SMC®
Networks

USER GUIDE

Barricade™ N
Draft 11n Wireless 4-port Broadband Router

SMCWBR14S-N2

Wireless Broadband Router User's Guide

From SMC's line of award-winning connectivity solutions

SMC®
Networks
20 Mason
Irvine, CA 92618
Phone: (949) 679-8000

September 2007
R01 F/W 1.0

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

Trademarks:

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.

SMC Networks, Inc.
20 Mason
Irvine, CA 92618

COMPLIANCES

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

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 20 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.

EC Declaration of Conformity CE0682 (!)

SMC contact for these products in Europe is:

SMC Networks Europe,
Edificio Conata II,
Calle Fructuos Gelabert 6-8, 2o, 4a,
08970 - Sant Joan Despi,
Barcelona, Spain.

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN 300 328

EN 301 489

EN 60950-1

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.

DGT Statement of Taiwan

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，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。

第十四條 低功率射頻電機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。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Safety Compliance

Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Operating Voltage	**Cord Set Specifications**
120 Volts	UL Listed/CSA Certified Cord Set
	Minimum 18 AWG
	Type SVT or SJT three conductor cord
	Maximum length of 15 feet
	Parallel blade, grounding type attachment plug rated 15 A, 125 V
240 Volts (Europe only)	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm2
	IEC-320 receptacle
	Male plug rated 10 A, 250 V

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the power adapter.

Information for Power Source

N11846

This unit is to be used with a class 2 or level 3 external power adapter, approved suitable for use in North American equipment installation, having an output voltage rating of 12 V DC, and output current rating of 1.0 A or equivalent.

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. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN 60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8 V, 50-60 Hz nicht über oder unterschreiten sowie den minimalen Strom von 1 A nicht unterschreiten.

Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70 dB(A) oder weniger.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Congratulations on your purchase of the Barricade™ N Draft 11n Wireless 4-port Broadband Router (SMCWBR14S-N2). 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. This new technology provides many secure and cost-effective functions. 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 IEEE 802.11b/g standards. This next generation wireless networking standard utilizes advanced MIMO (multiple-in, multiple-out) technology to deliver incredible speed and range. With wireless speeds up to 300Mbps - five times faster than 802.11g, the SMCWBR14S-N2 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

- IEEE802.11n draft v2.0 compliant
- Wireless speeds up to 300 Mbps
- Increased speed and coverage - up to 15 times the speed of IEEE 802.11g
- Fully backwards compatible with 802.11b/g wireless networks
- Allows you to stream HD video, listen to digital music, play online games, transfer large files, make VoIP calls and surf the Internet simultaneously
- Wi-Fi Multimedia (WMM) for wireless quality-of-service
- Local network connection via a 10/100 Mbps Ethernet port
- DHCP for dynamic IP configuration, and DNS 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, email, and Telnet)
- VPN transparent 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 this 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 allows you to share your Cable/xDSL Internet connection. Since many ADSL providers use PPPoE to establish communications with end users, the Barricade includes a built-in client for this protocol, eliminating the need to install these services on your computer.

- **Shared IP Address**

  The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web 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. WPA/WPA2, IEEE802.1x, WEP, SSID, and MAC filtering provide security over the wireless network.

- **Virtual Private Network (VPN Pass-through)**

  The Barricade supports three of the most commonly used VPN protocols – PPTP, L2TP, and IPSec. These VPN protocols are transparent pass-through. The 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 "Package Contents." If any of the items are missing or damaged, contact your local distributor. Also be sure that you have all the necessary cabling before installing the Barricade. After installing the Barricade, refer to "Configuring the Barricade" on page 4-1.

Package Contents

After unpacking the Barricade, check the contents of the box to be sure you have received the following components:

- Barricade™ N Draft 11n Wireless 4-port Broadband Router (SMCWBR14S-N2)
- Power adapter
- One CAT-5 Ethernet cable (RJ-45)
- One documentation CD
- Quick Install Guide
- 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:

- Broadband (Cable/xDSL) Internet service and Modem with Ethernet connection
- 2.4GHz 802.11n draft wireless adapter or 2.4GHz 802.11b/g wireless adapter installed on each PC. Alternatively an Ethernet adapter can be used.
- An up to date web browser: Internet Explorer 5.5 or above, Netscape 4.7 or above, Mozilla Firefox 1.0 or above.

Hardware Description

The Barricade connects to a cable or xDSL modem with Ethernet connection using it's RJ-45 WAN port. It can be connected directly to your PC or to a local area network using the Fast Ethernet LAN ports.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet port and up to 300 Mbps over the built-in wireless access point.

The Barricade includes an LED display on the top panel for system power and port indications that simplifies installation and network troubleshooting.

The following figures show the top and rear panels of the Barricade.

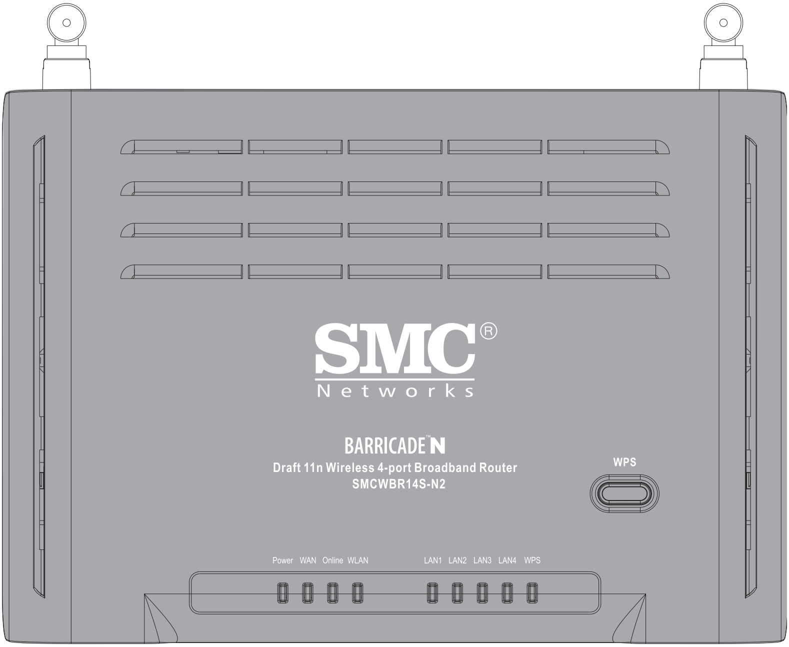


Figure 2-1. Top Panel

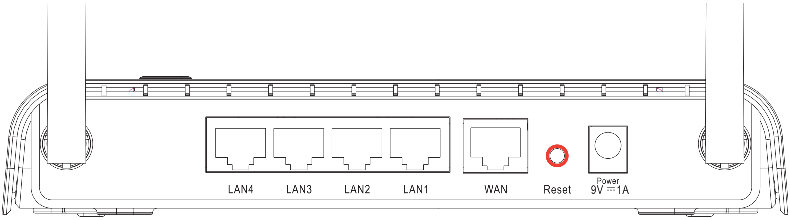


Figure 2-2. Rear Panel

The power and port LED indicators on the top panel are illustrated by the following table.

LED	Status	Description
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
WAN	On	WAN link.
	Off	No WAN link.
Online	On	Internet connection is functioning correctly.
	Flashing	The Barricade is establishing an Internet link.
	Off	No Internet link.
WLAN	On	WLAN link.
	Flashing	The Barricade is sending or receiving data via WLAN.
	Off	No WLAN link.
LAN 1~4	On	Ethernet link.
	Flashing	The LAN port is sending or receiving data.
	Off	No Ethernet link.
WPS (Wi-Fi Protected Setup)	On	WPS link is successfully established.
	Off	• This LED will be on for 300 seconds after WPS connection is successfully established, then go off. • The WPS is disabled.
	Slow Flashing	WPS association is establishing between the Barricade and clients.
	Quick Flashing	WPS access failed.

The Barricade contains the following ports and buttons:

Item	**Description**
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, switch or IP set top box).
WAN Port	WAN port (RJ-45). Connect your cable/xDSL modem line to this port.
Reset Button	Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-66.
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may cause damage.
WPS Button (on top panel)	Press this button for over 4 seconds to start using the WPS.

ISP Settings

If you are not sure of your connection method, please contact your Internet Service Provider. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP and L2TP.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

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 Cable/xDSL Modem

Connect the cable/xDSL modem using a CAT-5 Ethernet cable (RJ-45) to the Barricade's WAN port. When inserting the RJ-45 plug, be sure the tab on the plug clicks into position to ensure it is properly seated.

Connecting the Barricade to your LAN

The four LAN ports on the Barricade auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.

Use RJ-45 cables to connect any of the four LAN ports on the Barricade to an Ethernet adapter on your PC. Otherwise, cascade any of the LAN ports on the Barricade to an Ethernet hub or switch, and then connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

Notes: **1.** Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.

2. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).

Connect the Power Adapter

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

Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to “Troubleshooting” on page A-1.

In case of a power input failure, the Barricade will automatically restart and begin to operate once the input power is restored.

CHAPTER 3
CONFIGURING THE CLIENT PC

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade. You can either configure your computer to automatically obtain IP settings (DHCP) or manually configure IP address settings (Static IP).

Depending on your operating system see:

“Windows 2000” on page 3-3,

“Windows XP” on page 3-9,

or

“Configuring Your Macintosh Computer” on page 3-15.

TCP/IP Configuration

To access the Internet through the Barricade, you must configure the network settings of the computers on your LAN to use the same IP subnet as the Barricade. The default network settings for the Barricade are:

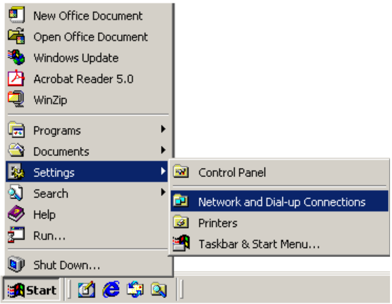
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0

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

Windows 2000

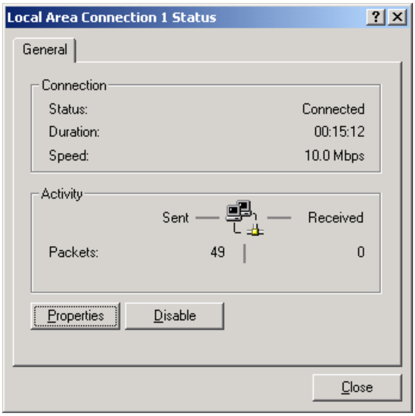
DHCP IP Configuration

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



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

3. The connection status screen will open. Click **Properties**.


Local Area Connection 1 Status

General

Connection

Status: Connected

Duration: 00:15:12

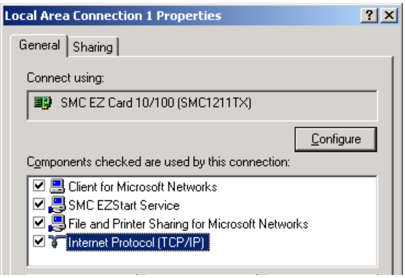
Speed: 10.0 Mbps

Activity

Sent — Received

Packets: 49 | 0

4. Double-click **Internet Protocol (TCP/IP)**.



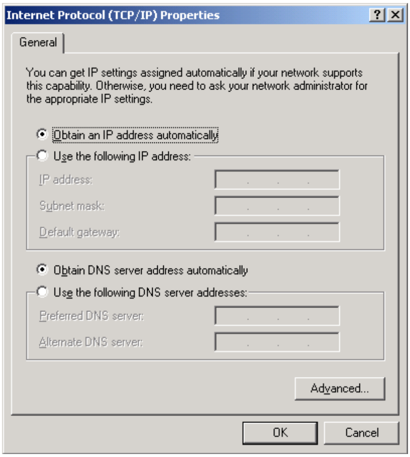
Connect using:

SMC EZ Card 10/100 (SMC1211TX)

Components checked are used by this connection:

- ☑ Client for Microsoft Networks
- ☑ SMC EZStart Service
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

5. If **Obtain an IP address automatically** and **Obtain DNS server address automatically** are already selected, your computer is already configured for DHCP. If not, select these options now and click **OK**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

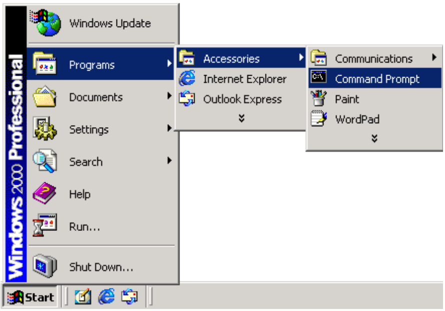
Preferred DNS server: . . .

Alternate DNS server: . . .

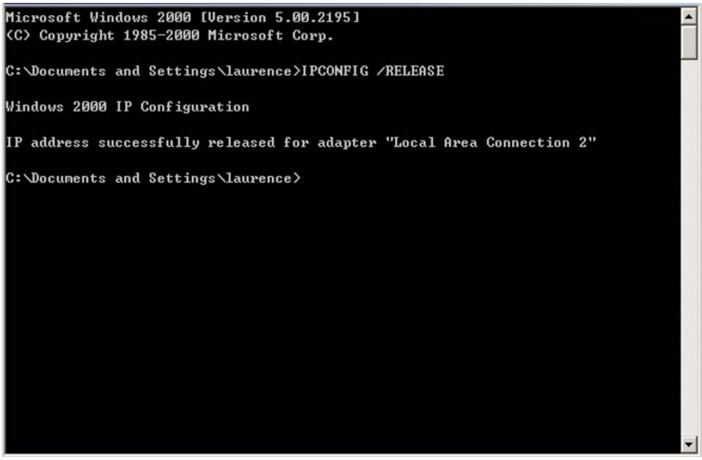
Obtain IP Settings From Your Barricade

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**.

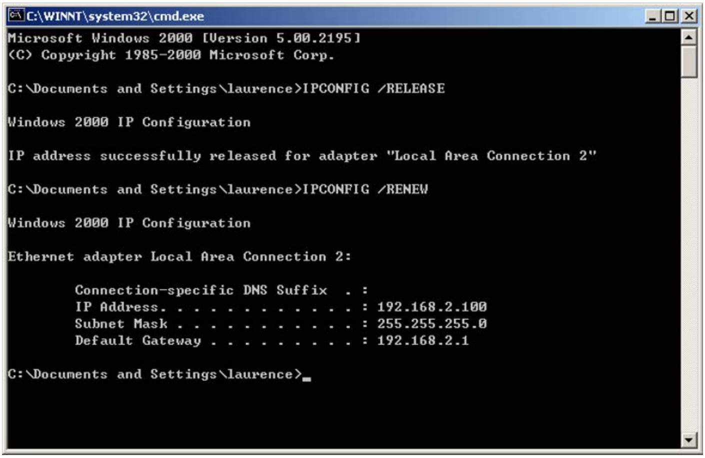


2. In the Command Prompt window, type **ipconfig /release** and press the **Enter** key.



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

C:\Documents and Settings\laurence>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 2"

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

3. Type **ipconfig /renew** and press the **Enter** key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning correctly.



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

C:\Documents and Settings\laurence>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 2"

C:\Documents and Settings\laurence>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

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

C:\Documents and Settings\laurence>_
```

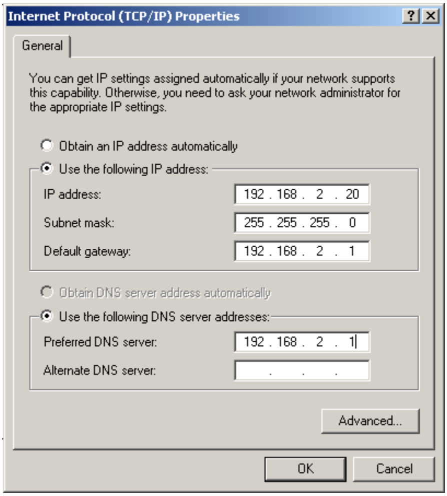
4. Type **exit** and press the **Enter** key to close the Command Prompt window.

Manual IP Configuration

1. Follow steps 1-4 in "DHCP IP Configuration" on page 3-3.

2. Select **Use the following IP address**. Enter an IP address based on the default network **192.168.2.x** (where x is between 2 and 254), and use **255.255.255.0** for the subnet mask. Use **192.168.2.1** for the Default gateway field.

3. Select **Use the following DNS server addresses**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 1

Alternate DNS server: . . .

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

5. Record the configured information in the following table.

TCP/IP Configuration Setting

IP Address _____._____._____._____

Subnet Mask _____._____._____._____

Preferred DNS Server _____._____._____._____

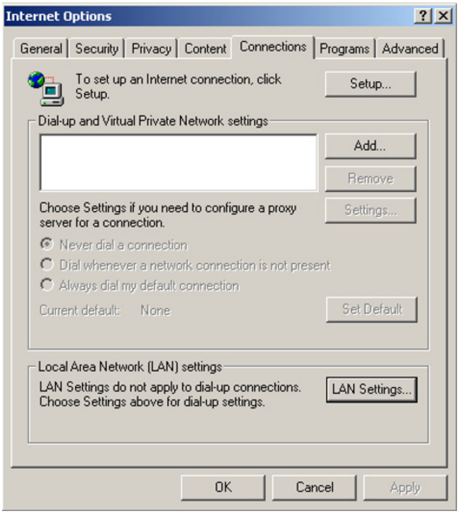
Alternate DNS Server _____._____._____._____

Default Gateway _____._____._____._____

Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages.

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



Internet Options

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

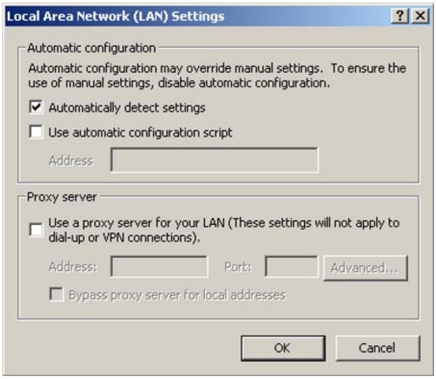
Current default: None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

2. In the Proxy server section, ensure the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** check box is not ticked.

3. Click **OK**.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

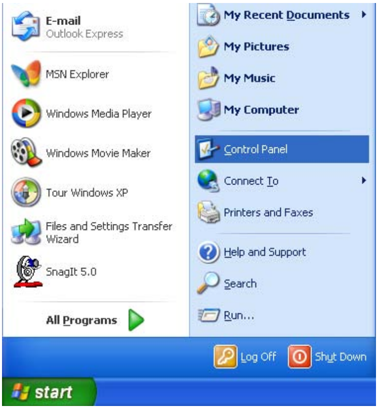
Address: Port:

□ Bypass proxy server for local addresses

Windows XP

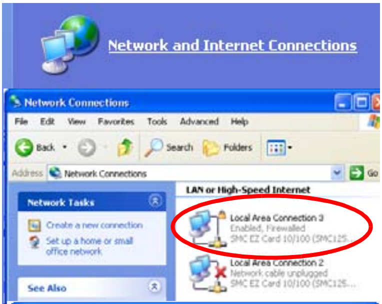
DHCP IP Configuration

1. On the Windows desktop, click **Start/Control Panel**.

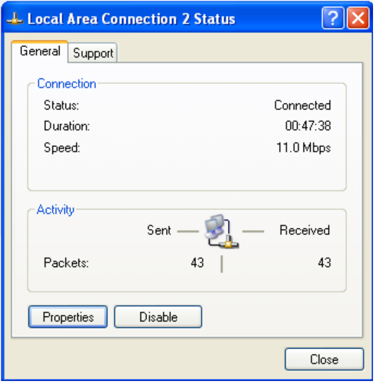


2. In the Control Panel window, click **Network and Internet Connections**.

3. The Network Connections window will open. Locate and double-click the **Local Area Connection** icon for the Ethernet adapter that is connected to the Barricade.



4. In the connection status screen, click **Properties**.


Local Area Connection 2 Status

General | Support

Connection

Status: Connected

Duration: 00:47:38

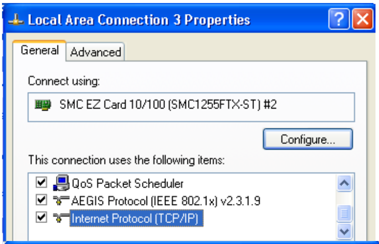
Speed: 11.0 Mbps

Activity

Sent — — Received

Packets: 43 | 43

5. Double-click **Internet Protocol (TCP/IP)**.



Local Area Connection 3 Properties

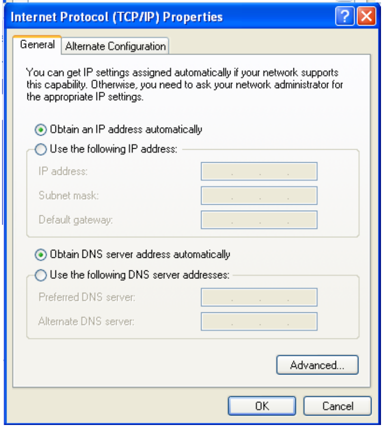
Connect using:

SMC EZ Card 10/100 (SMC1255FTX-ST) #2

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v2.3.1.9
☑ Internet Protocol (TCP/IP)

6. If **Obtain an IP address automatically** and **Obtain DNS server address automatically** are already selected, your computer is already configured for DHCP. If not, select these options now and click **OK**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

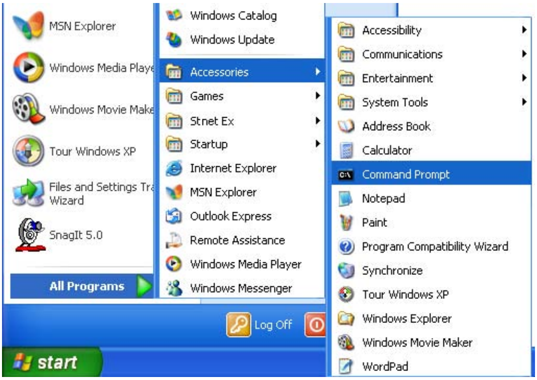
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

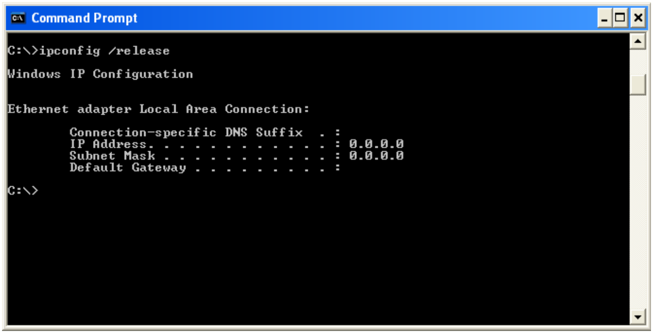
Obtain IP Settings From Your Barricade

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**.

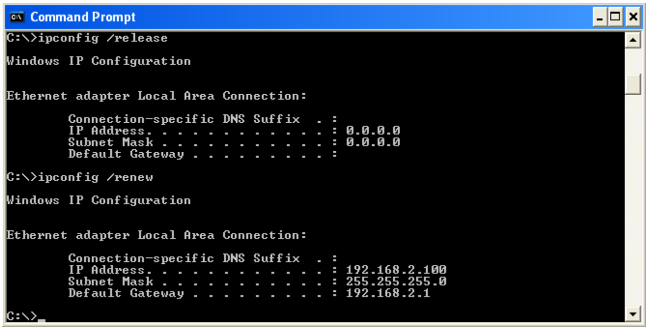


2. In the Command Prompt window, type **ipconfig /release** and press the **Enter** key.



```
C:\>ipconfig /release
Windows IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\>
```

3. Type **ipconfig /renew** and press the **Enter** key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning correctly.



```
C:\>ipconfig /release

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 0.0.0.0
        Subnet Mask . . . . . . . . . . . : 0.0.0.0
        Default Gateway . . . . . . . . . :

C:\>ipconfig /renew

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

C:\>_
```

4. Type **exit** and press the **Enter** key to close the Command Prompt window.

Your computer is now configured to connect to the Barricade.

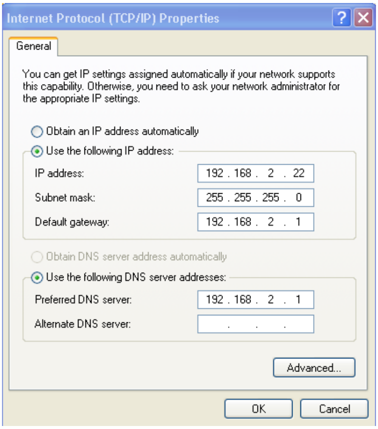
Manual IP Configuration

1. Follow steps 1-5 in “DHCP IP Configuration” on page 3-9.

2. Select **Use the following IP Address**.

3. Enter an IP address based on the default network **192.168.2.x** (where x is between 2 and 254), and use **255.255.255.0** for the subnet mask. Use **192.168.2.1** for the Default gateway field.

4. Select **Use the following DNS server addresses**.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 22

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 2 . 1

Alternate DNS server: . . .

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

6. Record the configured information in the following table.

TCP/IP Configuration Setting

IP Address ____.____.____.____

Subnet Mask ____.____.____.____

Preferred DNS Server ____.____.____.____

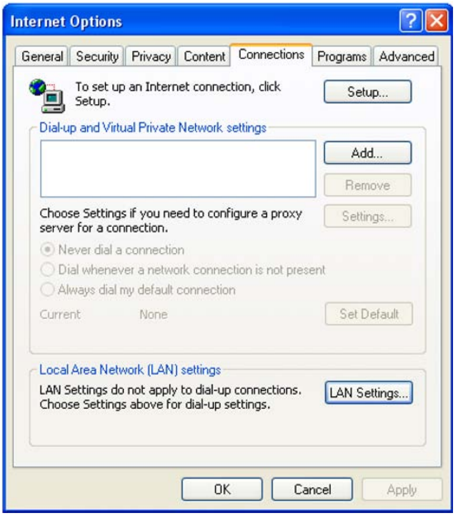
Alternate DNS Server ____.____.____.____

Default Gateway ____.____.____.____

Disable HTTP Proxy

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

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



Internet Options

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

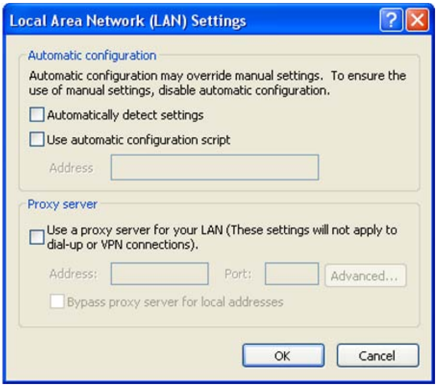
Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

2. In the Proxy server section, ensure the **Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)** check box is not ticked.

3. Click **OK**.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

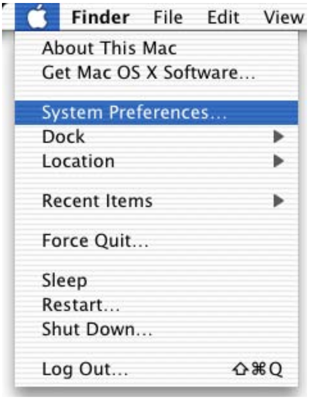
□ Bypass proxy server for local addresses

Configuring Your Macintosh Computer

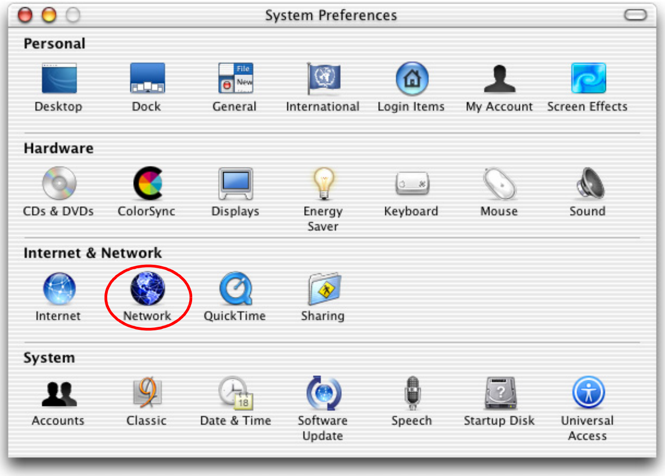
You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

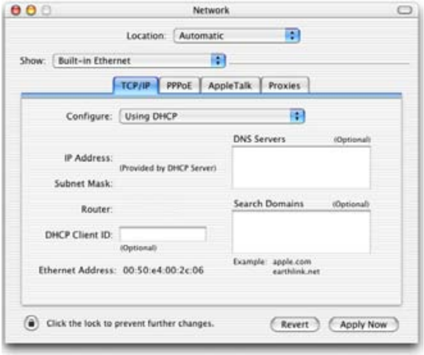
1. Pull down the **Apple Menu** . Click **System Preferences**.



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.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: (Provided by DHCP Server)

Ethernet Address: 00:50:e4:00:2c:06

Click the lock to prevent further changes.

4. Your new settings are shown in the TCP/IP tab. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your Barricade is functioning.

5. Close the Network window.

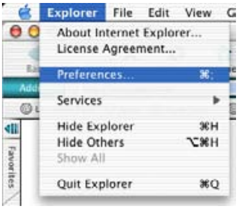
Now your computer is configured to connect to the Barricade.

Disable HTTP Proxy

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

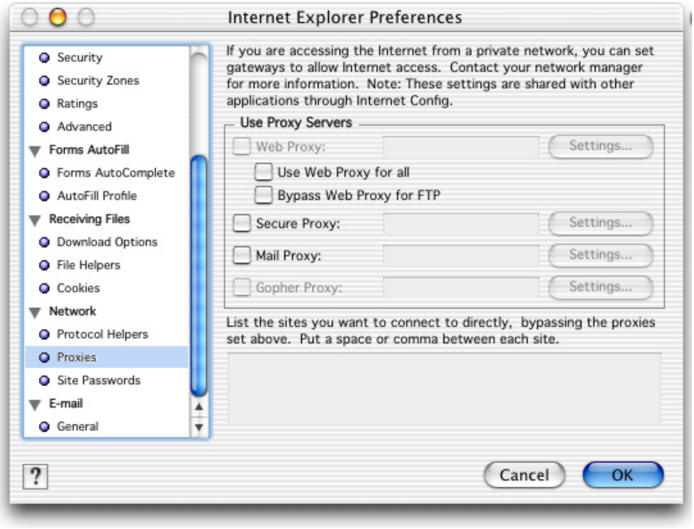
Internet Explorer

1. Open Internet Explorer and click the **Stop** button. Click **Explorer/Preferences**.



2. In the Internet Explorer Preferences window, under Network, select **Proxies**.

3. Uncheck all check boxes and click **OK**.



If you are accessing the Internet from a private network, you can set gateways to allow Internet access. Contact your network manager for more information. Note: These settings are shared with other applications through Internet Config.

Use Proxy Servers

□ Web Proxy: Settings...

□ Use Web Proxy for all

□ Bypass Web Proxy for FTP

□ Secure Proxy: Settings...

□ Mail Proxy: Settings...

□ Gopher Proxy: Settings...

List the sites you want to connect to directly, bypassing the proxies set above. Put a space or comma between each site.

CHAPTER 4
CONFIGURING THE BARRICADE

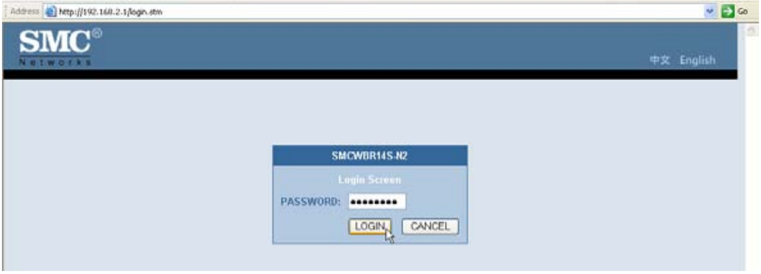
After you have configured TCP/IP on a client computer, use a web browser to configure the Barricade. The Barricade can be configured by any Java-supported browser such as Internet Explorer 5.5 or above. Using the web management interface, you can configure the Barricade and view statistics to monitor network activity.

To access the Barricade's management interface, enter the IP address of the Barricade in your web browser: http://192.168.2.1.

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

Notes: 1 Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

2 You might click the language selection at the top right corner of the screen for your regional location before accessing the management interface.



Address: http://192.168.2.1/login.stm

SMCWBR14S-N2

Login Screen

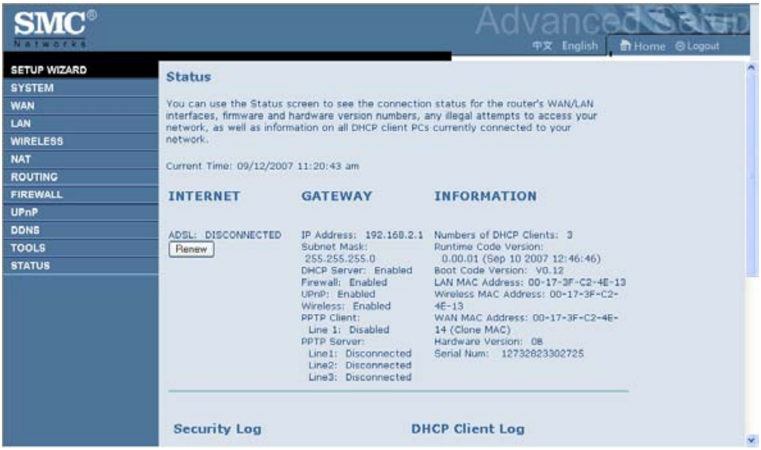
PASSWORD: •••••••••

Navigating the Web Browser Interface

The Barricade's management interface consists of a Setup Wizard and an Advanced Settings section.

Setup Wizard: Use the Setup Wizard for quick and easy configuration of your Internet connection and basic LAN settings.

Advanced Settings: Advanced Settings supports more advanced functions like NAT, system maintenance, firewall and UPnP.



Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 09/12/2007 11:20:43 am

INTERNET

ADSL: DISCONNECTED

GATEWAY

IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
Firewall: Enabled
UPnP: Enabled
Wireless: Enabled
PPTP Client:
Line 1: Disabled
PPTP Server:
Line1: Disconnected
Line2: Disconnected
Line3: Disconnected

INFORMATION

Numbers of DHCP Clients: 3
Runtime Code Version: 0.00.01 (Sep 10 2007 12:46:46)
Boot Code Version: V0.12
LAN MAC Address: 00-17-3F-C2-4E-13
Wireless MAC Address: 00-17-3F-C2-4E-13
WAN MAC Address: 00-17-3F-C2-4E-14 (Clone MAC)
Hardware Version: 08
Serial Num: 12732823302725

Making Configuration Changes

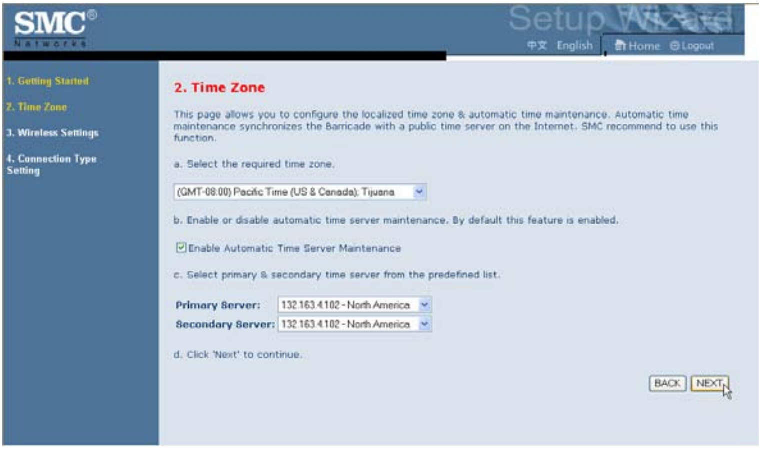
Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a screen, click the **APPLY** or **SAVE SETTINGS** or **NEXT** button at the bottom of the screen to enable the new setting.

Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 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**, then 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.



2. Time Zone

This page allows you to configure the localized time zone & automatic time maintenance. Automatic time maintenance synchronizes the Barricade with a public time server on the Internet. SMC recommend to use this function.

a. Select the required time zone.

(GMT-08:00) Pacific Time (US & Canada); Tijuana

b. Enable or disable automatic time server maintenance. By default this feature is enabled.

☑ Enable Automatic Time Server Maintenance

c. Select primary & secondary time server from the predefined list.

Primary Server: 132.163.4.102 - North America
Secondary Server: 132.163.4.102 - North America

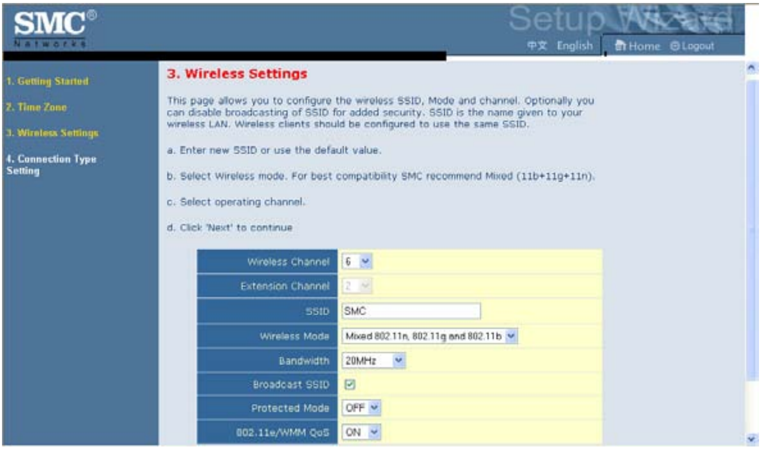
d. Click 'Next' to continue.

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

Click **NEXT** to continue.

Wireless Settings

This screen allows you to configure the SSID, wireless Mode and channel. Optionally you can disable broadcasting of SSID for added security. SSID is the name given to your wireless LAN. Wireless clients within the same network should be configured to use the same SSID.



3. Wireless Settings

This page allows you to configure the wireless SSID, Mode and channel. Optionally you can disable broadcasting of SSID for added security. SSID is the name given to your wireless LAN. Wireless clients should be configured to use the same SSID.

a. Enter new SSID or use the default value.

b. Select Wireless mode. For best compatibility SMC recommend Mixed (11b+11g+11n).

c. Select operating channel.

d. Click 'Next' to continue

Wireless Channel	6
Extension Channel	2
SSID	SMC
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Bandwidth	20MHz
Broadcast SSID	☑
Protected Mode	OFF
802.11e/WMM QoS	ON

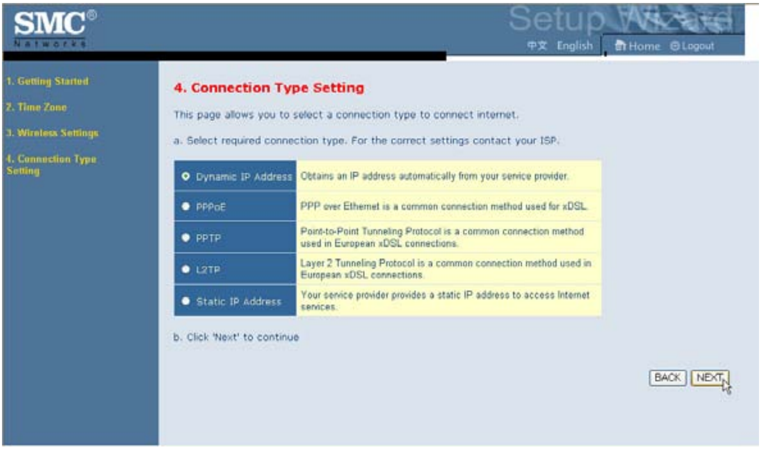
Parameter	Description
Wireless Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients. The Barricade will automatically assign itself a radio channel, or you may select one manually.
Extension Channel	Setting the Bandwith Mode as 20/40MHz allows you to use this extension channel as the secondary channel for doubling the bandwith of your wireless network.
SSID	Service Set ID. The SSID must be the same on the Barricade and all of its wireless clients. (Default: SMC)
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
Bandwidth	• 20MHz: Sets the operation bandwidth as 20 MHz. • 20/40MHz: Allows automatic detection of the operation bandwidth between 20 MHz and 40 MHz. Choosing the bandwidth mode as 20/40MHz allows you to use the extension channel.
Broadcast SSID	Enable or disable the broadcasting of the SSID. Disabling SSID broadcast will provide increased security by hiding the SSID of your wireless network.
Protected Mode	Enabling this function to ensure the best performance of your 11n throughput in case there is a lot of interference from the 11g and 11b devices in the wireless network.
802.11e/WMM QoS	Enable or disable the use of QoS. The QoS (Quality of Service) function allows you to differentiate WMM (Wi-Fi Multimedia) traffic and provide it with high-priority forwarding service

Click **NEXT** to continue.

Connection Type Setting

Specify the WAN connection type required by your Internet Service Provider. Specify Dynamic IP Address, PPPoE, PPTP, L2TP or Static IP Address.



4. Connection Type Setting

This page allows you to select a connection type to connect internet.

a. Select required connection type. For the correct settings contact your ISP.

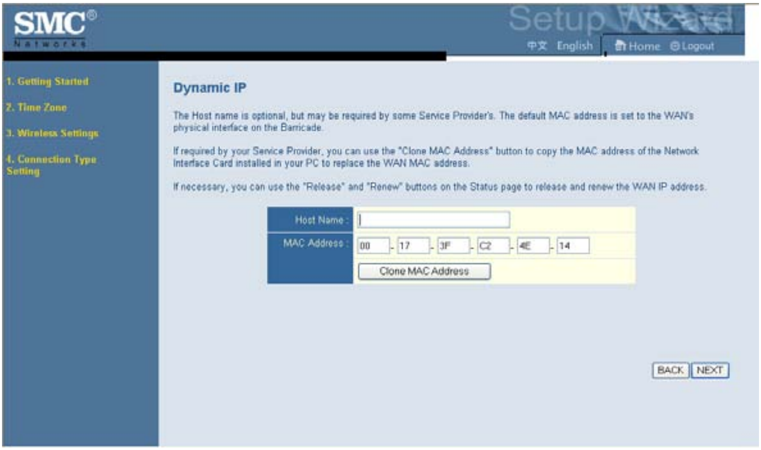
◉ Dynamic IP Address	Obtains an IP address automatically from your service provider.
○ PPPoE	PPP over Ethernet is a common connection method used for xDSL.
○ PPTP	Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.
○ L2TP	Layer 2 Tunneling Protocol is a common connection method used in European xDSL connections.
○ Static IP Address	Your service provider provides a static IP address to access Internet services.

b. Click 'Next' to continue

Select your connection type to proceed. Click **BACK** to go back and change your settings.

Dynamic IP Address

If the ISP requires you to input a Host Name, type it in the **Host Name** field. Click on the **Clone the MAC Address** and the **MAC Address** of the current PC will be filled automatically.



Dynamic IP

The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Barricade.

If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.

If necessary, you can use the "Release" and "Renew" buttons on the Status page to release and renew the WAN IP address.

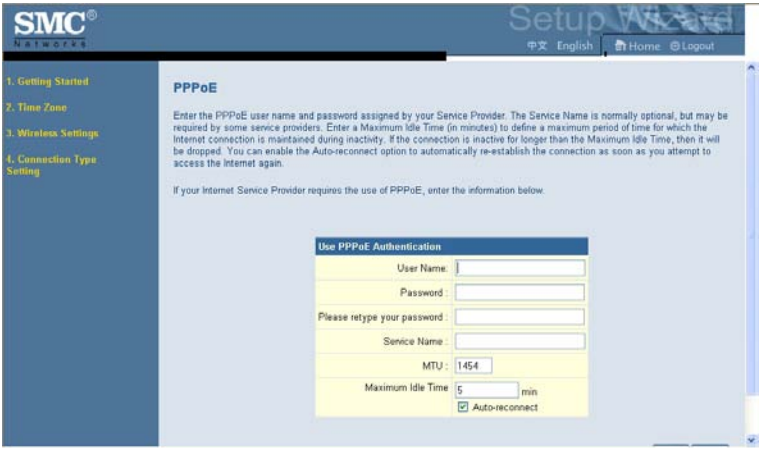
Host Name :

MAC Address : 00 - 17 - 3F - C2 - 4E - 14

Click **NEXT** to proceed, or **BACK** to change your settings.

PPPoE

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a Service Name enter it in the **Service Name** field, otherwise, leave it blank. Leave the Maximum Transmission Unit (MTU) at the default value (1454) unless you have a particular reason to change it. Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. Check the **Auto-reconnect** check box to automatically re-establish the connection as soon as you attempt to access the Internet again.



PPPoE

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

If your Internet Service Provider requires the use of PPPoE, enter the information below.

Use PPPoE Authentication	
User Name:	
Password :	
Please retype your password :	
Service Name :	
MTU :	1454
Maximum Idle Time	5 min ☑ Auto-reconnect

Click **NEXT** to proceed, or **BACK** to change your settings.

Note: Clicking **NEXT** will not automatically connect the Barricade to the Internet. The Barricade will only connect when you explicitly request it to, for example, by launching your web browser.

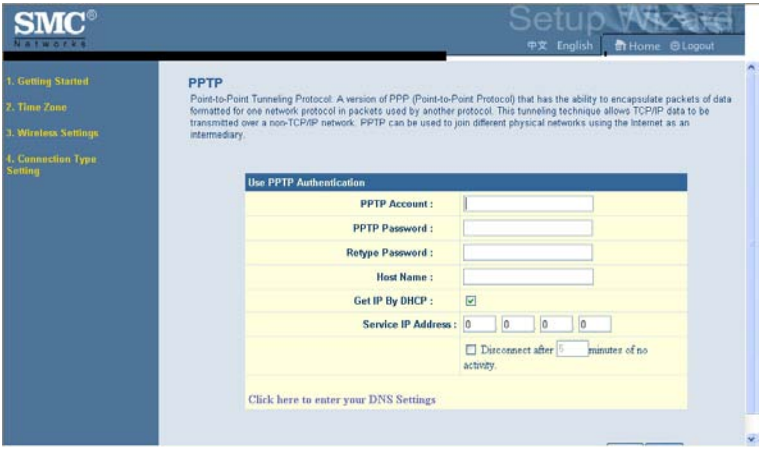
PPTP (Point-to-Point Tunneling Protocol)

The Barricade supports PPTP connection. The PPTP connection delivers user-level authentication VPN (virtual private network) for secure network path.

Enter the user account ID and password required by your ISP in the appropriate fields. If your ISP has provided you with a Host Name enter it in the **Host Name** field, otherwise, leave it blank. If your ISP uses DHCP service, enable the **Get IP by DHCP**. Then enter the **Service IP Address** provided by your ISP.

Click on the **Disconnect after x minutes of no activity** and then enter the idle time for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. If your ISP charges you by the minute, you should change the idle time out to one minute.

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. Clicking on the **Click here to enter your DNS Settings** for DNS configuration. See "DNS" on page 4-22.



PPTP

Point-to-Point Tunneling Protocol: A version of PPP (Point-to-Point Protocol) that has the ability to encapsulate packets of data formatted for one network protocol in packets used by another protocol. This tunneling technique allows TCP/IP data to be transmitted over a non-TCP/IP network. PPTP can be used to join different physical networks using the Internet as an intermediary.

Use PPTP Authentication

PPTP Account :	
PPTP Password :	
Retype Password :	
Host Name :	
Get IP By DHCP :	☑
Service IP Address :	0 . 0 . 0 . 0
	☐ Disconnect after 5 minutes of no activity.

Click here to enter your DNS Settings

Click **NEXT** to proceed, or **BACK** to change your settings.

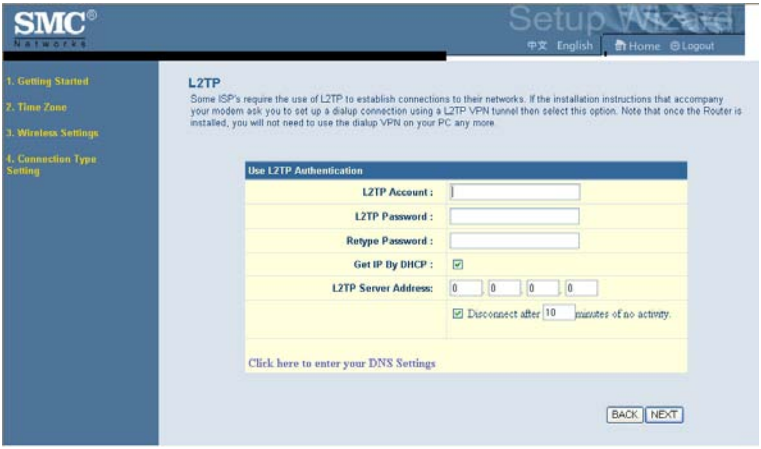
L2TP (Layer 2 Tunneling Protocol)

The Barricade supports L2TP connection. The L2TP connection delivers computer-level authentication VPN (virtual private network) for secure network path.

Enter the user account ID and password required by your ISP in the appropriate fields. If your ISP uses DHCP service, enable the **Get IP by DHCP**. Then enter the **L2TP Server Address** provided by your ISP.

Click on the **Disconnect after x minutes of no activity** and then enter the idle time for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. If your ISP charges you by the minute, you should change the idle time out to one minute.

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. Clicking on the **Click here to enter your DNS Settings** for DNS configuration. See "DNS" on page 4-22.



L2TP

Some ISP's require the use of L2TP to establish connections to their networks. If the installation instructions that accompany your modem ask you to set up a dialup connection using a L2TP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more

Use L2TP Authentication

L2TP Account :

L2TP Password :

Retype Password :

Get IP By DHCP : ☑

L2TP Server Address: 0 . 0 . 0 . 0

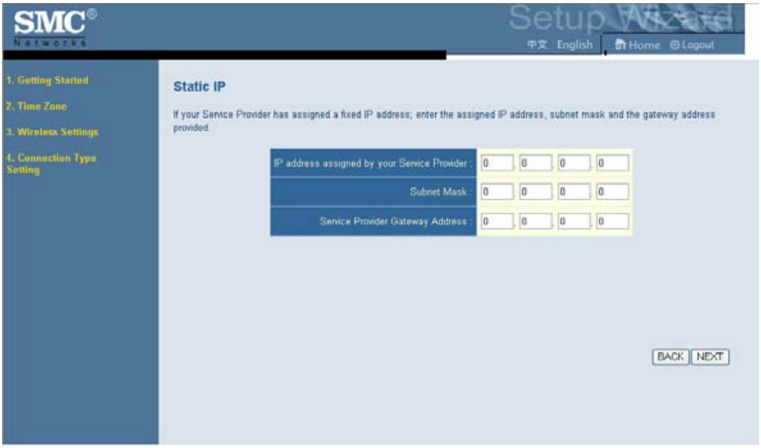
☑ Disconnect after 10 minutes of no activity.

Click here to enter your DNS Settings

Click **NEXT** to proceed, or **BACK** to change your settings.

Static IP Address

Enter the IP address, Subnet Mask and Gateway Address provided to you by your ISP in the appropriate fields below.



Static IP

If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.

IP address assigned by your Service Provider : 0 . 0 . 0 . 0

Subnet Mask : 0 . 0 . 0 . 0

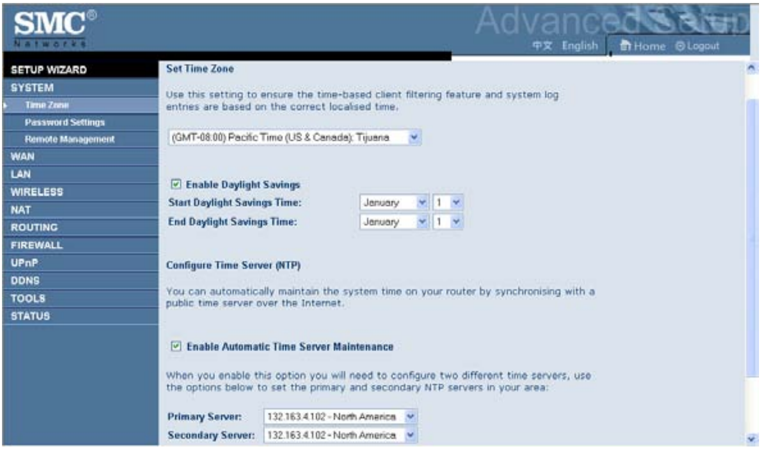
Service Provider Gateway Address : 0 . 0 . 0 . 0

Click **NEXT** to proceed, or **BACK** to change your settings.

System

Time Zone

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



Set Time Zone

Use this setting to ensure the time-based client filtering feature and system log entries are based on the correct localised time.

(GMT-08:00) Pacific Time (US & Canada); Tijuana

☑ **Enable Daylight Savings**

Start Daylight Savings Time: January 1

End Daylight Savings Time: January 1

Configure Time Server (NTP)

You can automatically maintain the system time on your router by synchronising with a public time server over the Internet.

☑ **Enable Automatic Time Server Maintenance**

When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:

Primary Server: 132.163.4.102 - North America

Secondary Server: 132.163.4.102 - North America

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

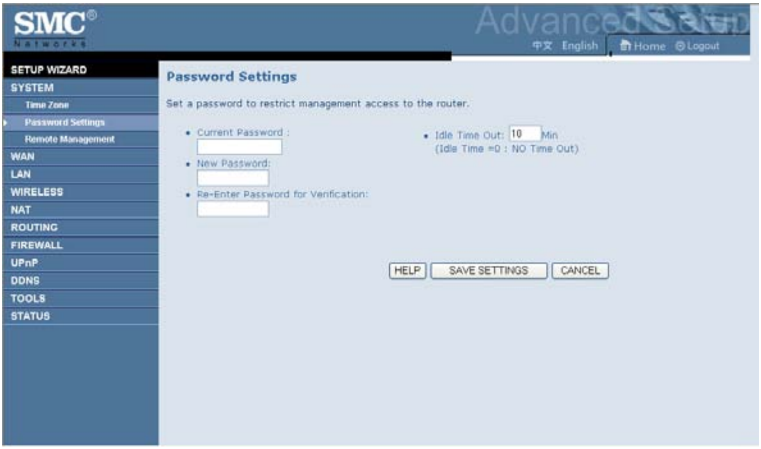
If daylight savings is used in your area, check the box to enable the function, and select the start/end dates.

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

Click **SAVE SETTINGS**.

Password Settings

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



Password Settings

Set a password to restrict management access to the router.

- Current Password :
- New Password:
- Re-Enter Password for Verification:
- Idle Time Out: 10 Min
  (Idle Time =0 : NO Time Out)

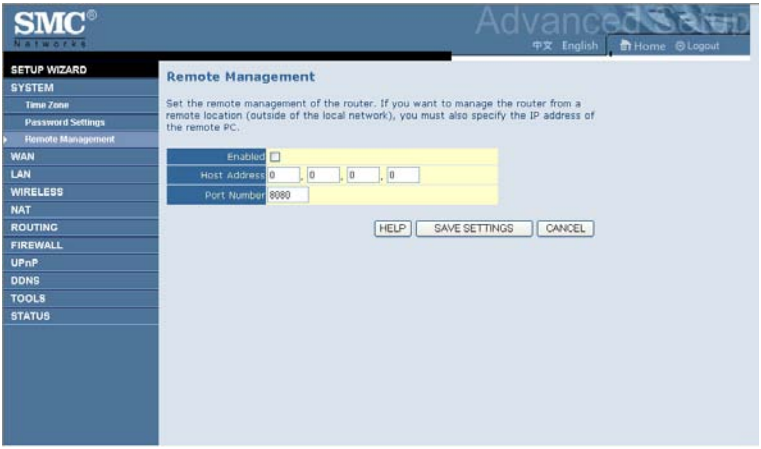
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

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**.



Remote Management

Set the remote management of the router. If you want to manage the router from a remote location (outside of the local network), you must also specify the IP address of the remote PC.

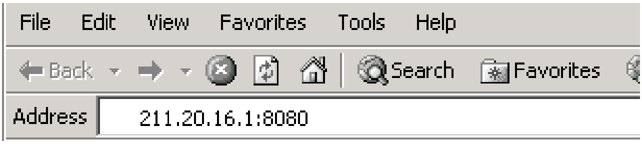
Enabled □

Host Address 0 . 0 . 0 . 0

Port Number 8080

Note: If you check Enable and specify an IP address of 0.0.0.0, any remote host can manage the Barricade.

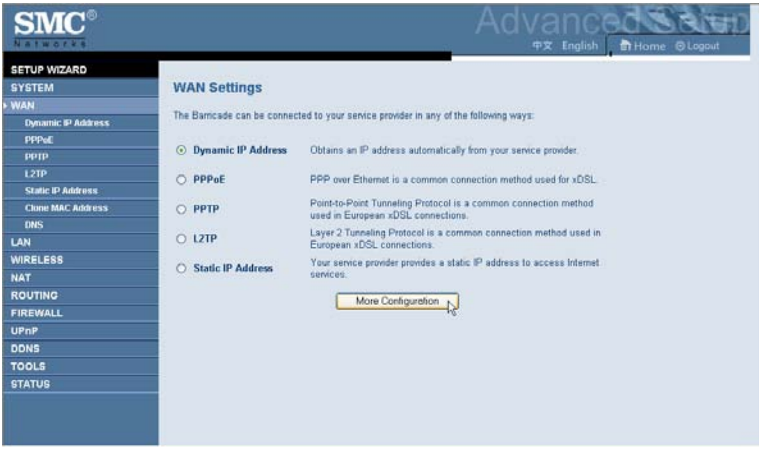
For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080, for example, 211.20.16.1:8080.



Address 211.20.16.1:8080

WAN Settings

Specify the WAN connection type required by your Internet Service Provider. Choose **Dynamic IP Address**, **PPPoE**, **PPTP**, **L2TP** or **Static IP Address** for your WAN link.



WAN Settings

The Barricade can be connected to your service provider in any of the following ways:

● Dynamic IP Address — Obtains an IP address automatically from your service provider.

○ PPPoE — PPP over Ethernet is a common connection method used for xDSL.

○ PPTP — Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.

○ L2TP — Layer 2 Tunneling Protocol is a common connection method used in European xDSL connections.

○ Static IP Address — Your service provider provides a static IP address to access Internet services.

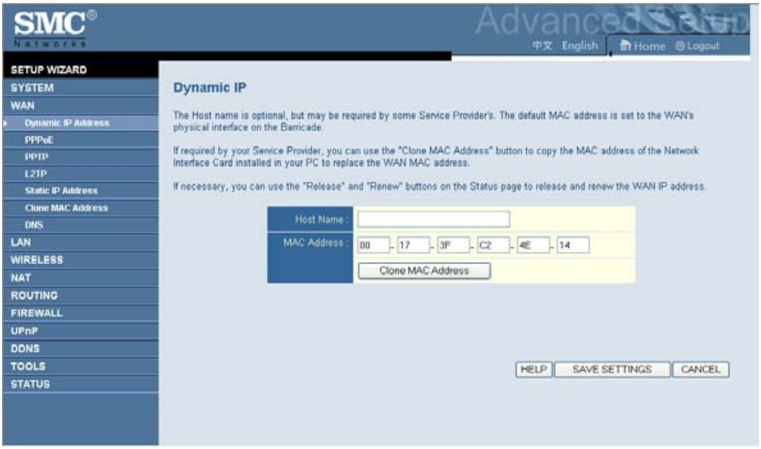
Select the connection type and click **More Configuration**.

Dynamic IP

The Host Name is optional, but may be required by some service provider's. The default MAC address is set to the WAN's physical interface on the Barricade.

If required by your service provider, you can use the **Clone MAC Address** button to copy the MAC address of the Network Interface Card (NIC) installed in your PC to replace the WAN MAC address.

If necessary, you can use the **Renew** button on the Status page to renew the WAN IP address.



Dynamic IP

The Host name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the Barricade.

If required by your Service Provider, you can use the "Clone MAC Address" button to copy the MAC address of the Network Interface Card installed in your PC to replace the WAN MAC address.

If necessary, you can use the "Release" and "Renew" buttons on the Status page to release and renew the WAN IP address.

Host Name :

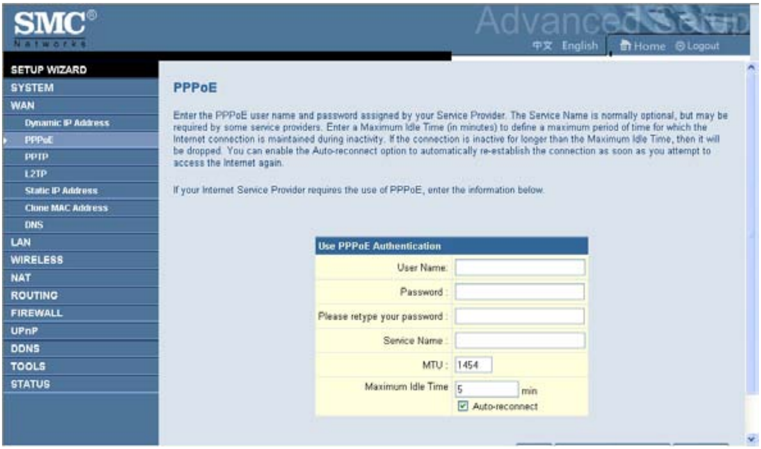
MAC Address : 00 - 17 - 3F - C2 - 4E - 14

Note: Make sure you record the MAC address that you clone, so that if you lose your settings you will be able to re-connect to the Internet.

Click **SAVE SETTINGS** to proceed, or **CANCEL** to change your settings.

PPPoE

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the **Auto-reconnect** option to automatically re-establish the connection as soon as you attempt to access the Internet again.



PPPoE

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.

If your Internet Service Provider requires the use of PPPoE, enter the information below.

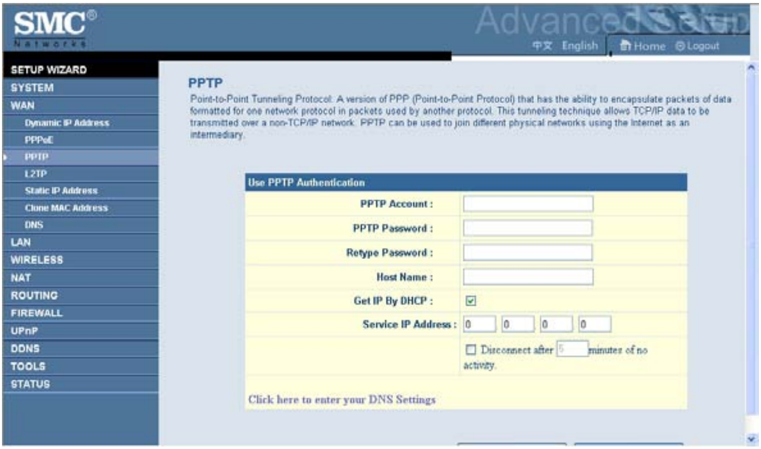
Use PPPoE Authentication	
User Name:	
Password :	
Please retype your password :	
Service Name :	
MTU :	1454
Maximum Idle Time	5 min ☑ Auto-reconnect

Click **SAVE SETTINGS** to proceed, or **CANCEL** to change your settings.

PPTP

Enter the Account ID and Password, and Host Name assigned by your ISP in the appropriate fields. If your ISP uses DHCP service, enable the **Get IP by DHCP**. Then enter the **Service IP Address** provided by your ISP. Click on the **Disconnect after x minutes of no activity** and then enter the idle time for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. If your ISP charges you by the minute, you should change the idle time out to one minute.

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. Clicking on the **Click here to enter your DNS Settings** for DNS configuration. See "DNS" on page 4-22.



PPTP

Point-to-Point Tunneling Protocol: A version of PPP (Point-to-Point Protocol) that has the ability to encapsulate packets of data formatted for one network protocol in packets used by another protocol. This tunneling technique allows TCP/IP data to be transmitted over a non-TCP/IP network. PPTP can be used to join different physical networks using the Internet as an intermediary.

Use PPTP Authentication

PPTP Account :

PPTP Password :

Retype Password :

Host Name :

Get IP By DHCP : ☑

Service IP Address : 0 . 0 . 0 . 0

☐ Disconnect after 5 minutes of no activity.

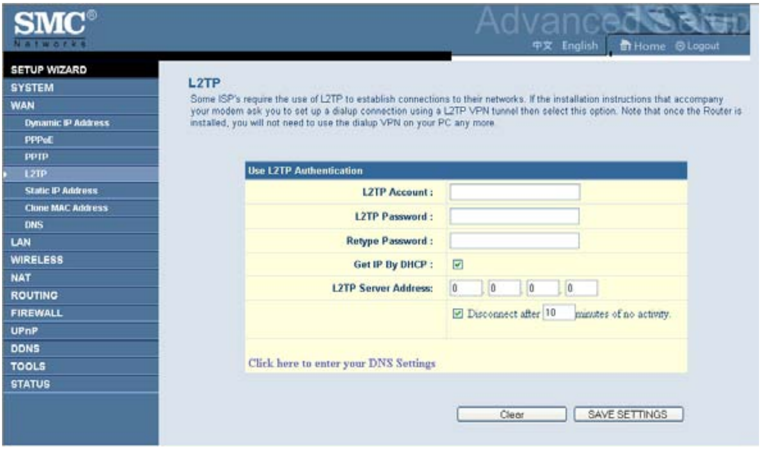
Click here to enter your DNS Settings

Click **SAVE SETTINGS** to proceed, or **Clear** to change your settings.

L2TP

Enter the L2TP Account ID and Password assigned by your ISP in the appropriate fields. If your ISP uses DHCP service, enable the **Get IP by DHCP**. Then enter the **L2TP Server Address** provided by your ISP. Click on the **Disconnect after x minutes of no activity** and then enter the idle time for the Internet connection. This is the period of time for which the connection to the Internet is maintained during inactivity. If your ISP charges you by the minute, you should change the idle time out to one minute.

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. Clicking on the **Click here to enter your DNS Settings** for DNS configuration. See "DNS" on page 4-22.



L2TP

Some ISP's require the use of L2TP to establish connections to their networks. If the installation instructions that accompany your modem ask you to set up a dialup connection using a L2TP VPN tunnel then select this option. Note that once the Router is installed, you will not need to use the dialup VPN on your PC any more

Use L2TP Authentication

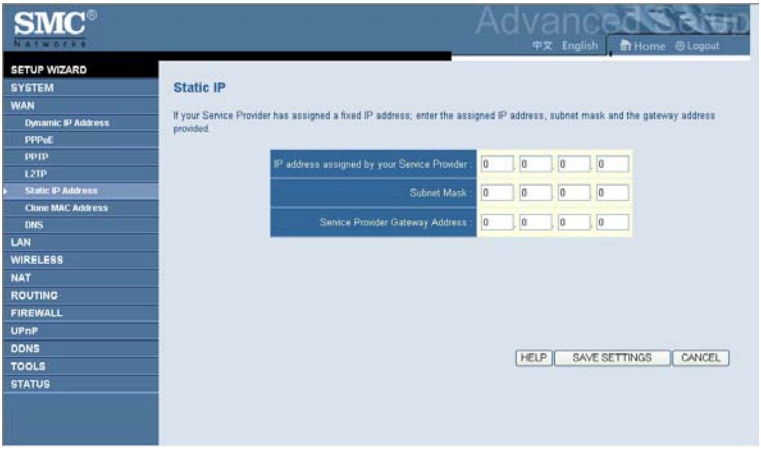
L2TP Account :	
L2TP Password :	
Retype Password :	
Get IP By DHCP :	☑
L2TP Server Address:	0 . 0 . 0 . 0
	☑ Disconnect after 10 minutes of no activity

Click here to enter your DNS Settings

Click **SAVE SETTINGS** to proceed, or **Clear** to change your settings.

Static IP

If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address on this screen.



Static IP

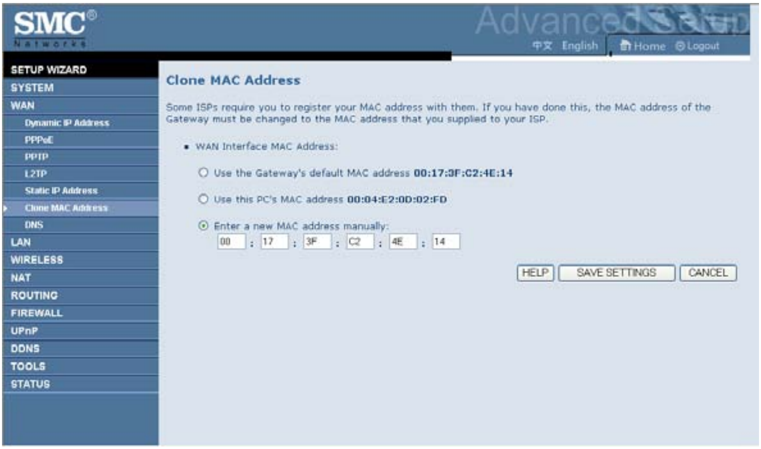
If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.

IP address assigned by your Service Provider :	0	0	0	0
Subnet Mask :	0	0	0	0
Service Provider Gateway Address :	0	0	0	0

Click **SAVE SETTINGS** to proceed, or **CANCEL** to change your settings.

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.



Clone MAC Address

Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.

- WAN Interface MAC Address:

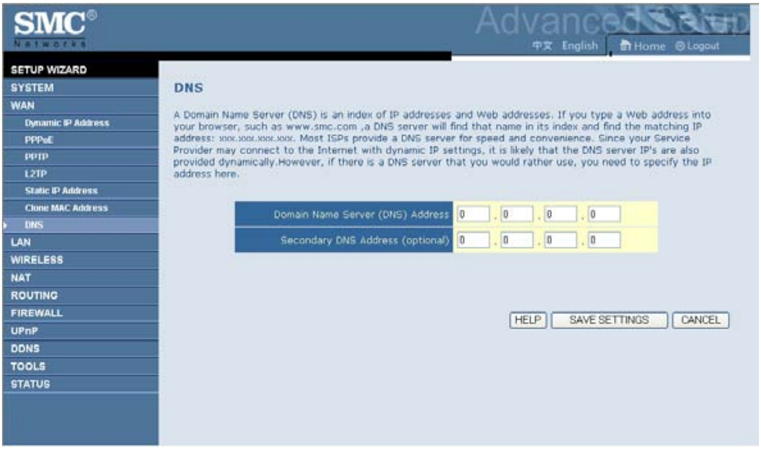
○ Use the Gateway's default MAC address **00:17:3F:C2:4E:14**

○ Use this PC's MAC address **00:04:E2:0D:02:FD**

● Enter a new MAC address manually:
00 : 17 : 3F : C2 : 4E : 14

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.



DNS

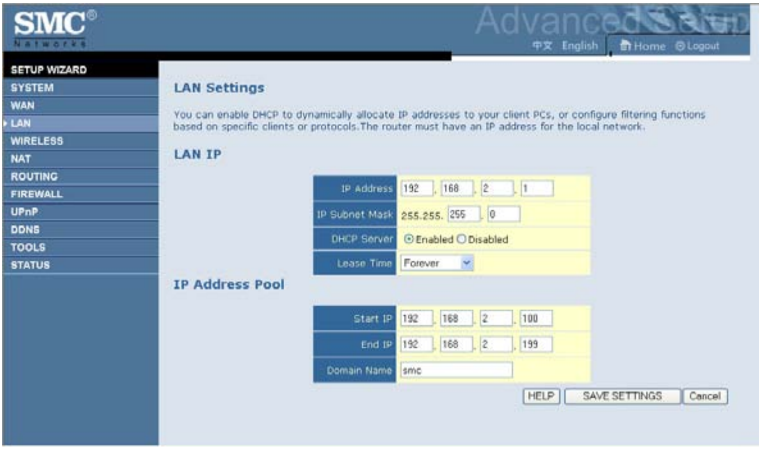
A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com ,a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since 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.

Domain Name Server (DNS) Address 0 . 0 . 0 . 0

Secondary DNS Address (optional) 0 . 0 . 0 . 0

LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Barricade must have an IP address for the local network.



LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols.The router must have an IP address for the local network.

LAN IP

IP Address: 192 . 168 . 2 . 1
IP Subnet Mask: 255.255. 255 . 0
DHCP Server: ● Enabled ○ Disabled
Lease Time: Forever

IP Address Pool

Start IP: 192 . 168 . 2 . 100
End IP: 192 . 168 . 2 . 199
Domain Name: smc

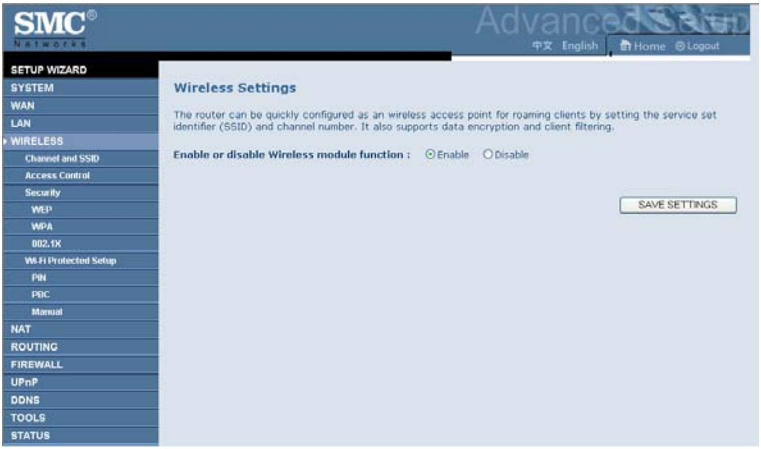
The LAN Settings parameters are listed below.

Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	The IP subnet mask.
DHCP Server	DHCP allows individual computers to obtain the TCP/IP configuration at startup from a centralized DHCP server. To dynamically assign an IP address to a client PC, enable the DHCP (Dynamic Host Configuration Protocol) function.

Parameter	Description
Lease Time	The length of time the DHCP server will reserve the IP address for each computer. Setting lease times for shorter intervals such as one day or one hour frees IP addresses after the specified period of time. This also means that a particular computer's IP address may change over time. If you have set any advanced features such as DMZ, this is dependent on the IP address. For this reason, you will not want the IP address to change.
IP Address Pool	The DHCP IP Address Pool is the range of IP addresses set aside for dynamic assignment to the computers on your network.
Start IP	This field indicates the first of the contiguous IP addresses in the IP address pool.
End IP	This field indicates the last of the contiguous IP addresses in the IP address pool.
Domain Name	The domain name is the name you assign to your network.

Wireless

The Barricade 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 to enable the wireless function, define the radio channel, the SSID, and the security options.



Wireless Settings

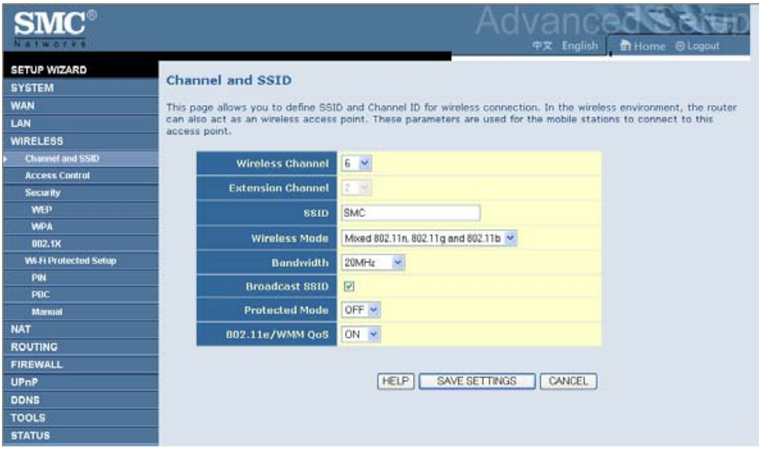
The router can be quickly configured as an wireless access point for roaming clients by setting the service set identifier (SSID) and channel number. It also supports data encryption and client filtering.

Enable or disable Wireless module function : ● Enable ○ Disable

Check **Enable** and click **SAVE SETTINGS**.

Channel and SSID

You must specify a common radio channel and SSID (Service Set ID) to be used by the Barricade and all of its wireless clients. Be sure you configure all of its clients to the same values.



Channel and SSID

This page allows you to define SSID and Channel ID for wireless connection. In the wireless environment, the router can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.

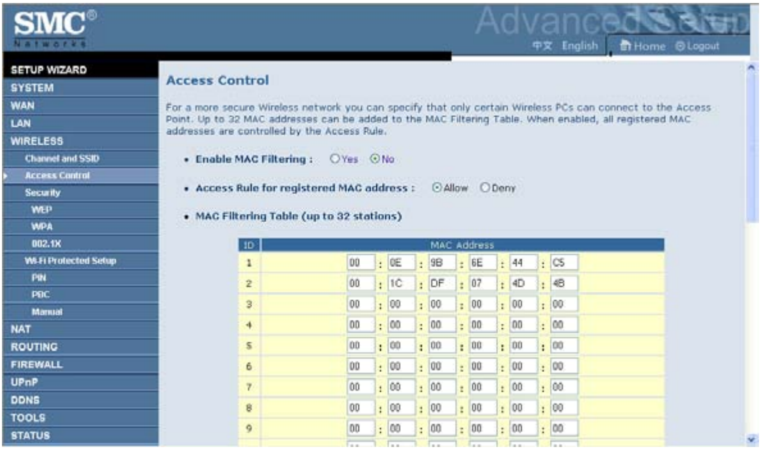
Wireless Channel	6
Extension Channel	2
SSID	SMC
Wireless Mode	Mixed 802.11n, 802.11g and 802.11b
Bandwidth	20MHz
Broadcast SSID	☑
Protected Mode	OFF
802.11e/WMM QoS	ON

Parameter	Description
Wireless 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 Barricade and all of its wireless clients. The Barricade will automatically assign itself a radio channel, or you may select one manually.
Extension Channel	Setting the Bandwith Mode as 20/40MHz allows you to use this extension channel as the secondary channel for doubling the bandwith of your wireless network.
SSID	Service Set ID. The SSID must be the same on the Barricade and all of its wireless clients. (Default: SMC)
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
Bandwidth	• 20MHz: Sets the operation bandwidth as 20 MHz. • 20/40MHz: Allows automatic detection of the operation bandwidth between 20 MHz and 40 MHz. Choosing the bandwidth mode as 20/40MHz allows you to use the extension channel.
Broadcast SSID	Enable or disable the broadcasting of the SSID. Disabling SSID broadcast will provide increased security by hiding the SSID of your wireless network.
Protected Mode	Enabling this function to ensure the best performance of your 11n throughput in case there is a lot of interference from the 11g and 11b devices in the wireless network.
802.11e/WMM QoS	Enable or disable the use of QoS. The QoS (Quality of Service) function allows you to differentiate WMM (Wi-Fi Multimedia) traffic and provide it with high-priority forwarding service

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 Barricade.



Access Control

For a more secure Wireless network you can specify that only certain Wireless PCs can connect to the Access Point. Up to 32 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the Access Rule.

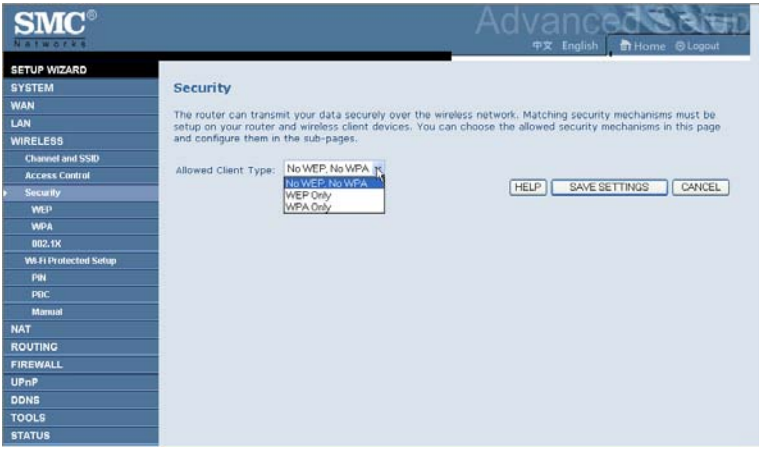
- Enable MAC Filtering : ○ Yes ● No
- Access Rule for registered MAC address : ● Allow ○ Deny
- MAC Filtering Table (up to 32 stations)

ID	MAC Address
1	00 : 0E : 9B : 6E : 44 : C5
2	00 : 1C : DF : 07 : 4D : 4B
3	00 : 00 : 00 : 00 : 00 : 00
4	00 : 00 : 00 : 00 : 00 : 00
5	00 : 00 : 00 : 00 : 00 : 00
6	00 : 00 : 00 : 00 : 00 : 00
7	00 : 00 : 00 : 00 : 00 : 00
8	00 : 00 : 00 : 00 : 00 : 00
9	00 : 00 : 00 : 00 : 00 : 00

Security

To make your wireless network safe, you should turn on the security function. The Barricade supports the following security mechanism:

- WEP
- WPA



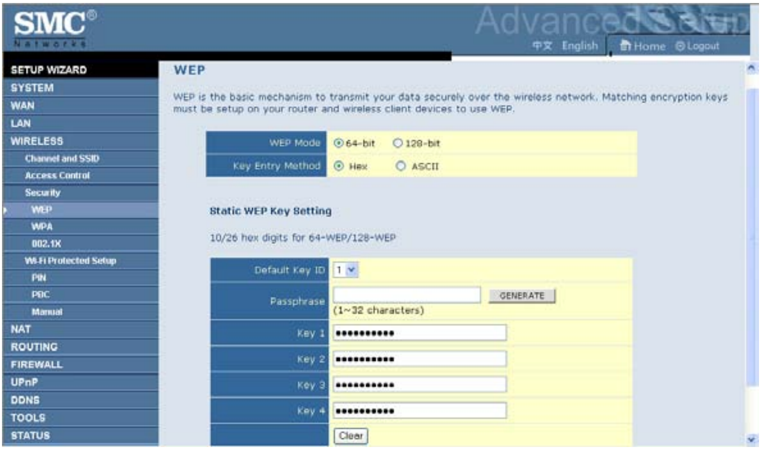
Security

The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages.

Allowed Client Type: No WEP, No WPA

WEP

If you want to use WEP to protect your wireless network, you need to set the same parameters for the Barricade and all your wireless clients.



WEP

WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your router and wireless client devices to use WEP.

WEP Mode ● 64-bit ○ 128-bit

Key Entry Method ● Hex ○ ASCII

Static WEP Key Setting

10/26 hex digits for 64-WEP/128-WEP

Default Key ID 1

Passphrase (1~32 characters)

Key 1 ••••••••••

Key 2 ••••••••••

Key 3 ••••••••••

Key 4 ••••••••••

Parameter	Description
WEP Mode	Select 64 bit or 128 bit key to use for encryption.
Key Entry Method	Select Hex or ASCII to use for encryption key.
Static WEP Key Setting	You may automatically generate encryption keys or manually enter the keys.

To generate the key automatically with passphrase, enter a string of characters and click the **GENERATE** button. Select the default key from the drop-down menu. Click **SAVE SETTINGS**.

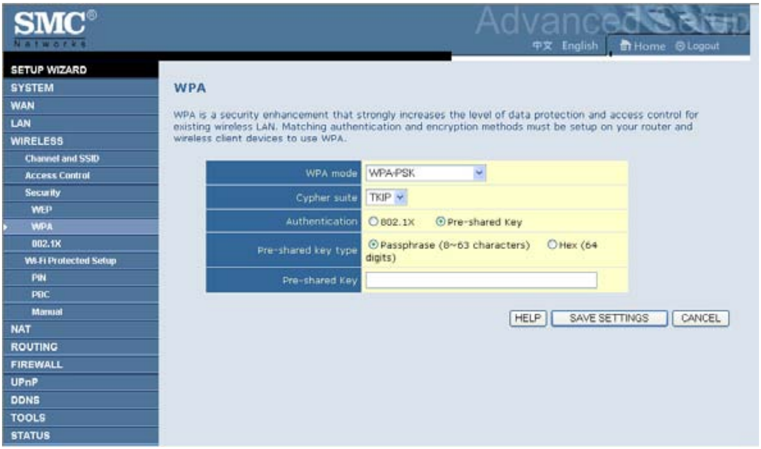
Note: The passphrase can consist of up to 32 alphanumeric characters.

To manually configure the encryption key, enter five hexadecimal pairs of digits for the 64-bit key, or enter 13 pairs for the 128-bit key.
(A hexadecimal digit is a number or letter in the range 0-9 or A-F.)

Note: WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

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.



WPA

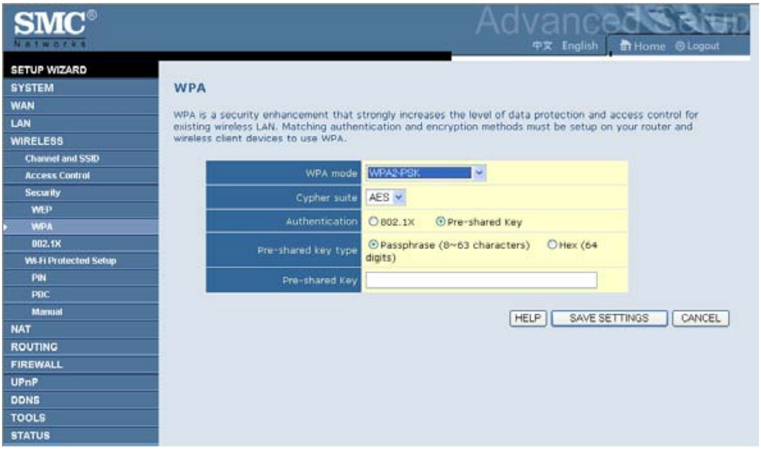
WPA is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your router and wireless client devices to use WPA.

WPA mode	WPA-PSK
Cypher suite	TKIP
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	

Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. See “802.1X” on page 4-34. • 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	Type in the key here.

WPA2

WPA2 is a product certification that is available through the Wi-Fi Alliance. WPA2 certifies that wireless equipment is compatible with the IEEE 802.11i standard. The WPA2 product certification formally replaces Wired Equivalent Privacy (WEP) and the other security features of the original IEEE 802.11 standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA.



WPA

WPA is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your router and wireless client devices to use WPA.

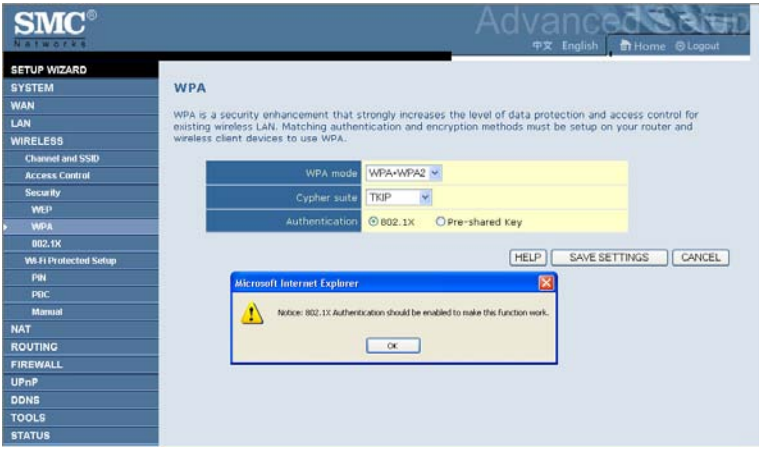
WPA mode	WPA2-PSK
Cypher suite	AES
Authentication	○ 802.1X ● Pre-shared Key
Pre-shared key type	● Passphrase (8~63 characters) ○ Hex (64 digits)
Pre-shared Key	

Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. See “802.1X” on page 4-34. • 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	Type in the key here.

WPA+WPA2

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.

Wi-Fi Protected Access 2 (WPA2) is a product certification that is available through the Wi-Fi Alliance. WPA2 certifies that wireless equipment is compatible with the IEEE 802.11i standard. The WPA2 product certification formally replaces Wired Equivalent Privacy (WEP) and the other security features of the original IEEE 802.11 standard. The goal of WPA2 certification is to support the additional mandatory security features of the IEEE 802.11i standard that are not already included for products that support WPA.



WPA

WPA is a security enhancement that strongly increases the level of data protection and access control for existing wireless LAN. Matching authentication and encryption methods must be setup on your router and wireless client devices to use WPA.

WPA mode: WPA•WPA2

Cypher suite: TKIP

Authentication: ● 802.1X ○ Pre-shared Key

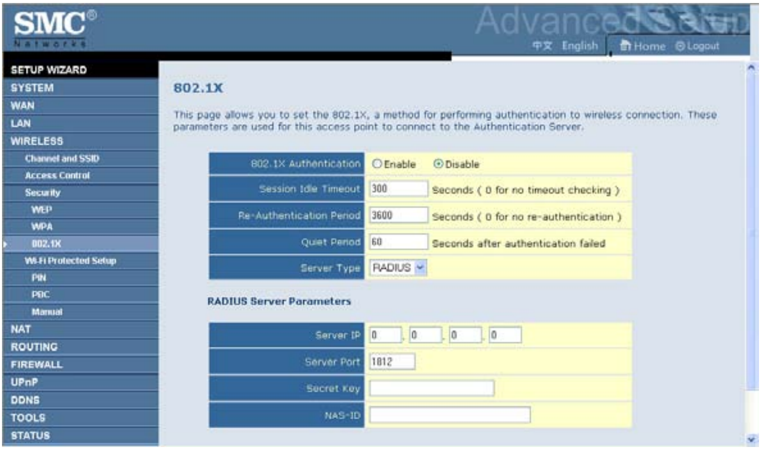
Microsoft Internet Explorer

Notice: 802.1X Authentication should be enabled to make this function work.

Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. See “802.1X” on page 4-34. • 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	Type in the key here.

802.1X

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



802.1X

This page allows you to set the 802.1X, a method for performing authentication to wireless connection. These parameters are used for this access point to connect to the Authentication Server.

802.1X Authentication	○ Enable ● Disable
Session Idle Timeout	300 Seconds (0 for no timeout checking)
Re-Authentication Period	3600 Seconds (0 for no re-authentication)
Quiet Period	60 Seconds after authentication failed
Server Type	RADIUS

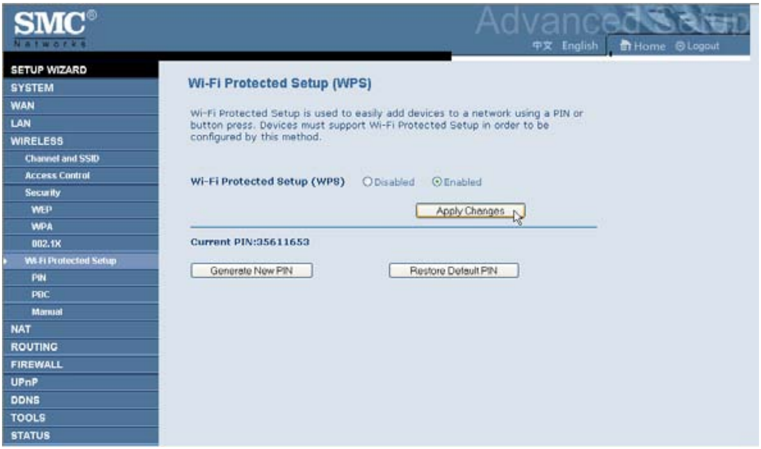
RADIUS Server Parameters

Server IP	0 . 0 . 0 . 0
Server Port	1812
Secret Key	
NAS-ID	

Parameter	Description
Authentication	Enable 802.1X authentication.
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 ADSL Router will wait between failed authentications.
Server Type	The Server Type of your authentication server is RADIUS.
RADIUS Server Parameters	
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

Wi-Fi Protected Setup (WPS)

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 an eight-digit PIN number and the Push Button Control (PBC).



Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

Wi-Fi Protected Setup (WPS) ○ Disabled ● Enabled

Current PIN:35611653

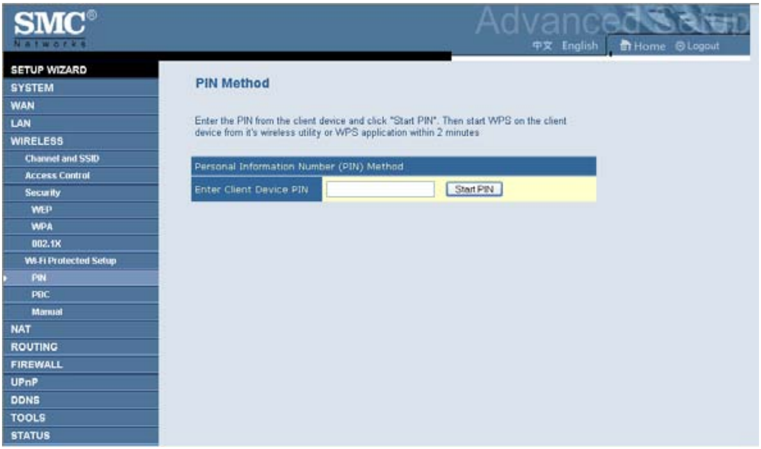
Check **Enable** and click **Apply Changes**.

Pressing **Generate New PIN** creates a new Current PIN number.

Pressing **Restore Default PIN** sets the PIN code to the factory default number.

Take the following steps for easy network security settings.

PIN Code Setup



PIN Method

Enter the PIN from 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

Personal Information Number (PIN) Method

Enter Client Device PIN [ ] Start PIN

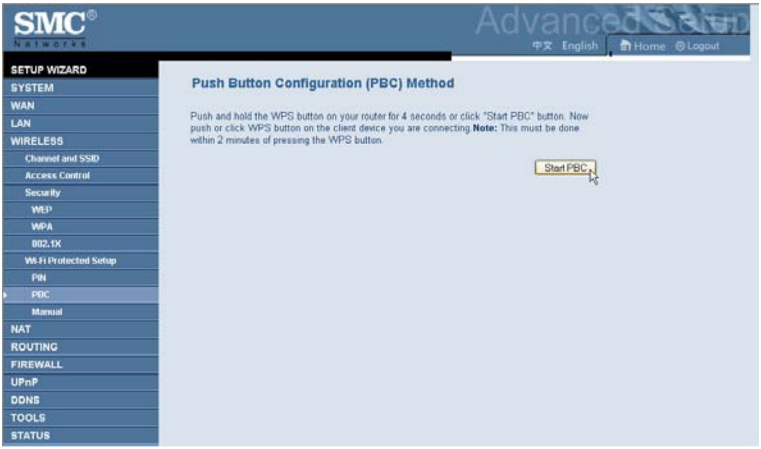
1. Power on your client device supporting WPS PIN code method.
2. Start WPS PIN process on client device. For instructions on how to do this refer to the user manual of the client device.
3. Enter the PIN code of client device.

Note: The PIN code is generally printed on the bottom of the unit or displayed in the configuration utility.

4. Click the **Start PIN** button on the screen.

Push Button Configuration (PBC) Method

To achieve successful WPS connection, you can use one of the following ways: (1) push and hold the WPS button on your Barricade, or (2) click the Start PBC button on this screen.



Push Button Configuration (PBC) Method

Push and hold the WPS button on your router for 4 seconds or click "Start PBC" button. Now push or click WPS button on the client device you are connecting **Note:** This must be done within 2 minutes of pressing the WPS button.

1. Power on your network devices such as an access point and client network devices.

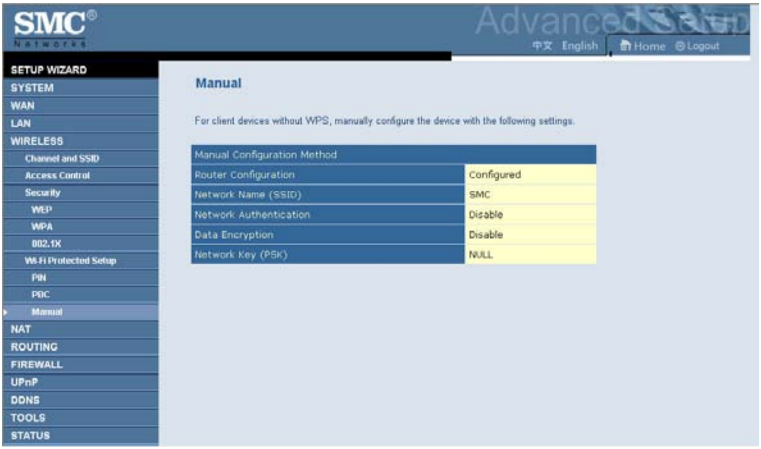
2. Press the WPS button for 4 seconds, or click the **Start PBC** button on the screen.

3. Press the WPS button or click the PBC button on your client devices of your network.

Note: This connection procedure must be done within 2 minutes after pressing the WPS button on the Barricade.

Manual

For client devices without WPS, manually configure the device as displayed on the screen.



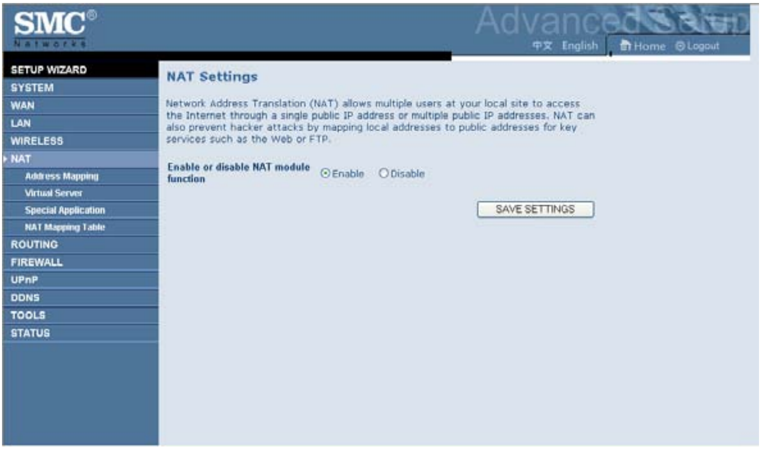
Manual

For client devices without WPS, manually configure the device with the following settings.

Manual Configuration Method	
Router Configuration	Configured
Network Name (SSID)	SMC
Network Authentication	Disable
Data Encryption	Disable
Network Key (PSK)	NULL

NAT

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



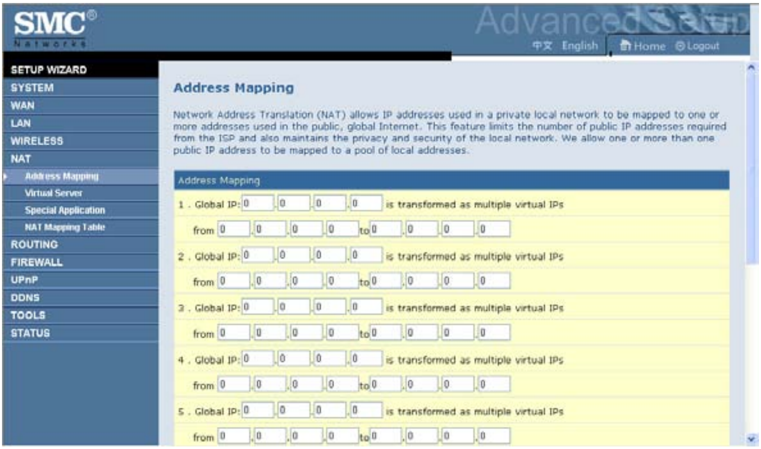
NAT Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Enable or disable NAT module function ⊙ Enable ○ Disable

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.



Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping

1 . Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

2 . Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

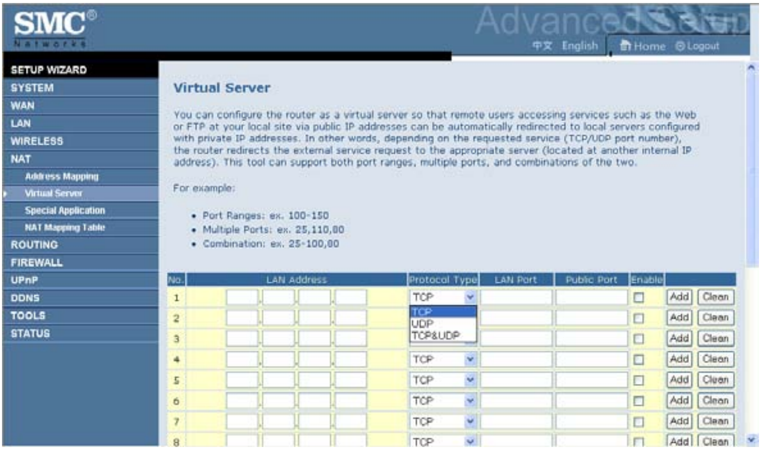
3 . Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

4 . Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

5 . Global IP: 0 . 0 . 0 . 0 is transformed as multiple virtual IPs
from 0 . 0 . 0 . 0 to 0 . 0 . 0 . 0

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).



Virtual Server

You can configure the router as a virtual server so that remote users accessing services such as the 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 router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:

- Port Ranges: ex. 100-150
- Multiple Ports: ex. 25,110,80
- Combination: ex. 25-100,80

No.	LAN Address	Protocol Type	LAN Port	Public Port	Enable	
1	. . .	TCP			□	Add Clean
2	. . .	TCP UDP TCP&UDP			□	Add Clean
3	. . .				□	Add Clean
4	. . .	TCP			□	Add Clean
5	. . .	TCP			□	Add Clean
6	. . .	TCP			□	Add Clean
7	. . .	TCP			□	Add Clean
8	. . .	TCP			□	Add Clean

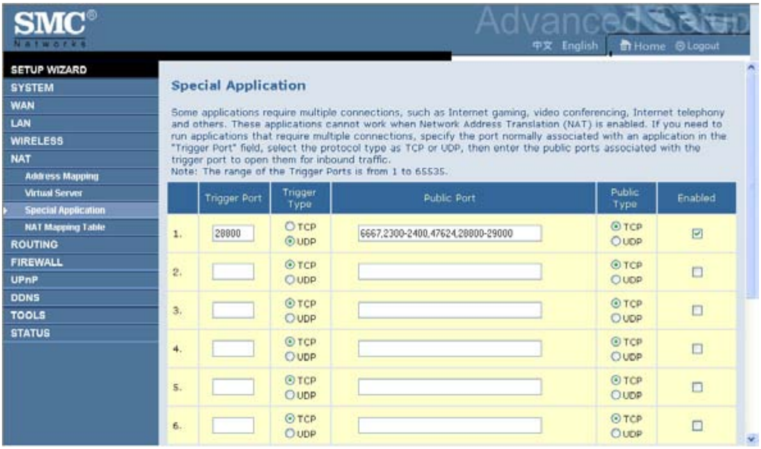
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they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

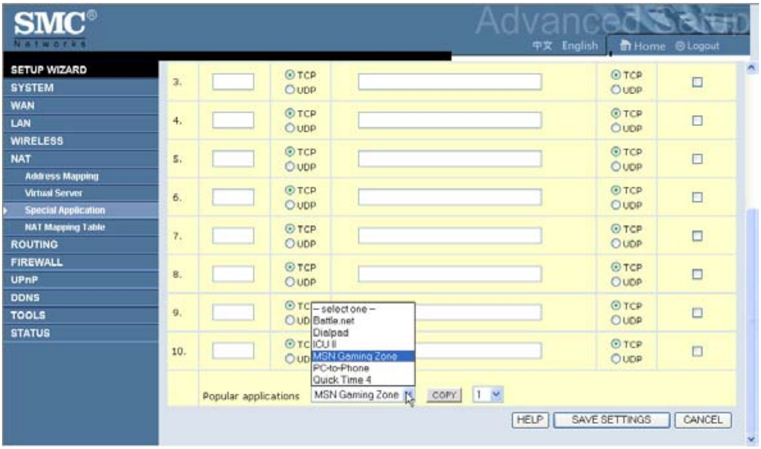
Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these screens to specify the additional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



Special Application

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.
Note: The range of the Trigger Ports is from 1 to 65535.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	28800	○ TCP ● UDP	6667,2300-2400,47624,28800-29000	● TCP ○ UDP	☑
2.		● TCP ○ UDP		● TCP ○ UDP	☐
3.		● TCP ○ UDP		● TCP ○ UDP	☐
4.		● TCP ○ UDP		● TCP ○ UDP	☐
5.		● TCP ○ UDP		● TCP ○ UDP	☐
6.		● TCP ○ UDP		● TCP ○ UDP	☐

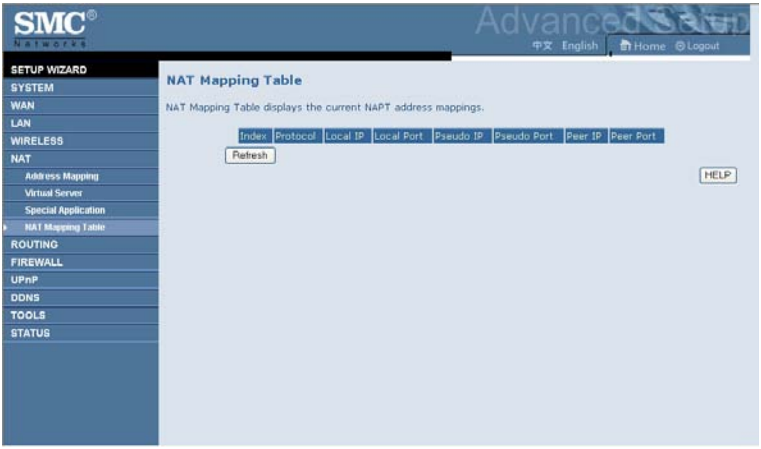


3.		● TCP ○ UDP		● TCP ○ UDP	☐
4.		● TCP ○ UDP		● TCP ○ UDP	☐
5.		● TCP ○ UDP		● TCP ○ UDP	☐
6.		● TCP ○ UDP		● TCP ○ UDP	☐
7.		● TCP ○ UDP		● TCP ○ UDP	☐
8.		● TCP ○ UDP		● TCP ○ UDP	☐
9.		● TC ○ UD		● TCP ○ UDP	☐
10.		● TC ○ UD		● TCP ○ UDP	☐

Popular applications MSN Gaming Zone 1

NAT Mapping Table

This screen displays the current NAPT (Network Address Port Translation) address mappings.



NAT Mapping Table

NAT Mapping Table displays the current NAPT address mappings.

Index	Protocol	Local IP	Local Port	Pseudo IP	Pseudo Port	Peer IP	Peer Port

NAT Mapping Table displays the current NAPT address mappings. The NAT address mappings are listed 20 lines per page, click the control buttons to move forwards and backwards. As the NAT mapping is dynamic, a Refresh button is provided to refresh the NAT Mapping Table with the mots updated values.

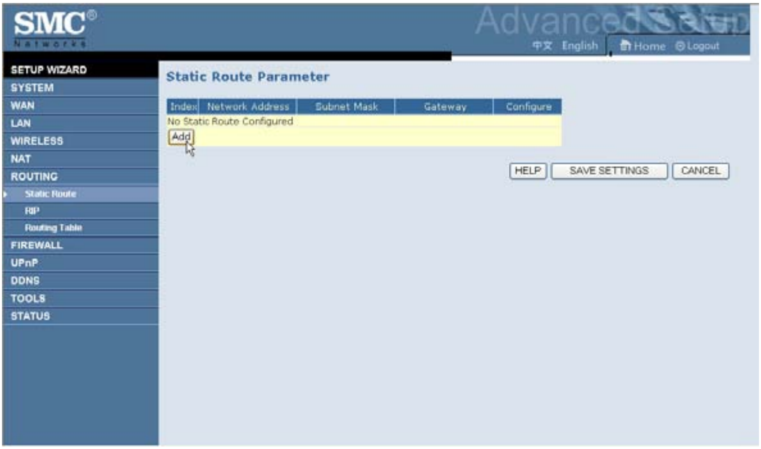
The content of the NAT Mapping Table is described as follows.

- Protocol - protocol of the flow.
- Local IP - local (LAN) host's IP address for the flow.
- Local Port - local (LAN) host's port number for the flow.
- Pseudo IP - translated IP address for the flow.
- Pseudo Port - translated port number for the flow.
- Peer IP - remote (WAN) host's IP address for the flow.
- Peer Port - remote (WAN) host's port number for the flow.

Routing

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

Static Route



Static Route Parameter

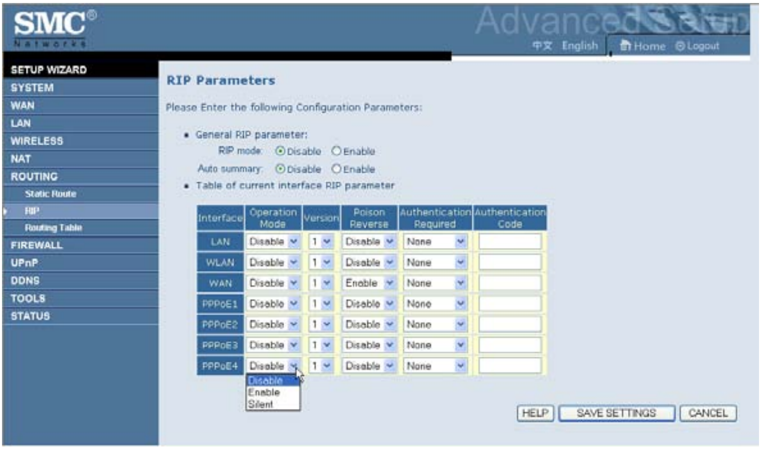
Index	Network Address	Subnet Mask	Gateway	Configure
No Static Route Configured				

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

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.



RIP Parameters

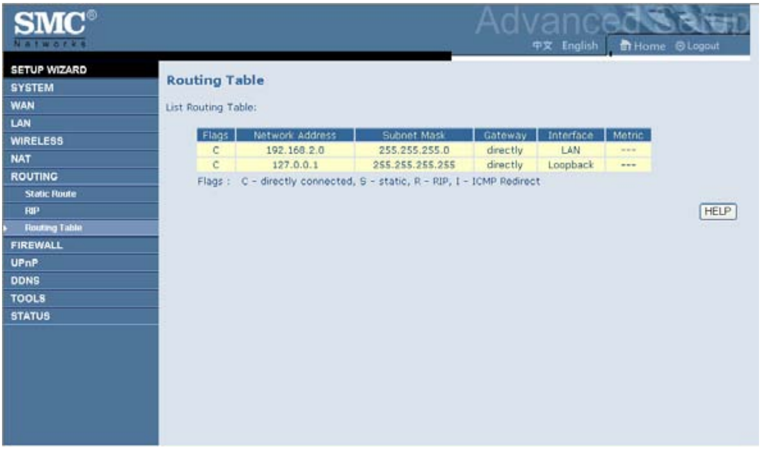
Please Enter the following Configuration Parameters:

- General RIP parameter:
  RIP mode: ● Disable ○ Enable
  Auto summary: ● Disable ○ Enable
- Table of current interface RIP parameter

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
LAN	Disable	1	Disable	None	
WLAN	Disable	1	Disable	None	
WAN	Disable	1	Enable	None	
PPPoE1	Disable	1	Disable	None	
PPPoE2	Disable	1	Disable	None	
PPPoE3	Disable	1	Disable	None	
PPPoE4	Disable	1	Disable	None	

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.
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.
Authentication Code	Password Authentication key.

Routing Table



Routing Table

List Routing Table:

Flags	Network Address	Subnet Mask	Gateway	Interface	Metric
C	192.168.2.0	255.255.255.0	directly	LAN	---
C	127.0.0.1	255.255.255.255	directly	Loopback	---

Flags : C - directly connected, S - static, R - RIP, I - ICMP Redirect

Parameter	Description

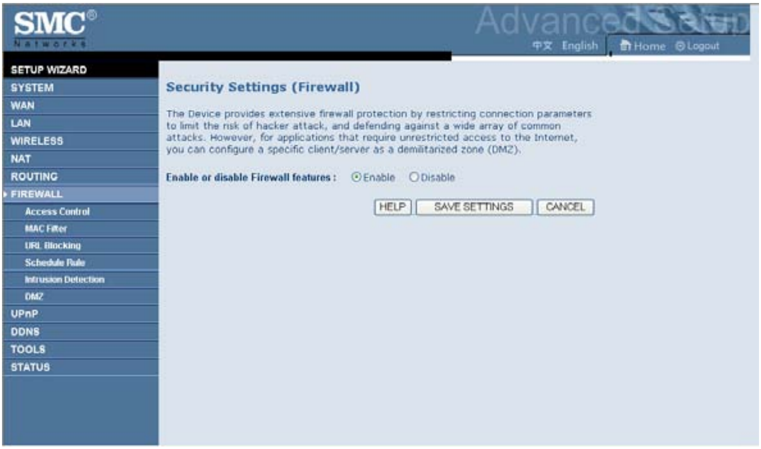
Flags	Indicates the route status:
	C = Direct connection on the same subnet.
	S = Static route.
	R = RIP (Routing Information Protocol) assigned route.
	I = ICMP (Internet Control Message Protocol) Redirect route.

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.



Security Settings (Firewall)

The Device provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ).

Enable or disable Firewall features : ● Enable ○ Disable

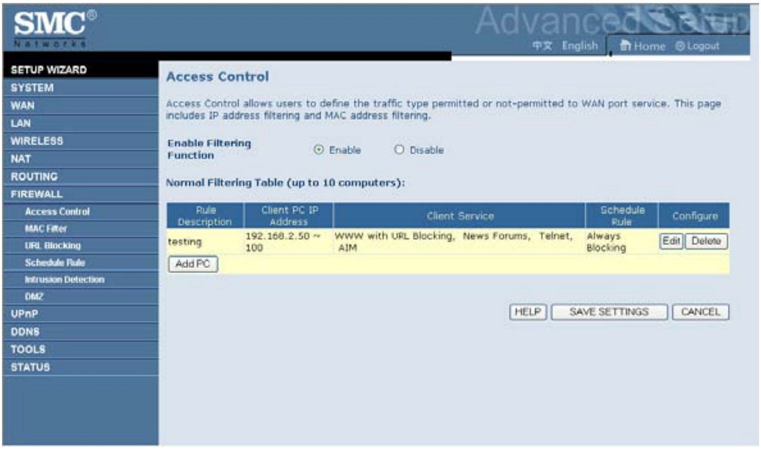
The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (For details see"Intrusion Detection," page 4-56.)

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.



Access Control

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

Enable Filtering Function ● Enable ○ Disable

Normal Filtering Table (up to 10 computers):

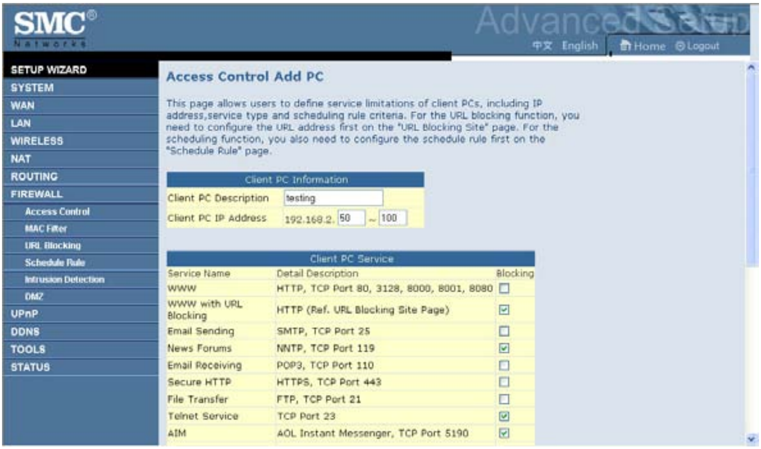
Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure
testing	192.168.2.50 ~ 100	WWW with URL Blocking, News Forums, Telnet, AIM	Always Blocking	Edit Delete
Add PC				

The following items are on the Access Control screen:

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 settings for client PC services.
3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

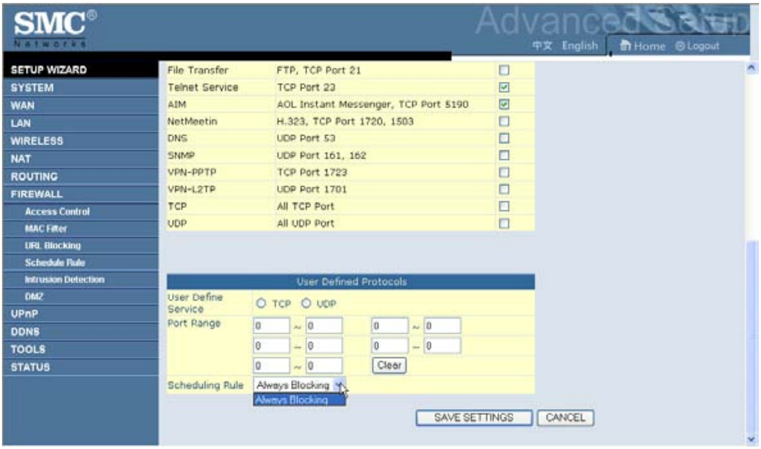


Access Control Add PC

This page allows users to define service limitations of client PCs, including IP address,service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you also need to configure the schedule rule first on the "Schedule Rule" page.

Client PC Information	
Client PC Description	testing
Client PC IP Address	192.168.2. 50 ~ 100

Client PC Service		
Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	□
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☑
Email Sending	SMTP, TCP Port 25	□
News Forums	NNTP, TCP Port 119	☑
Email Receiving	POP3, TCP Port 110	□
Secure HTTP	HTTPS, TCP Port 443	□
File Transfer	FTP, TCP Port 21	□
Telnet Service	TCP Port 23	☑
AIM	AOL Instant Messenger, TCP Port 5190	☑



File Transfer	FTP, TCP Port 21	□
Telnet Service	TCP Port 23	☑
AIM	AOL Instant Messenger, TCP Port 5190	☑
NetMeetin	H.323, TCP Port 1720, 1503	□
DNS	UDP Port 53	□
SNMP	UDP Port 161, 162	□
VPN-PPTP	TCP Port 1723	□
VPN-L2TP	UDP Port 1701	□
TCP	All TCP Port	□
UDP	All UDP Port	□

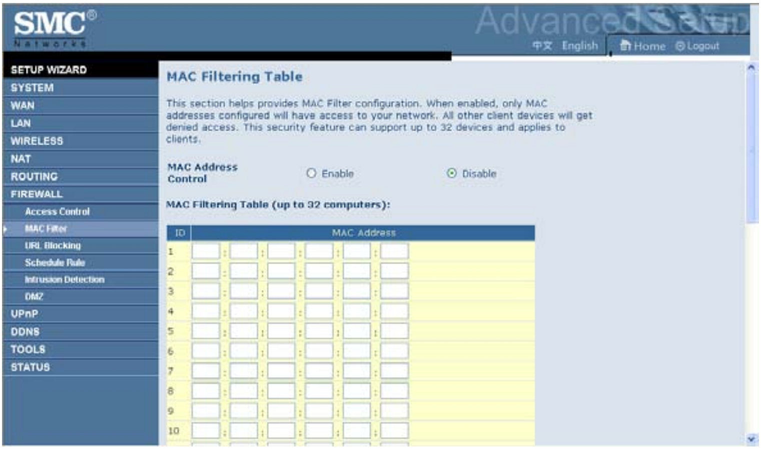
User Defined Protocols		
User Define Service	○ TCP ○ UDP	
Port Range	0 ~ 0	0 ~ 0
	0 ~ 0	0 ~ 0
	0 ~ 0	Clear
Scheduling Rule	Always Blocking Always Blocking	

SAVE SETTINGS CANCEL

MAC Filter

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

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



MAC Filtering Table

This section helps provides MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.

MAC Address Control ○ Enable ● Disable

MAC Filtering Table (up to 32 computers):

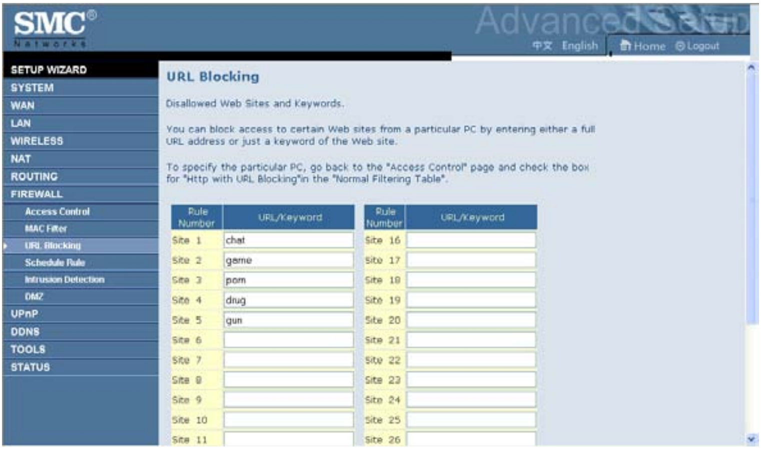
ID	MAC Address
1	: : : : :
2	: : : : :
3	: : : : :
4	: : : : :
5	: : : : :
6	: : : : :
7	: : : : :
8	: : : : :
9	: : : : :
10	: : : : :

1. MAC Address Control: select enable or disable.

2. 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.



URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

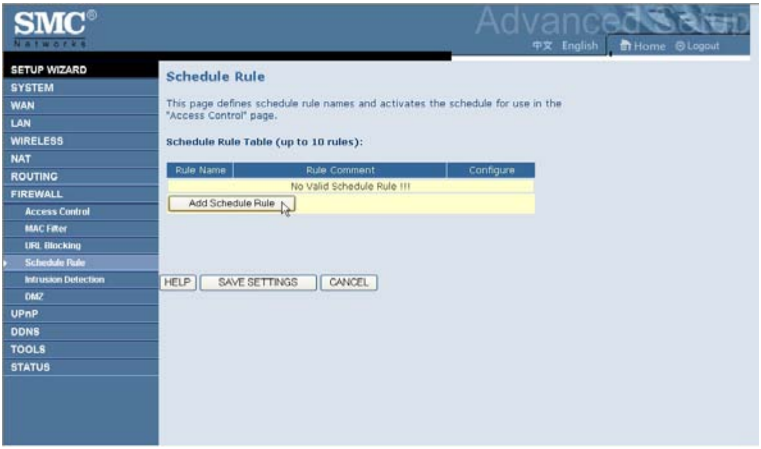
To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking"in the "Normal Filtering Table".

Rule Number	URL/Keyword	Rule Number	URL/Keyword
Site 1	chat	Site 16	
Site 2	game	Site 17	
Site 3	porn	Site 18	
Site 4	drug	Site 19	
Site 5	gun	Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	

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.



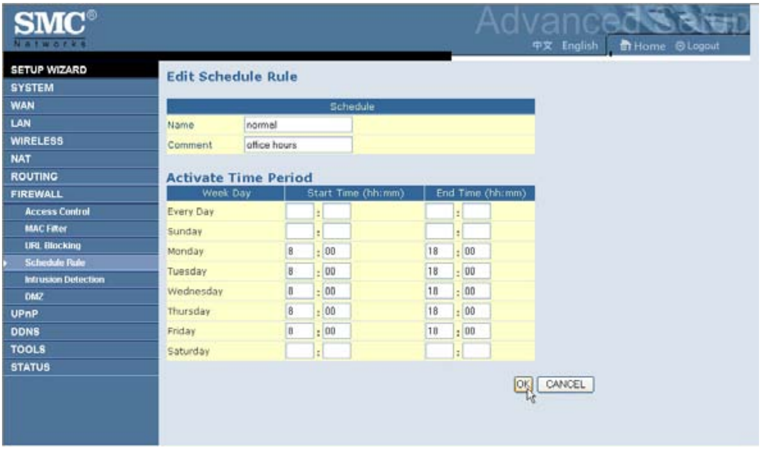
Schedule Rule

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Schedule Rule Table (up to 10 rules):

Rule Name	Rule Comment	Configure
	No Valid Schedule Rule !!!	

Follow these steps to add a schedule rule:



Edit Schedule Rule

Schedule	
Name	normal
Comment	office hours

Activate Time Period

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	:	:
Sunday	:	:
Monday	8 : 00	18 : 00
Tuesday	8 : 00	18 : 00
Wednesday	8 : 00	18 : 00
Thursday	8 : 00	18 : 00
Friday	8 : 00	18 : 00
Saturday	:	:

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.

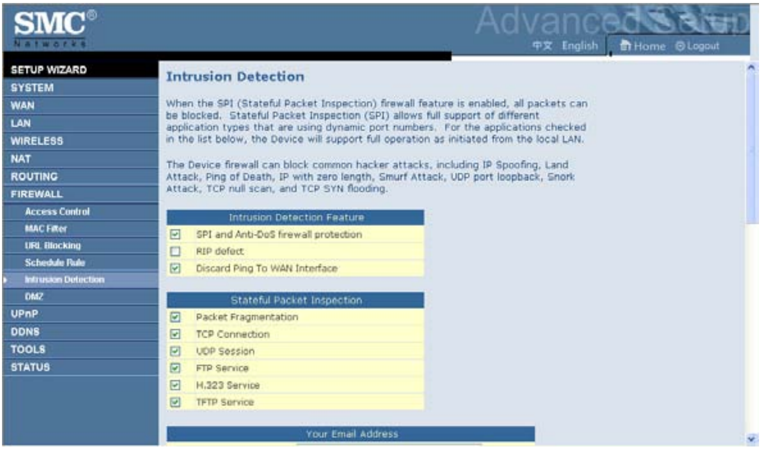
Intrusion Detection

- **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.



Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.

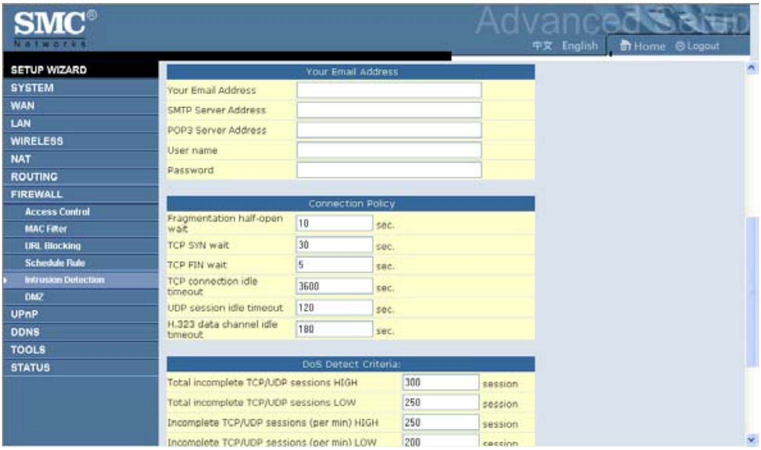
The Device firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

Intrusion Detection Feature	
☑	SPI and Anti-DoS firewall protection
□	RIP defect
☑	Discard Ping To WAN Interface

Stateful Packet Inspection	
☑	Packet Fragmentation
☑	TCP Connection
☑	UDP Session
☑	FTP Service
☑	H.323 Service
☑	TFTP Service

Your Email Address

Scroll down to view more information.



Your Email Address

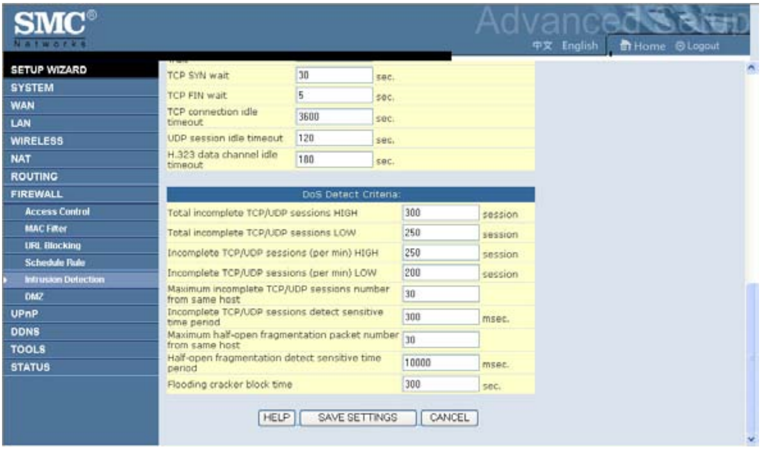
Your Email Address	
SMTP Server Address	
POP3 Server Address	
User name	
Password	

Connection Policy

Fragmentation half-open wait	10	sec.
TCP SYN wait	30	sec.
TCP FIN wait	5	sec.
TCP connection idle timeout	3600	sec.
UDP session idle timeout	120	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



TCP SYN wait	30	sec.
TCP FIN wait	5	sec.
TCP connection idle timeout	3600	sec.
UDP session idle timeout	120	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	30	
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.

- **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**

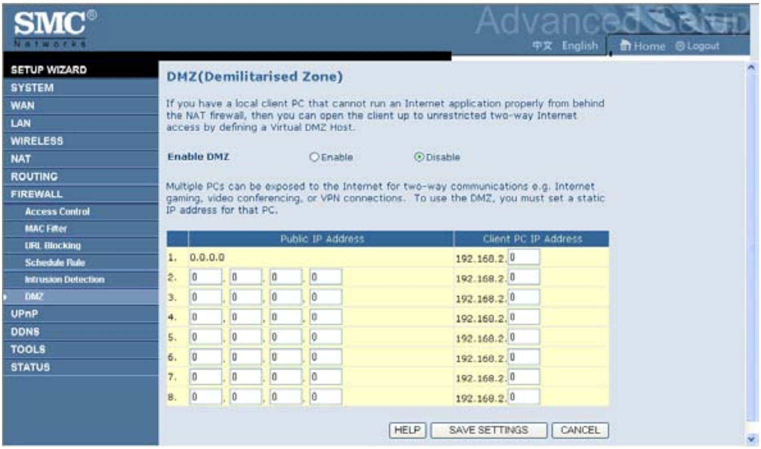
Set up DoS and port scan criteria in the spaces provided (as shown below).

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.



DMZ(Demilitarised Zone)

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

Enable DMZ ○ Enable ● Disable

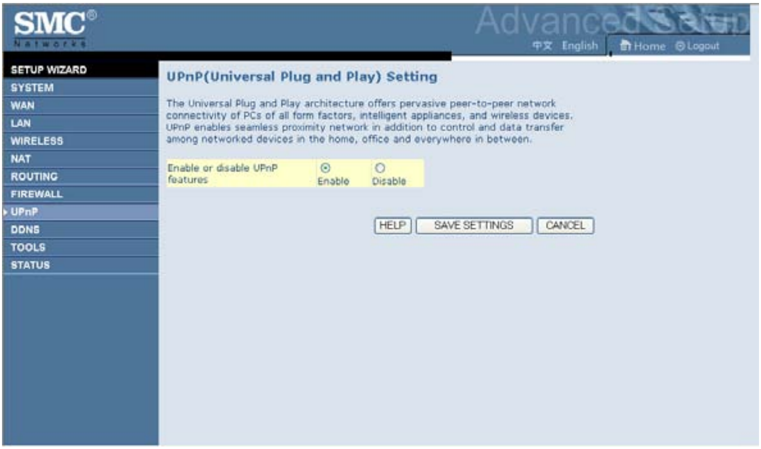
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

	Public IP Address	Client PC IP Address
1.	0.0.0.0	192.168.2. 0
2.	0 . 0 . 0 . 0	192.168.2. 0
3.	0 . 0 . 0 . 0	192.168.2. 0
4.	0 . 0 . 0 . 0	192.168.2. 0
5.	0 . 0 . 0 . 0	192.168.2. 0
6.	0 . 0 . 0 . 0	192.168.2. 0
7.	0 . 0 . 0 . 0	192.168.2. 0
8.	0 . 0 . 0 . 0	192.168.2. 0

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(Universal Plug and Play) Setting

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 home, office and everywhere in between.

Enable or disable UPnP features	● Enable	○ Disable

UPnP allows the device to automatically:

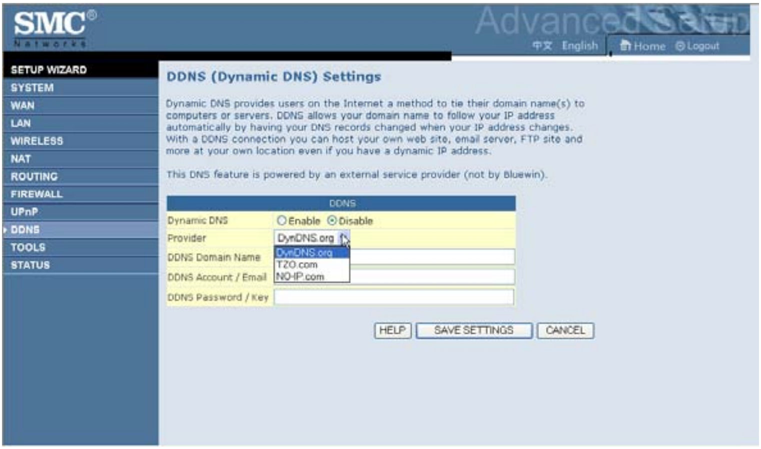
- join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices.

Check the **Enable** radio button to activate this function.

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 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.



DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes. 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.

This DNS feature is powered by an external service provider (not by Bluewin).

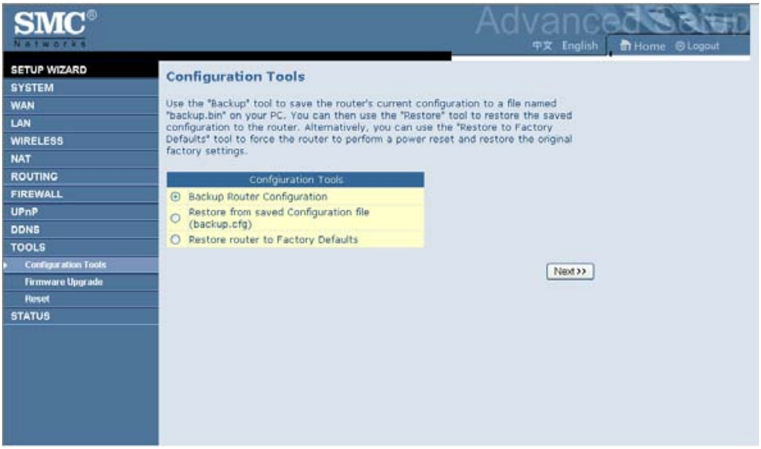
DDNS	
Dynamic DNS	○ Enable ● Disable
Provider	DynDNS.org DynDNS.org TZO.com NO-IP.com
DDNS Domain Name	
DDNS Account / Email	
DDNS Password / Key	

Tools

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

Configuration Tools

Choose a function and click **Next**.



Configuration Tools

Use the "Backup" tool to save the router's current configuration to a file named "backup.bin" on your PC. You can then use the "Restore" tool to restore the saved configuration to the router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the router to perform a power reset and restore the original factory settings.

Confgiuration Tools

● Backup Router Configuration
○ Restore from saved Configuration file (backup.cfg)
○ Restore router to Factory Defaults

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.

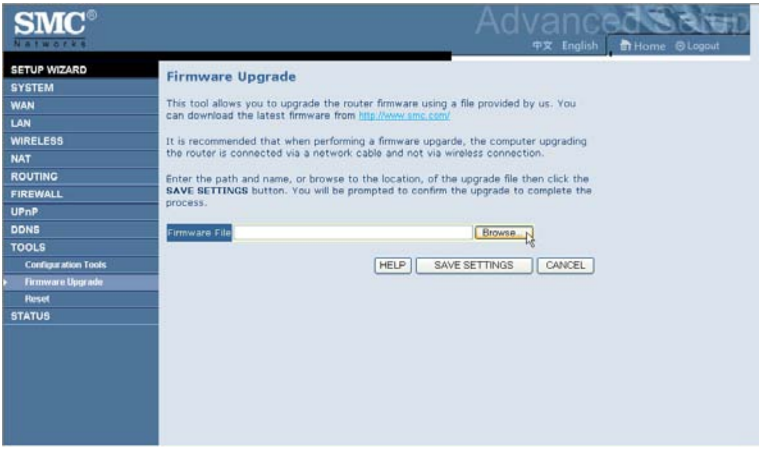
Firmware Upgrade

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 **SAVE SETTINGS**.

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



Firmware Upgrade

This tool allows you to upgrade the router firmware using a file provided by us. You can download the latest firmware from http://www.smc.com/

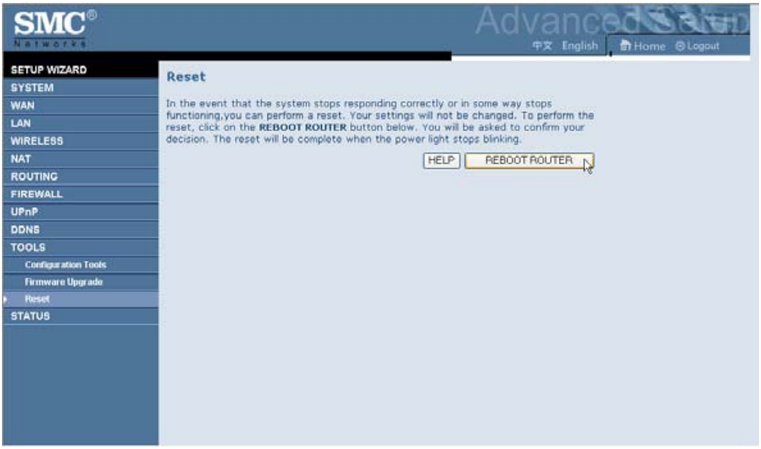
It is recommended that when performing a firmware upgarde, the computer upgrading the router is connected via a network cable and not via wireless connection.

Enter the path and name, or browse to the location, of the upgrade file then click the **SAVE SETTINGS** button. You will be prompted to confirm the upgrade to complete the process.

Firmware File

Reset

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



Reset

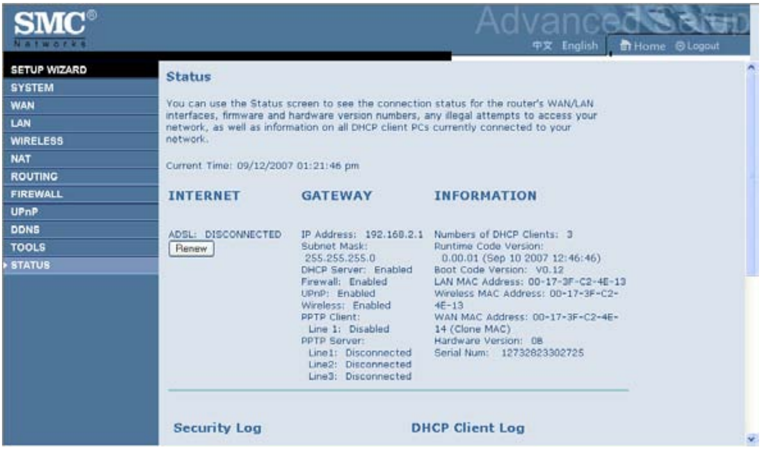
In the event that the system stops responding correctly or in some way stops functioning,you can perform a reset. Your settings will not be changed. To perform the reset, click on the **REBOOT ROUTER** button below. You will be asked to confirm your decision. The reset will be complete when the power light 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.



Status

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

Current Time: 09/12/2007 01:21:46 pm

INTERNET

ADSL: DISCONNECTED

GATEWAY

IP Address: 192.168.2.1
Subnet Mask:
255.255.255.0
DHCP Server: Enabled
Firewall: Enabled
UPnP: Enabled
Wireless: Enabled
PPTP Client:
Line 1: Disabled
PPTP Server:
Line1: Disconnected
Line2: Disconnected
Line3: Disconnected

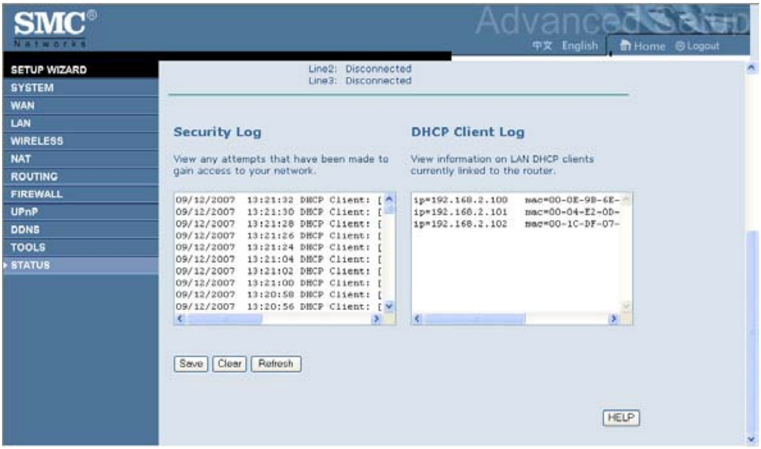
INFORMATION

Numbers of DHCP Clients: 3
Runtime Code Version:
0.00.01 (Sep 10 2007 12:46:46)
Boot Code Version: V0.12
LAN MAC Address: 00-17-3F-C2-4E-13
Wireless MAC Address: 00-17-3F-C2-4E-13
WAN MAC Address: 00-17-3F-C2-4E-14 (Clone MAC)
Hardware Version: 08
Serial Num: 12732823302725

Security Log

DHCP Client Log

Scroll down to view more information on the Status screen.



Line2: Disconnected
Line3: Disconnected

Security Log

View any attempts that have been made to gain access to your network.

```
09/12/2007  13:21:32 DHCP Client: [
09/12/2007  13:21:30 DHCP Client: [
09/12/2007  13:21:28 DHCP Client: [
09/12/2007  13:21:26 DHCP Client: [
09/12/2007  13:21:24 DHCP Client: [
09/12/2007  13:21:04 DHCP Client: [
09/12/2007  13:21:02 DHCP Client: [
09/12/2007  13:21:00 DHCP Client: [
09/12/2007  13:20:58 DHCP Client: [
09/12/2007  13:20:56 DHCP Client: [
```

DHCP Client Log

View information on LAN DHCP clients currently linked to the router.

```
ip=192.168.2.100   mac=00-0E-9B-6E-
ip=192.168.2.101   mac=00-04-E2-0D-
ip=192.168.2.102   mac=00-1C-DF-07-
```

The following items are included on the Status screen:

Parameter	Description
INTERNET	Displays WAN connection type and status.
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 ADSL Router, as well as the hardware version and serial number.
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 NT4/2000/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	
LAN 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, or the Barricade cannot ping any device on 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 six seconds) to restore the factory defaults.

Troubleshooting Chart	
Symptom	**Action**
Wireless Problems	
A wireless PC cannot associate with the Barricade.	• Make sure the wireless PC has the same SSID settings as the Barricade. See "Channel and SSID" on page 4-26. • You need to have the same security settings on the clients and the Barricade. See "Security" on page 4-29.
The wireless network is often interrupted.	• Move your wireless PC closer to the Barricade to find a better signal. If the signal is still weak, change the angle of the antenna. • There may be interference, possibly caused by microwave ovens or wireless phones. Change the location of the possible sources of interference or change the location of the Barricade. • Change the wireless channel on the Barricade. See "Channel and SSID" on page 4-26. • Check that the antenna, connectors, and cabling are firmly connected.
The Barricade cannot be detected by a wireless client.	• The distance between the Barricade and wireless PC is too great. • Make sure the wireless PC has the same SSID and security settings as the Barricade. See "Channel and SSID" on page 4-26 and "Security" on page 4-29.

Appendix B Cables

Ethernet Cable

Caution: Do not plug a phone jack connector into an RJ-45 port. For Ethernet connections, use only twisted-pair cables with RJ-45 connectors that conform to 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.

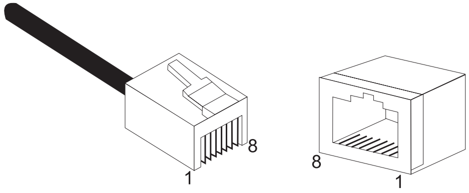


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Ethernet 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 10BASE-T/100BASE-TX 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	Tx+
2	Tx-
3	Rx+
6	Rx-

* 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-)

Appendix C Specifications

IEEE Standards

IEEE 802.3 10 BASE-T Ethernet
IEEE 802.3u 100 BASE-TX Fast Ethernet
IEEE 802.3, 802.3u, 802.11g, 802.1D

LAN Interface

4 RJ-45 10 BASE-T/100 BASE-TX ports
Auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half-duplex or full-duplex

WAN Interface

1 RJ-45 port

Indicator Panel

Power, WAN, Online, WLAN, LAN 1~4, WPS

Dimensions

188 x 133 x 33 mm (7.40 x 5.24 x 1.30 in)

Weight

0.285 kg (0.764 lbs)

Input Power

9 V 1 A

Power Consumption

8 Watts maximum

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Firewall – Client privileges, hacker prevention and logging, Stateful Packet Inspection

Virtual Private Network – PPTP, L2TP, IPSec pass-through, VPN pass-through

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 783 TFTP, RFC 1661 PPP, RFC 1866 HTML, RFC 2068 HTTP

Radio Features

Wireless RF module Frequency Band

802.11n Radio: 2.4GHz
802.11g Radio: 2.4GHz
802.11b Radio: 2.4GHz
USA - FCC
2412~2462MHz (Ch1~Ch11)
Canada - IC
2412~2462MHz (Ch1~Ch11)
Europe - ETSI
2412~2472MHz (Ch1~Ch13)
Japan - STD-T66/STD-33
2412~2484MHz (Ch1~Ch14)

Modulation Type

OFDM, CCK

Operating Channels IEEE 802.11n Compliant:

11 channels (US, Canada, Europe, Japan)

Operating Channels IEEE 802.11g Compliant:

11 channels (US, Canada)
13 channels (Europe, Japan)

Operating Channels IEEE 802.11b Compliant:

11 channels (US, Canada)
13 channels (Europe)
14 channels (Japan)

Standards Compliance

Safety

LVD

Environmental

CE Mark

Temperature

Operating 0 to 40 °C (32 to 104 °F)
Storage -40 to 70 °C (-40 to 158 °F)

Humidity

5% to 95% (non-condensing)

Vibration

IEC 68-2-36, IEC 68-2-6

Shock

IEC 68-2-29

Drop

IEC 68-2-32

SMC®
Networks

TECHNICAL SUPPORT
From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: (800) SMC-4-YOU / (949) 679-8000
Fax: (949) 679-1481

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

INTERNET
E-mail address: techsupport@smc.com

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

World Wide Web
http://www.smc.com/

SMCWBR14S-N2