The following items are included on the Status screen:

Parameter	Description
INTERNET	Displays WAN connection type and status.
Release	Click on this button to disconnect from the WAN.
Renew	Click on this button to establish a connection to the WAN.
GATEWAY	Displays system IP settings, as well as DHCP Server and Firewall status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface and for the Barricade, as well as the hardware version and serial number.
ATM PVC	Displays ATM connection type and status.
Disabled	The ATM connection is disabled.
Connect	Click on this button to establish a connection to the ATM connection.
Security Log	Displays attempts to access your network.
Save	Click on this button to save the security log file.
Clear	Click on this button to delete the access log.
Refresh	Click on this button to refresh the screen.
DHCP Client Log	Displays information on DHCP clients on your network.

Finding the MAC address of a Network Card

Windows 2000/XP

Click Start/Programs/Command Prompt. Type "ipconfig /all" and press "ENTER".

The MAC address is listed as the "Physical Address."

Macintosh

Click System Preferences/Network.

The MAC address is listed as the "Ethernet Address" on the TCP/IP tab.

Linux

Run the command "/sbin/ifconfig."

The MAC address is the value after the word "HWaddr."

APPENDIX A
TROUBLESHOOTING

This section describes common problems you may encounter and possible solutions to them. The Barricade can be easily monitored through panel indicators to identify problems.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Power LED is Off	• Check connections between the Barricade, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Link LED is Off	• Verify that the Barricade and attached device are powered on. • Be sure the cable is plugged into both the Barricade and the corresponding device. • Verify that the proper cable type is used and that its length does not exceed the specified limits. • Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.
Network Connection Problems	
Cannot ping the Barricade from the attached LAN	• Verify that the IP addresses are properly configured. For most applications, you should use the Barricade's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Barricade and any attached LAN devices. • Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.

Troubleshooting Chart	
Symptom	**Action**
Management Problems	
Cannot connect using the web browser	• Be sure to have configured the Barricade with a valid IP address, subnet mask, and default gateway. • Check that you have a valid network connection to the Barricade and that the port you are using has not been disabled. • Check the network cabling between the management station and the Barricade.
Forgot or lost the password	• Press the Reset button on the rear panel (holding it down for at least 10 seconds) to restore the factory defaults.

Troubleshooting Chart	
Symptom	**Action**
Wireless Problems	
WEP encryption not working when using Windows Zero Configuration (WZC) service	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. This is caused by a conflict with beacon packet element ID 221 used by the WPS protocol and Windows Zero Configuration (WZC) service. There are four different ways you can easily solve this problem. Take any one of the following actions: 1. Update WZC. Please visit Microsoft download center for upgrading the WZC: Wireless LAN API (KB918997) at http://www.microsoft.com/downloads/details.aspx?FamilyID=52a43bab-dc4e-413f-ac71-158efd1ada50&DisplayLang=en 2. Disable WPS. Check **Disabled** and click **Apply Changes** on Wi-Fi Protected Setup (WPS) screen. See "WPS (Wi-Fi Protected Setup)" on page 4-40 for details. 3. Use WPA/WPA2-PSK. See "WPA" on page 4-38 for configuring WPA/WPA2-PSK security. 4. Manually configure profile using WZC. Disable the security authentication manually. - Click on **Wireless Network Connection/change advanced settings** of the client PC. - Click on the **Wireless Networks**, choose the appropriate wireless network name, and click **Properties**. - Click **Authentication** and uncheck the Enable IEEE 802.1X authentication for this network. - Click **OK** to finish configuration.

APPENDIX B
CABLES

Ethernet Cable

Caution: DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

Specifications

Cable Types and Specifications			
Cable	**Type**	**Max. Length**	**Connector**
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

Wiring Conventions

For Ethernet connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-45 connectors in a specific orientation. The following figure illustrates how the pins on an Ethernet RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

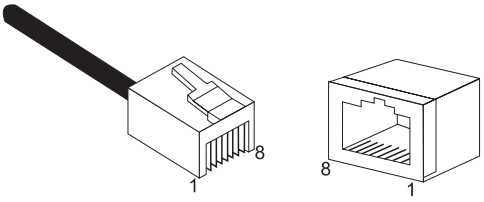


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Connection

Use the straight-through CAT-5 Ethernet cable provided in the package to connect the Barricade to your PC. When connecting to other network devices such as an Ethernet switch, use the cable type shown in the following table.

Attached Device Port Type	Connecting Cable Type
MDI-X	Straight-through
MDI	Crossover

Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

RJ-45 Pin Assignments	
Pin Number	Assignment[1]
1	Tx+
2	Tx-
3	Rx+
6	Rx-

1: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the port on the attached device has internal crossover wiring (MDI-X), then use straight-through cable.

Straight-Through Cable Pin Assignments	
End 1	End 2
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

Crossover Wiring

If the port on the attached device has straight-through wiring (MDI), use crossover cable.

Crossover Cable Pin Assignments	
End 1	End 2
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

ADSL Cable

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-11 ADSL port on the ADSL Router.

Caution: Do not plug a phone jack connector into an RJ-45 port.

Specifications

Cable Types and Specifications		
Cable	**Type**	**Connector**
ADSL Line	Standard Telephone Cable	RJ-11

Wiring Conventions

For ADSL connections, a cable requires one pair of wires. Each wire is identified by different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-11 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-11 connectors in a specific orientation. The following figure illustrates how the pins on the RJ-11 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.

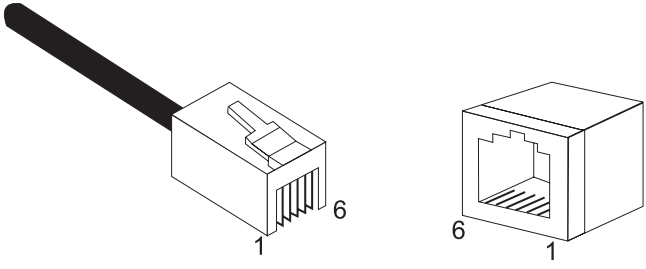
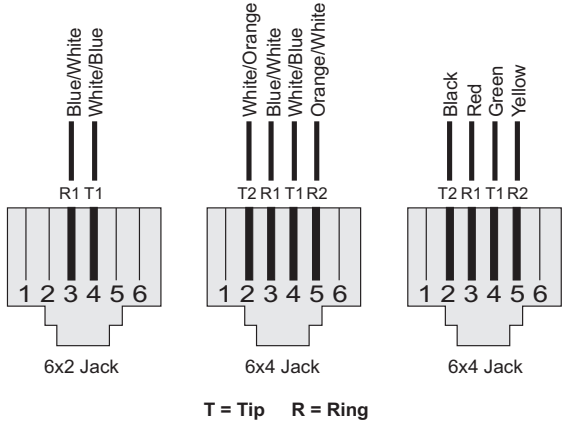


Figure B-2. RJ-11 Connector Pin Numbers



Pin	Signal Name	Wire Color
1	Not used	
2	Line 2 Tip	Black or White/Orange
3	Line 1 Ring	Red or Blue/White
4	Line 1 Tip	Green or White/Blue
5	Line 2 Ring	Yellow or Orange/White
6	Not used	

Figure B-3. RJ-11 Pinouts

APPENDIX C
SPECIFICATIONS

Physical Characteristics

Ports

Four 10/100Mbps RJ-45 ports
One ADSL port (RJ-11)

ADSL Features

Supports DMT line modulation
Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 &T1.413, Issue 2) and ADSL2 (G.992.3) and ADSl2+ (G.992.5)
Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream
Dying GASP support

ATM Features

RFC1483 Encapsulation (IP, Bridging and encapsulated routing)
PPP over ATM (LLC &VC multiplexing) (RFC2364)
Classical IP (RFC1577)
Traffic shaping (UBR, CBR)
OAM F4/F5 support
PPP over Ethernet Client

Management Features

Firmware upgrade via web based management
web based management (configuration)
Power Indicators
Event and History logging
Network Ping
Traceroute

Security Features
Password protected configuration access
User authentication (PAP/CHAP) with PPP
Firewall NAT NAPT
VPN pass through (IPSec-ESP Tunnel mode,L2TP, PPTP)

LAN Features
IEEE 802.1D (self-learning transparent Bridging)
DHCP Server
DNS Proxy
Static Routing, RIPv1 and RIP

Temperature: IEC 68-2-14
0 to 40 degrees C (Standard Operating)
-40 to 70 degree C (Non-operation)

Humidity
10% to 90% (Non-condensing)

Vibration: IEC 68-2-36, IEC 68-2-6

Shock: IEC 68-2-29

Drop: IEC 68-2-32

Dimensions: 143mm(L) x 94mm(D) x 32mm(H)

Weight: 500 g

Input Power: 15 V 0.8A

IEEE Standards
IEEE 802.3, 802.3u, 802.11g, 802.1D , 802.11 n draft
ITU G.dmt, ITU G.Handshake, ITU T.413 issue 2 - ADSL full rate

Standards Conformance Electromagnetic Compatibility
CE, ETSI, R&TTE, FCC part 15 class B & FCC part 68

Safety
EN 60950-1

Wireless Frequency Band

802.11b/g/n Radio: 2.4 GHz
USA - FCC
2412~2462 MHz (Ch1~Ch11)
Europe - ETSI
2412~2472 MHz (Ch1~Ch13)
France
2457~2472 MHz (Ch10~Ch13)

Modulation Technology: DSSS/OFDM

Operating Channels:
IEEE 802.11b compliant:
11 channels (US, Canada)
13 channels (ETSI)
4 channels (France)

IEEE 802.11g compliant:
11 channels (US, Canada)
13 channels (Europe)

IEEE draft 802.11n 20MHz compliant:
11 channels (US, Canada)
13 channels (Europe)

IEEE draft 802.11n 40MHz compliant:
7 channels (US, Canada)
9 channels (Europe)

Signal Type: DSSS/OFDM
Operating Frequency: 2.412 - 2.462GHz

FOR TECHNICAL SUPPORT, CALL:

1300 725 323

INTERNET

E-mail addresses: support@smc-australia.com.au

ENGLISH
Technical Support information available at www.smc.com

FRENCH
Informations Support Technique sur www.smc.com

DEUTSCH
Technischer Support und weitere Information unter www.smc.com

SPANISH
En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

DUTCH
Technische ondersteuningsinformatie beschikbaar op www.smc.com

PORTUGUES
Informações sobre Suporte Técnico em www.smc.com

SWEDISH
Information om Teknisk Support finns tillgängligt på www.smc.com

Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web:
http://www.smc-australia.com.au