



SMC7904WBRA2

BARRICADE™ g

Wireless 4-port Annex A ADSL2/2+
Modem Router

USER GUIDE



54Mbps Wireless Router with built-in ADSL Modem

From SMC's line of award-winning connectivity solutions

SMC[®]

Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

April 2006

R.01 f/w 0.03

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

Copyright © 2006 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618
All rights reserved.

Trademarks:

SMC is a registered trademark; and Barricade is a trademark of SMC Networks, Inc. Other product and company names are trademarks or registered trademarks of their respective holders.

LIMITED WARRANTY

Limited Warranty Statement: SMC Networks, Inc. (“SMC”) warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 90-day limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavor to repair or replace any product returned under warranty within 30 days of receipt of the product.

The standard limited warranty can be upgraded to a Limited Lifetime* warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as the period of time during which the product is an “Active” SMC product. A product is considered to be “Active” while it is listed on the current SMC price list. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies. At that point, the obsolete product is discontinued and is no longer an “Active” SMC product. A list of discontinued products with their respective dates of discontinuance can be found at:

http://www.smc.com/index.cfm?action=customer_service_warranty.

All products that are replaced become the property of SMC. Replacement products may be either new or reconditioned. Any replaced or repaired product carries either a 30-day limited warranty or the remainder of the initial warranty, whichever is longer. SMC is not responsible for any custom software or firmware, configuration information, or memory data of Customer contained in, stored on, or integrated with any products returned to SMC pursuant to any warranty. Products returned to SMC should have any customer-installed accessory or add-on components, such as expansion modules, removed prior to returning the product for replacement. SMC is not responsible for these items if they are returned with the product.

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. For warranty claims within North America, please call our toll-free customer support number at (800) 762-4968. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

LIMITED WARRANTY

WARRANTIES EXCLUSIVE: IF AN SMC PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT OF THE PRODUCT IN QUESTION, AT SMC'S OPTION. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. SMC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. SMC SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), SHALL SMC BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF SMC OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR THE LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, WHICH MAY VARY FROM STATE TO STATE. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

* SMC will provide warranty service for one year following discontinuance from the active SMC price list. Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

COMPLIANCES

EC Conformance Declaration

SMC contact for these products in Europe is:

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

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

EN 300 328-1 December 2001 V1.3.1

EN 300 328-2 December 2001 V1.2.1

EN 301 489-1 September 2001 V1.4.1

EN 301 489-17 September 2000 V1.2.1

EN 60950 January 2000

CSA Statement

This unit is to be used with an external power adaptor of a Class 2 or level 3 type and Approved type suitable for use in the North America of equipment installation, having an output voltage rating of 12 V dc, and output current rating of 1.0A or equivalent.

Safety Compliance

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlusßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die 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 autorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
 - a. Netzkabel oder Netzstecker sind beschädigt.
 - b. Flüssigkeit ist in das Gerät eingedrungen.
 - c. Das Gerät war Feuchtigkeit ausgesetzt.
 - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden. Für einen Nennstrom bis 6 A und einem Gerätegewicht größer 3 kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75 mm² einzusetzen.

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

TABLE OF CONTENTS

Introduction	1-1
About the Barricade	1-1
Features and Benefits	1-1
Applications	1-2
Installation	2-1
Package Contents	2-1
System Requirements	2-2
Hardware Description	2-2
LED Indicators	2-4
ISP Settings	2-5
Connect the System	2-5
Connecting the ADSL Line	2-5
Connecting the network	2-6
Connecting the Power Adapter	2-7
Wall Mounting	2-7
Configuring Client PC	3-1
TCP/IP Configuration	3-2
Windows 98/Me	3-2
Disable HTTP Proxy	3-4
Obtain IP Settings from Your ADSL Router	3-6
Windows NT 4.0	3-7
Disable HTTP Proxy	3-9
Obtain IP Settings from Your Barricade	3-9
Windows 2000	3-11
Disable HTTP Proxy	3-12
Obtain IP Settings from Your Barricade	3-12
Windows XP	3-14
Disable HTTP Proxy	3-14
Obtain IP Settings from Your Barricade	3-14
Configuring Your Macintosh Computer	3-16
Disable HTTP Proxy	3-17

Configuring the ADSL Router	4-1
Navigating the Management Interface	4-2
Making Configuration Changes	4-3
Setup Wizard	4-4
Time Zone	4-4
Wireless Settings	4-5
ADSL Settings	4-6
Summary	4-7
ADSL Settings - Country or ISP Not Listed	4-9
Configuration Parameters	4-17
System	4-19
WAN	4-22
LAN	4-31
Wireless	4-34
NAT	4-45
Routing	4-50
Firewall	4-54
SNMP	4-67
UPnp	4-69
QOS	4-70
ADSL	4-73
DDNS	4-76
Tools	4-77
Status	4-82
Finding the MAC address of a Network Card	4-85
Windows NT4/2000/XP	4-85
Macintosh	4-85
Linux	4-85

Troubleshooting	A-1
Cables	B-1
Ethernet Cable	B-1
Specifications	B-1
Wiring Conventions	B-1
RJ-45 Port Connection	B-2
Pin Assignments	B-3
Specifications	C-1

CHAPTER 1

INTRODUCTION

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

About the Barricade

The Barricade provides Internet access to multiple users by sharing a single-user account. Support is provided for both wired and wireless devices. New technology provides wireless security via Wired Equivalent Privacy (WEP) encryption and MAC address filtering. It is simple to configure and can be up and running in minutes.

Features and Benefits

- Built-in ADSL2/2+ modem - supports download speeds up to 24Mbps
- Local network connection via four 10/100 Mbps Ethernet ports
- Built-in IEEE802.11g 54Mbps Wireless Access Point (AP)
- 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, e-mail, and Telnet)
- VLAN and QoS (Quality of Service) support
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP

Applications

Many advanced networking features are provided by the Barricade:

- **Wireless and Wired LAN**

The Barricade provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11g compatible devices, making it easy to create a network in small offices or homes.

- **Internet Access**

This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the Barricade includes built-in clients for these protocols, eliminating the need to install these services on your computer.

- **Shared IP Address**

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. WEP (Wired Equivalent Privacy), SSID Broadcast disable, and MAC filtering provide security over the wireless network.

CHAPTER 2

INSTALLATION

Before installing the ADSL2 Barricade™, verify that you have all the items listed under the Package Contents list. Also be sure that you have all the necessary cabling before installing the Barricade. After installing the Barricade, refer to “Configuring the ADSL Router” on page 4-1.

Package Contents

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

- SMC7904WBRA2 Barricade™ 54Mbps ADSL2/2+ router
- Power adapter
- One RJ-45 Cat-5 Ethernet cable
- One RJ-11 patch cable for connecting ADSL modem to splitter/phone line
- One Splitter for NE, UK and FR versions only
- Printed quick installation guide
- Documentation CD
- Warranty Registration Card

Immediately inform your dealer in the event of any incorrect, missing, or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

System Requirements

You must meet the following minimum requirements:

- ADSL Internet Service installed.
- 2.4GHz Wireless adapter or Ethernet Adapter installed on each PC.
- TCP/IP network protocols installed on each PC that will access the Internet.
- A Java enabled web browser such as Internet Explorer 5.5 or above, Netscape 4.7 or above, Mozilla 1.7 or above and Firefox 1.0 or above.

Hardware Description

The Barricade contains an integrated ADSL modem and connects to the Internet or to a remote site using its RJ-45 WAN port. It can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL provides up to 8 Mbps downstream and 1 Mbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 kbps upstream. ADSL2+ provides up to 24Mbps downstream and 1Mbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and 54 Mbps over the built-in wireless access point.

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

It also provides the following ports on the rear panel:

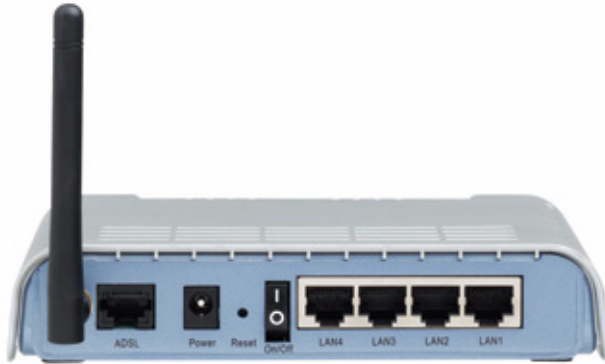


Figure 2-1. Rear Panel

Item	Description
ADSL Port	WAN port (RJ-11). Connect your ADSL line to this port.
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may damage the Barricade.
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 4-81.
On/Off switch	Use this switch to turn the Barricade ON and OFF.
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).

LED Indicators

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

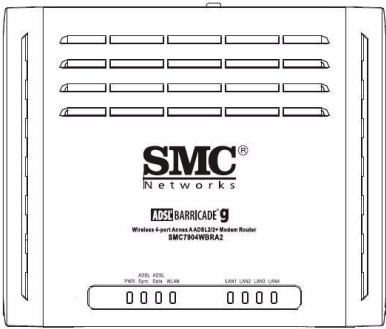


Figure 2-2. Top View

LED	Status	Description
PWR	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
ADSL Sync	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL Data	Flashing	Indicates ADSL port is sending or receiving data.
	Off	No data is being transferred.
WLAN	Flashing	The WLAN port is sending or receiving data.
LAN1 to LAN4	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.

ISP Settings

Please collect the following information from your ISP before setting up the Barricade:

- ISP account user name and password
- Protocol, encapsulation and VPI/VCI circuit numbers
- DNS server address
- IP address, subnet mask and default gateway (for fixed IP users only)

Connect the System

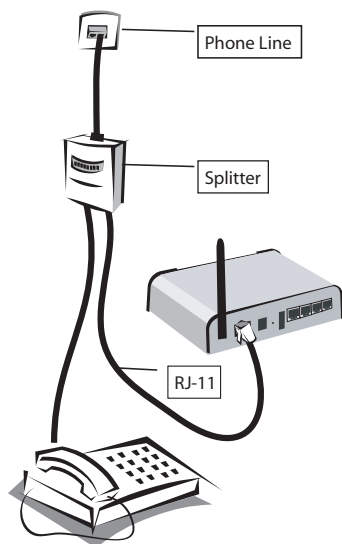
The Barricade can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the Barricade away from any heating devices.
- Do not place the Barricade in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the Barricade.

Connecting the ADSL Line

Connect the splitter to the phone line and the phone to the phone port of the splitter. Using the black RJ-11 cable provided connect the ADSL port of the Barricade to the ADSL port of the splitter. Refer to the below illustration.



The splitter is required for connecting your Barricade and phone to the same phone line. If you have a dedicated phone line for ADSL connect the Barricade directly to the phone line.

Note: To prevent high frequency ADSL signals interfering with telephone calls, each phone must be connected to the same phone line through a splitter (also known as an ADSL microfilter).

Connecting the network

Using the grey RJ-45 cable provided connect LAN port of the Barricade to the network card of your computer or other network device, e.g., hub or switch. The corresponding LAN LED will illuminate green to indicate good link.

Connecting the Power Adapter

Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet. Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to “Troubleshooting” on page A-1.

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

Wall Mounting

There are 2 slots on the underside of the Barricade that can be used for wall mounting. The distance between the 2 slots is 120 mm.

You will need 2 suitable screws, the diameter would be 4.4 mm, to wall mount the Barricade.

To wall mount the unit:

1. Determine where you want to mount the Barricade.
2. Drill two holes into the wall. Make sure the holes are 120 mm apart.
3. Insert a screw into each hole, and leave 5 mm of its head exposed.
4. Maneuver the Barricade so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Barricade down until the screws fit snugly into the wall-mount slots.

Note: When wall mounting the unit, ensure that it is within reach of the power outlet.

CHAPTER 3

CONFIGURING CLIENT PC

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the Barricade.

See:

“Windows 98/Me” on page 3-2

“Windows NT 4.0” on page 3-7

“Windows 2000” on page 3-11

“Windows XP” on page 3-14

or

“Configuring Your Macintosh Computer” on page 3-16

depending on your operating system.

TCP/IP Configuration

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

IP Address: 192.168.2.1

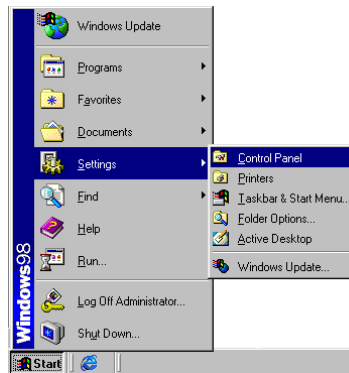
Subnet Mask: 255.255.255.0

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

Windows 98/Me

You may find that the instructions in this section do not exactly match your version of Windows. This is because these steps and screen shots were created from Windows 98. Windows Millennium Edition is similar, but not identical, to Windows 98.

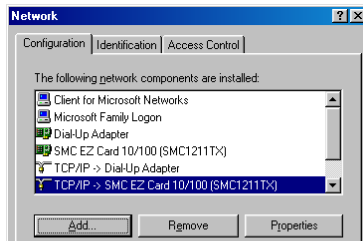
1. On the Windows desktop, click Start/Settings/Control Panel.



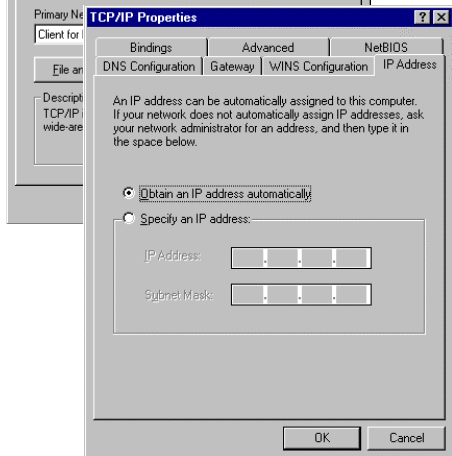
2. In Control Panel, double-click the Network icon.



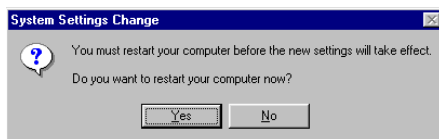
3. In the Network window, under the Configuration tab, double-click the TCP/IP item listed for your network card.



4. In the TCP/IP window, select the IP Address tab. If “Obtain an IP address automatically” is already selected, your computer is already configured for DHCP. If not, select this option.



- Windows may need your Windows 98/Me CD to copy some files. After it finishes copying, it will prompt you to restart your system. Click Yes and your computer will restart.




TCP/IP Configuration Setting

Primary DNS Server _____
Secondary DNS Server _____
Default Gateway _____
Host Name _____

Disable HTTP Proxy

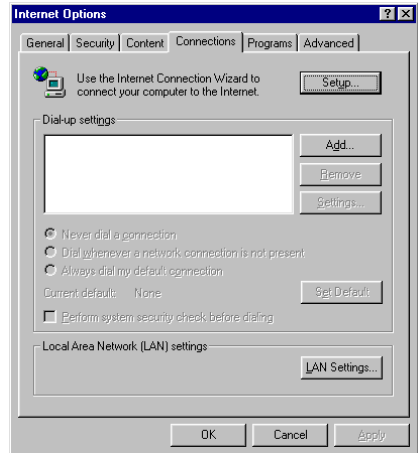
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

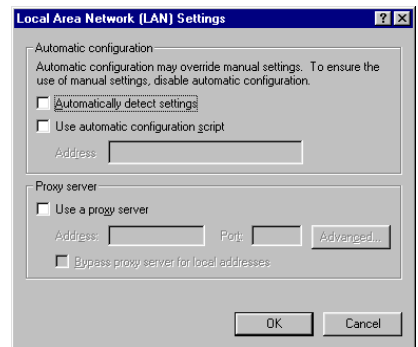
- Open Internet Explorer.
- Click the Stop  button, then click Tools/Internet Options.



3. In the Internet Options window, click the Connections tab. Next, click the LAN Settings... button.



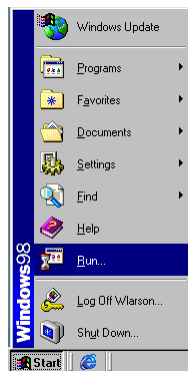
4. Clear all the check boxes.
5. Click OK, and then click OK again to close the Internet Options window.



Obtain IP Settings from Your ADSL Router

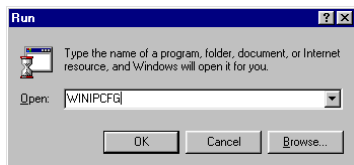
Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can also verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Run...



2. Type "WINIPCFG" and click OK.

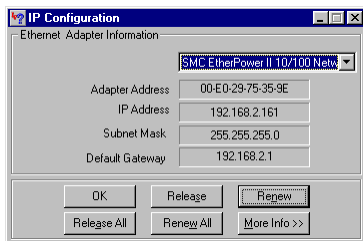
It may take a second or two for the IP Configuration window to appear.



3. In the IP Configuration window, select your network card from the drop-down menu. Click Release and then click Renew. Verify that your IP address is now

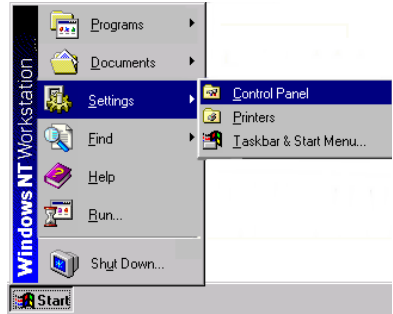
192.168.2.xxx, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**.

These values confirm that your Barricade is functioning. Click OK to close the IP Configuration window.

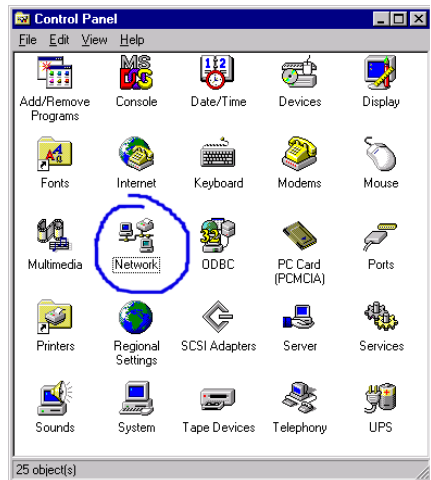


Windows NT 4.0

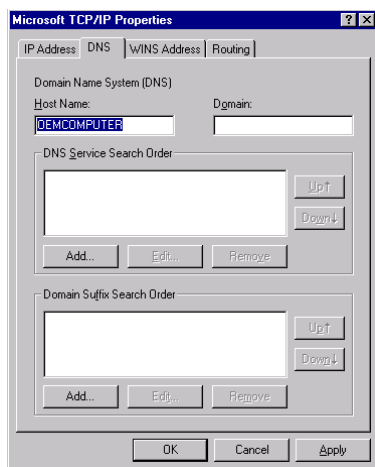
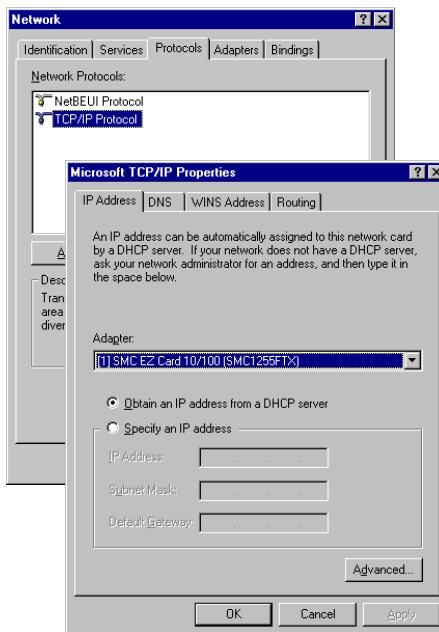
1. On the Windows desktop, click Start/Settings/Control Panel.



2. Double-click the Network icon.



3. In the Network window, Select the Protocols tab. Double-click TCP/IP Protocol.
4. When the Microsoft TCP/IP Properties window open, select the IP Address tab.
5. In the Adapter drop-down list, be sure your Ethernet adapter is selected.
6. If “Obtain an IP address automatically” is already selected, your computer is already configured for DHCP. If not, select this option and click “Apply.”
7. Click the DNS tab to see the primary and secondary DNS servers. Record these values, and then click “Remove.” Click “Apply”, and then “OK.”



8. Windows may copy some files, and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

TCP/IP Configuration Setting

Default Gateway	____.____.____.____
Primary DNS Server	____.____.____.____
Secondary DNS Server	____.____.____.____
Host Name	____.____.____.____

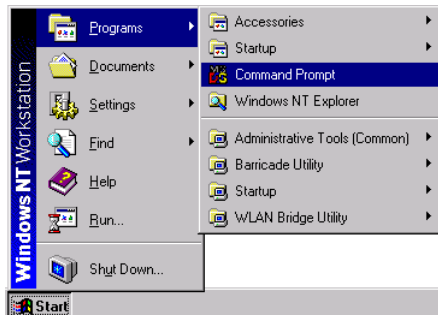
Disable HTTP Proxy

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. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

Obtain IP Settings from Your Barricade

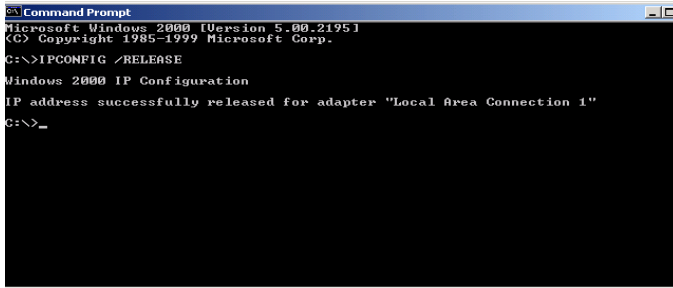
Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you will verify that you have configured your computer correctly.

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



CONFIGURING CLIENT PC

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



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

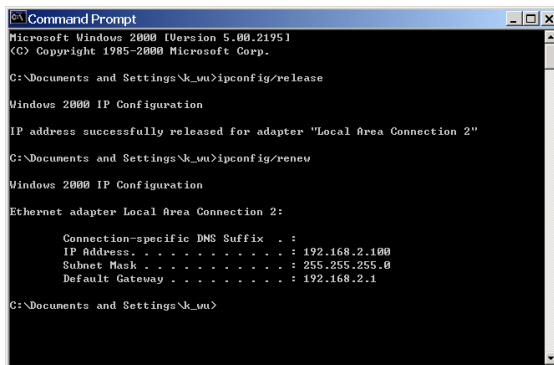
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 1"

C:\>_
```

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.



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

C:\Documents and Settings\k_yu>ipconfig/release

Windows 2000 IP Configuration

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

C:\Documents and Settings\k_yu>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

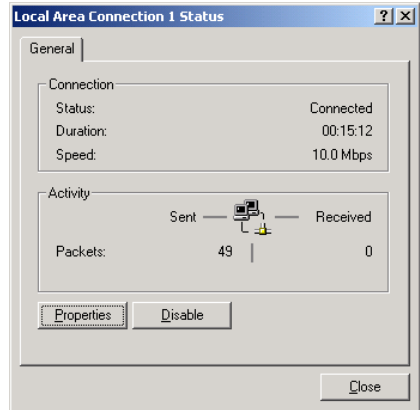
C:\Documents and Settings\k_yu>
```

4. Type “EXIT” and press the ENTER key to close the Command Prompt window.

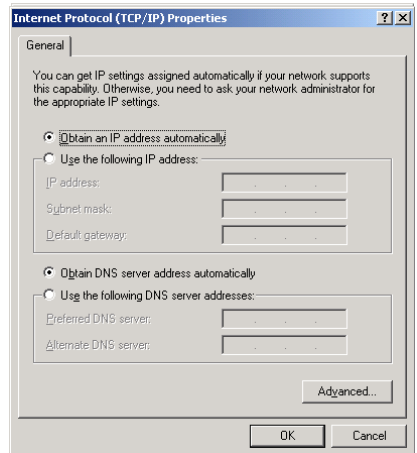
Your computer is now configured to connect to the Barricade.

Windows 2000

1. On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.
2. Click the icon that corresponds to the connection to your Barricade.
3. The connection status screen will open. Click Properties.



4. Double-click Internet Protocol (TCP/IP).
5. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.



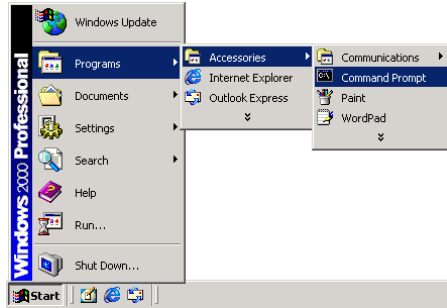
Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

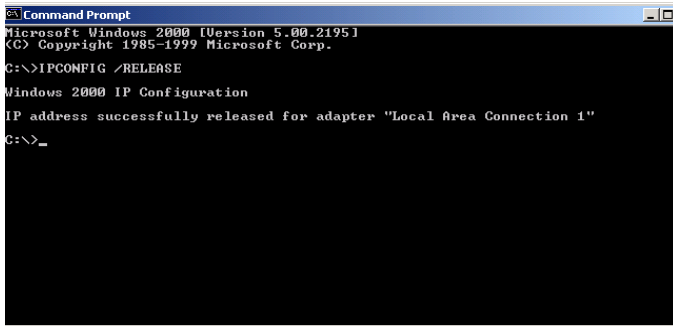
Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

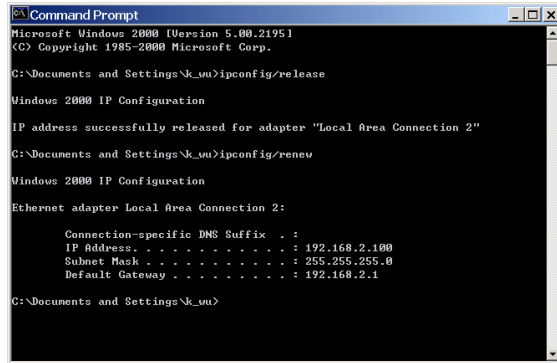
1. On the Windows desktop, click Start/Programs/Accessories/Command Prompt.



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



3. Type “IPCONFIG /RENEW” and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL Router is functioning.



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

C:\Documents and Settings\k_uu>ipconfig/release

Windows 2000 IP Configuration

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

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

4. Type “EXIT” and press the ENTER key to close the Command Prompt window.

Your computer is now configured to connect to the Barricade.

Windows XP

1. On the Windows desktop, click Start/Control Panel.
2. In the Control Panel window, click Network and Internet Connections.
3. The Network Connections window will open. Double-click the connection for this device.
4. On the connection status screen, click Properties.
5. Double-click Internet Protocol (TCP/IP).
6. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.

Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. Determine which browser you use and refer to “Internet Explorer” on page 3-4.

Obtain IP Settings from Your Barricade

Now that you have configured your computer to connect to your Barricade, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your Barricade, you can verify that you have configured your computer correctly.

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

2. In the Command Prompt window, type “IPCONFIG/RELEASE” and press the ENTER key.
3. Type “IPCONFIG /RENEW” and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL router is functioning.


Type “EXIT” and press the ENTER key to close the Command Prompt window.

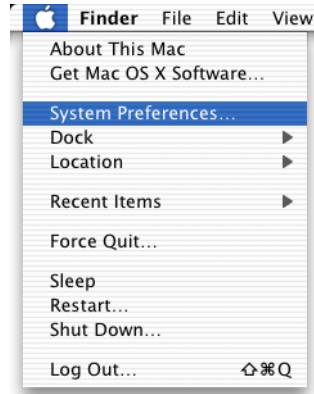
Your computer is now configured to connect to the Barricade.

Configuring Your Macintosh Computer

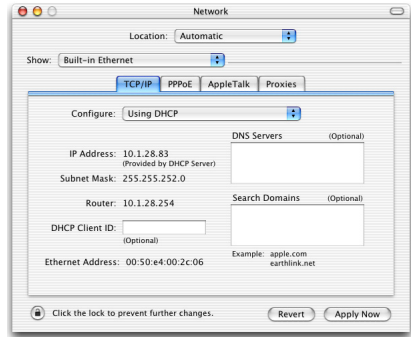
You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

1. Pull down the Apple Menu . Click System Preferences
2. Double-click the Network icon in the Systems Preferences window.



3. If “Using DHCP Server” is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option.



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

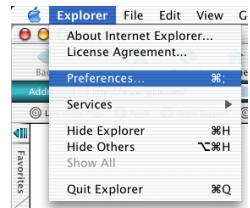
Now your computer is configured to connect to the Barricade.

Disable HTTP Proxy

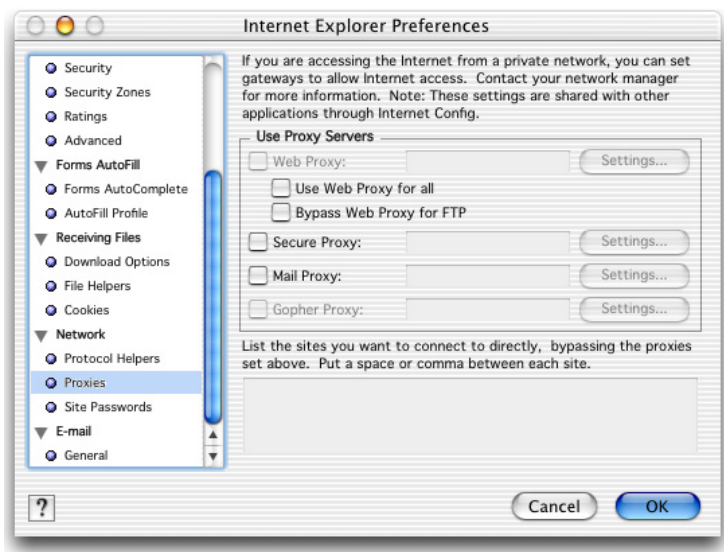
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

1. Open Internet Explorer and click 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.



CHAPTER 4

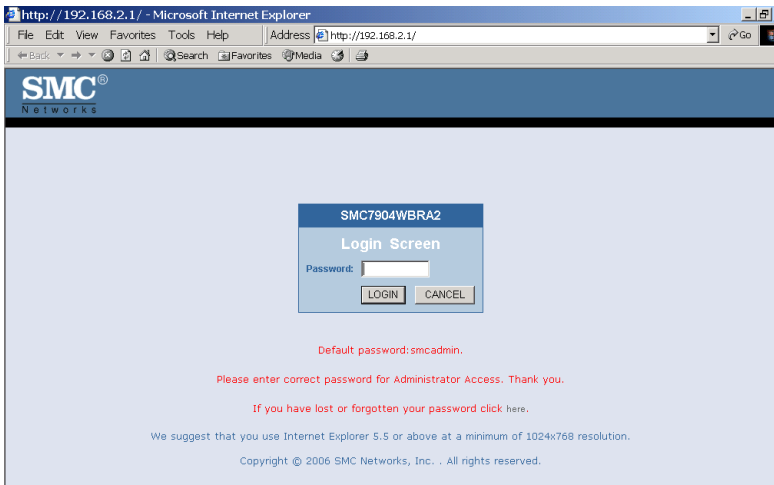
CONFIGURING THE ADSL ROUTER

After you have configured TCP/IP on a client computer, you can configure the Barricade using your web browser. Internet Explorer 5.5 or above, Netscape Navigator, Mozilla, Firefox and Opera are supported.

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

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

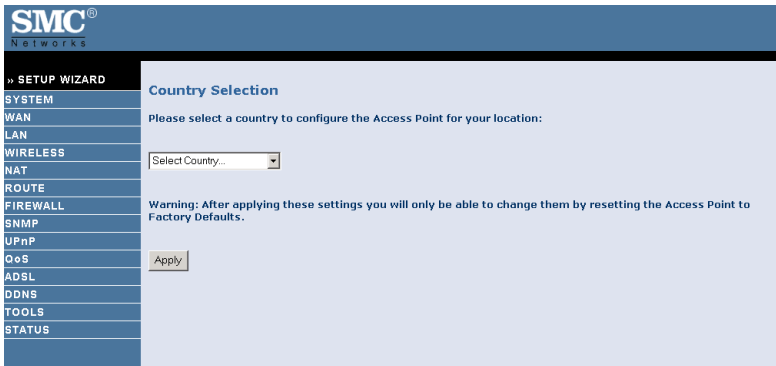
Note: Passwords can contain from 3~12 alphanumeric characters and are case sensitive.



Navigating the Management Interface

On initial configuration the first screen is Country Selection. Select your country from drop down list. This configures the correct channels for the wireless AP.

Note: The Country Selection screen only appears on initial configuration or when the Barricade is reset to factory defaults.



SMC®
Networks

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTE

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

Country Selection

Please select a country to configure the Access Point for your location:

Select Country...

Warning: After applying these settings you will only be able to change them by resetting the Access Point to Factory Defaults.

Apply

You will then see the Status screen appear. For details of this screen, please refer to page 4-82 of the manual.



The Setup Wizard is located on the top of the left hand side. Use the Setup Wizard for quick and easy configuration of your Internet connection and basic wireless settings. Go to “Setup Wizard” on page 4-4 for details.

MAKING CONFIGURATION CHANGES

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

Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.5 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”

Setup Wizard

TIME ZONE

Click on SETUP WIZARD and **NEXT**, 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.

SMC® Networks

Setup Wizard

Home Logout

1. Getting Started

2. Time Zone

3. Wireless Settings

4. ADSL Settings

5. Summary

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: 192.5.41.41 - North America

d. Click 'Next' to continue.

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

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.

Parameter	Description
SSID	Service Set ID. The SSID must be the same on the Barricade and all of its wireless clients.
SSID Broadcast	Enable or disable the broadcasting of the SSID.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have.
Channel	<p>The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients.</p> <p>The Barricade will automatically assign itself a radio channel, or you may select one manually.</p>

Click **NEXT** to continue.

ADSL Settings

Select your Country and Internet Service Provider. This will automatically configure the Barricade with the correct Protocol, Encapsulation and VPI/VCI settings for your ISP.

The screenshot shows the SMC Networks Setup Wizard interface. The top header includes the SMC Networks logo and a 'Setup Wizard' title. A navigation bar on the left lists five steps: 1. Getting Started, 2. Time Zone, 3. Wireless Settings, 4. ADSL Settings (highlighted), and 5. Summary. The main content area is titled '4. ADSL Settings' and contains instructions for configuring ADSL settings. It includes a note about selecting 'Other' if the country or ISP is not listed, and a list of steps: a. Select Country, b. Select ISP, c. Enter required values, and d. Click 'Next' to continue. Below the instructions are three dropdown menus for 'Country', 'Internet Service Provider', and 'Protocol', each with a placeholder text like '-- Select Country --'. At the bottom right are 'BACK' and 'NEXT' buttons.

SMC®
Networks

Setup Wizard

Home Logout

1. Getting Started
2. Time Zone
3. Wireless Settings
4. ADSL Settings
5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.
b. Select ISP.
c. Enter required values.
d. Click 'Next' to continue

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP.

Country -- Select Country --
Internet Service Provider -- Select ISP --
Protocol -- Select Protocol --

BACK NEXT

If your Country or Internet Service Provider is not listed in this screen, you will need to manually enter the settings. Go to “ADSL Settings - Country or ISP Not Listed” on page 4-9 in the manual for details.

If your ISP uses Protocols PPPoA or PPPoE you will need to enter the username and password supplied by your ISP.

If your ISP uses Protocol RFC1483 Routed you will need to enter the IP address, Subnet Mask, Default Gateway and DNS Server address supplied by your ISP.

Click **NEXT** to continue.

Summary

This screen shows a summary of the configuration parameters that you have made using the Setup Wizard.

SMC® Networks Setup Wizard

Home Logout

1. Getting Started
2. Wireless Settings
3. Time Zone
4. ADSL Settings
5. Summary

5. Summary

This page displays a summary of the values configured. Check the values are correct and click 'FINISH' to complete the set-up. To modify any values click 'BACK'.

After clicking 'FINISH' the Barricade will save settings & reboot. When complete the 'Status' page will be displayed.

- Wireless Parameters:**

SSID	SMC
SSID Broadcast	DISABLE
Wireless Mode	Mixed (11b+11g)
Channel	11
- Time Zone Parameters:**

Time Zone	(GMT-08:00)Pacific Time (US & Canada), Tijuana
NTP	ENABLE
Primary Server	132.163.4.102
Secondary Server	192.5.41.41
- ADSL operation mode (WAN):**

ISP	BigBlue
Protocol	PPPoE
VPI / VCI	8 / 35
AALS Encapsulation	LLC
- ISP Parameters:**

User Name	userjoe
Password	*****

BACK FINISH

Parameter	Description
Wireless Parameters	
SSID	This is the name of your wireless network.
SSID Broadcast	Broadcasting of your SSID is on/off.
Wireless Mode	802.11b only, 802.11g only or mixed mode.
Channel	The radio channel used for wireless communication.
Time Zone Parameters	
Time Zone	The time zone that you selected.
NTP	Network Time Protocol is enabled/disabled.
Primary Server	The time server that you selected, when Automatic Time Server Maintenance is enabled.
Secondary Server	The time server that you selected, when Automatic Time Server Maintenance is enabled.

Parameter	Description
ADSL Operation Mode (WAN)	
ISP	The type of ISP you have selected.
Protocol	Indicates the protocol used.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).
AAL5 Encapsulation	Shows the packet encapsulation type. Go to page 4-23 for a detailed description.
Network Layer Parameters (WAN)	
IP Address	WAN IP address (only displayed if you have static IP).
Subnet Mask	WAN subnet mask (only displayed if you have static IP).
Default Gateway	WAN gateway (only displayed if you have static IP).
DNS Server	The IP address of the DNS server.
ISP Parameters	
Username	The ISP assigned user name.
Password	The password (hidden).

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

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

ADSL Settings - Country or ISP Not Listed

If your Country or Internet Service Provider is not listed select “Others”. This will allow you to manually configure your ISP settings. For manual configuration you will need to know the Protocol, DNS Server, Encapsulation and VPI/VCI settings used by your ISP. If you have a Static IP address you will also need to know the IP address, Subnet Mask and Gateway address. Please contact your ISP for these details. After selecting “Others” you will need to select what Protocol your ISP uses from the drop-down menu.

SMC® Networks Setup Wizard

Home Logout

1. Getting Started
2. Time Zone
3. Wireless Settings
4. ADSL Settings
5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact you're ISP.

c. Enter required values.

d. Click 'Next' to continue

Country: Other
Internet Service Provider: Unknown ISP
Protocol: Select Protocol -

PPPoE
PPPoA
1483 Bridging(DHCP)
1483 Bridging(Static)
1483 Routing
Bridging
1483 Routing (DHCP)

BACK NEXT

PPPoE

SMC®
Networks

Setup Wizard

Home Logout

1. Getting Started

2. Time Zone

3. Wireless Settings

4. ADSL Settings

5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	PPPoE
VPI/VCI	8/35
Encapsulation	LLC
Username	userjoe
Password	*****
Confirm Password	*****

BACKNEXT

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

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

PPPoA

The screenshot shows the '4. ADSL Settings' step of the SMC Networks Setup Wizard. The left sidebar lists the steps: 1. Getting Started, 2. Time Zone, 3. Wireless Settings, 4. ADSL Settings (selected), and 5. Summary. The main content area has a title '4. ADSL Settings' and a description: 'This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.' Below this are instructions: 'a. Select Country.', 'b. Select ISP.', 'c. Enter required values.', and 'd. Click 'Next' to continue'. A note states: 'Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol and fill in blank fields. For correct values contact your ISP.' The configuration form includes fields for Country (set to 'Other'), Internet Service Provider (set to 'Unknown ISP'), Protocol (set to 'PPPoA'), VPI/VCI (set to '8/35'), Encapsulation (set to 'LLC'), Username (set to 'userjoe'), Password (masked with '*****'), and Confirm Password (masked with '*****'). At the bottom right are 'BACK' and 'NEXT' buttons.

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

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

1483 Bridging-DHCP

SMC®
Networks

Setup Wizard

Home Logout

1. Getting Started

2. Time Zone

3. Wireless Settings

4. ADSL Settings

5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact you're ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Bridging(DHCP)
DNS Server	
VPI/VCI	8 / 35
Encapsulation	LLC

BACKNEXT

Parameter	Description
DNS Server	Domain Name Servers are used to map a domain name (e.g., www.somesite.com) to the equivalent numerical IP address. Your ISP should provide the IP address of a Domain Name Server. Enter the address here.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by your ISP from the drop-down menu.

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

1483 Bridging-Static

SMC[®]
Networks

Setup Wizard

Home Logout

1. Getting Started
2. Time Zone
3. Wireless Settings
4. ADSL Settings
5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol and fill in blank fields. For correct values contact your ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Bridging(Static)
IP Address	0 0 0 0
Subnet Mask	
Default Gateway	
DNS Server	
VPI/VCI	8 / 35
Encapsulation	LLC

BACK NEXT

Parameter	Description
IP Address	Enter your ISP supplied static IP address here
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by your ISP from the drop-down menu.

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

1483 Routing

SMC®
Networks

Setup Wizard

Home Logout

1. Getting Started

2. Time Zone

3. Wireless Settings

4. ADSL Settings

5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Routing
IP Address	0.0.0.0
Subnet Mask	
Default Gateway	
DNS Server	
VPI/VCI	8 / 35
Encapsulation	LLC

BACKNEXT

Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by your ISP from the drop-down menu.

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

Bridging

SMC® Networks Setup Wizard

Home Logout

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact your ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	Bridging
Management IP Address	0.0.0.0
VPI/VC	8/35
Encapsulation	LLC

BACK NEXT

Parameter	Description
Management IP Address	This is the management IP address of the Barricade.
VPI/VC	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by your ISP from the drop-down menu.

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

1483 Routing-DHCP

SMC®
Networks

Setup Wizard

Home Logout

1. Getting Started

2. Time Zone

3. Wireless Settings

4. ADSL Settings

5. Summary

4. ADSL Settings

This page allows you to configure the ADSL settings. A predefined list of countries & Internet Service Providers (ISP) is available for easy configuration.

a. Select Country.

b. Select ISP.

Note: If Country or ISP is not listed select 'Other'. You will be required to manually select the Protocol & fill in blank fields. For correct values contact you're ISP.

c. Enter required values.

d. Click 'Next' to continue

Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Routing (DHCP)
DNS Server	
VPI/VCI	8 / 35
Encapsulation	LLC

BACKNEXT

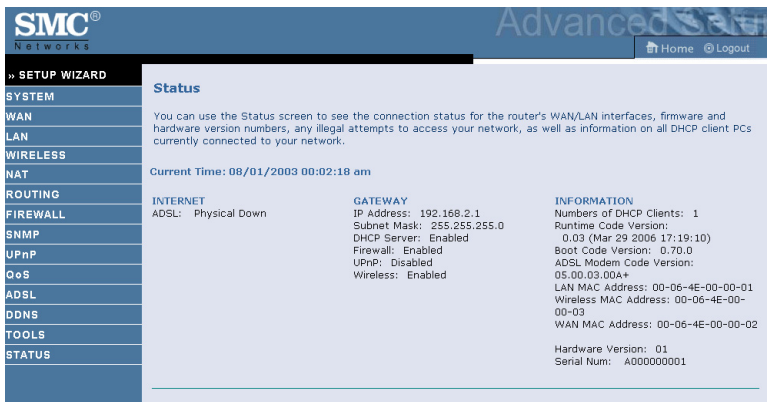
Parameter	Description
DNS Server	Enter the Domain Name Server address.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by your ISP from the drop-down menu.

Click **NEXT** to continue.

Go to “Summary” on page 4-7 in the manual for details about the settings.

Configuration Parameters

The left-hand side displays the main menu and the right-hand side shows descriptive information. There are 14 main menu items as described in the following table.



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

Menu	Description
QoS	Allows you to prioritize your network traffic.
ADSL	Sets the ADSL operation type and shows the ADSL status.
DDNS	Configures Dynamic DNS function.
Tools	Contains options to ping network connection, trace route, backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.
Status	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log.

SYSTEM

Time Zone

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

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with the following items: » SETUP WIZARD, SYSTEM, » Time Zone, » Password Settings, » Remote Management, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, CoS, ADSL, DDNS, TOOLS, and STATUS. The main content area is titled "Time Zone" and contains the following sections:

- Set Time Zone:** A text block stating "Use this setting to insure the time-based client filtering feature and system log entries are based on the correct localized time." Below this is a drop-down menu currently set to "(GMT-08:00)Pacific Time (US & Canada), Tijuana".
- Enable Daylight Savings:** A checkbox labeled "Enable Daylight Savings" which is currently unchecked.
- Start Daylight Savings Time:** Two drop-down menus set to "January" and "1".
- End Daylight Savings Time:** Two drop-down menus set to "January" and "1".
- Configure Time Server (NTP):** A text block stating "You can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet." Below this is a checked checkbox labeled "Enable Automatic Time Server Maintenance".
- Primary Server:** A drop-down menu set to "132.163.4.102 - North America".
- Secondary Server:** A drop-down menu set to "192.5.41.41 - North America".

At the bottom right of the form are three buttons: "HELP", "SAVE SETTINGS", and "CANCEL".

If daylight savings is applied in your area, check the box to **Enable Daylight Savings**. Select the start/end dates.

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

Password Settings

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

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

» Time Zone

» Password Settings

» Remote Management

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

Password Settings

Set a password to restrict management access to the router.

- Current Password :
- New Password:
- Re-Enter Password for Verification:

• Idle Time Out: Min
(Idle Time =0 : NO Time Out)

HELP SAVE SETTINGS CANCEL

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 five 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 remote host and click **SAVE SETTINGS**.

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with options: SETUP WIZARD, SYSTEM (selected), WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The SYSTEM menu is expanded, showing sub-options: Time Zone, Password Settings, and Remote Management (selected). The main content area is titled 'Remote Management' and contains the following text: '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.' Below this text are three input fields: 'Enabled' with a checked checkbox, 'Host Address' with a text box containing '0.0.0.0', and 'Port Number' with a text box containing '8080'. At the bottom right of the form are three buttons: 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

Note: If you check Enabled 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.

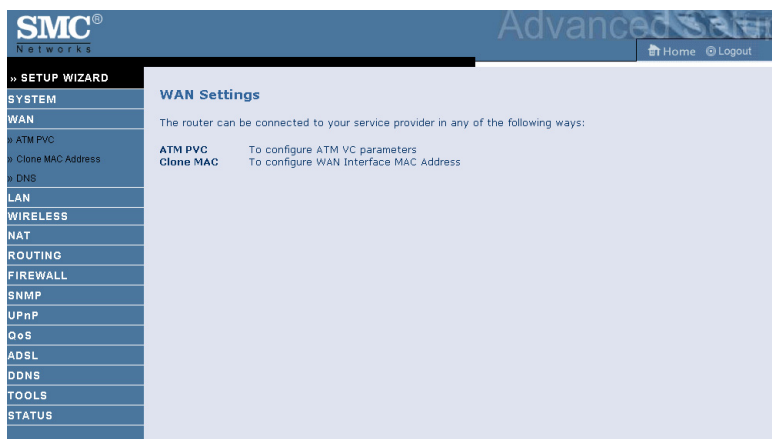
The screenshot shows a web browser's address bar. The address bar has a menu bar with 'File', 'Edit', 'View', 'Favorites', 'Tools', and 'Help'. Below the menu bar is a toolbar with icons for 'Back', 'Forward', 'Stop', 'Home', 'Search', and 'Favorites'. The address bar itself contains the text 'Address' followed by the URL '211.20.16.1:8080'.

WAN

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

The following three items are configurable:

- ATM PVC
- Clone MAC
- DNS



ATM PVC

Enter the ATM (Asynchronous Transfer Mode) virtual connection parameters here.

SMC® Networks Advanced Setup Wizard

Home Logout

SETUP WIZARD

- SYSTEM
- WAN
- ATM PVC
- Clone MAC Address
- DNS
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
- SNMP
- UPnP
- QoS
- ADSL
- DDNS
- TOOLS
- STATUS

ATM PVC

ADSL router uses ATM as its layer 2 protocol. ATM PVC is a virtual connection which acts as a WAN interface. The Gateway supports up to 8 ATM PVCs.

Description	VPI/VCI	Encapsulation	Protocol
VC1	8/35	VC MUX	PPPoA
VC2	-/-	---	---
VC3	-/-	---	---
VC4	-/-	---	---
VC5	-/-	---	---
VC6	-/-	---	---
VC7	-/-	---	---
VC8	-/-	---	---

HELP

Parameter	Description
VC1 - VC8	Click on the desired VC to set the values for the connection. In most cases you ISP will provide a single VC. For single VC use VC1.
VPI/VCI	Displays Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for corresponding VC.
Encapsulation	Displays Encapsulation configured for corresponding VC. <ul style="list-style-type: none"> VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. LLC: Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead).
Protocol	Displays protocol configured for corresponding VC.

ATM Interface

1483 Bridging

Enter the Bridging settings provided by your ISP.

ATM Interface

	ATM1
Protocol	1483 Bridging
VLAN	Default
VPI/VCI	8 / 35
Encapsulation	VC MUX
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10

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

PPPoA

ATM Interface

	ATM1
Protocol	PPPoA
VPI/VCI	8 / 35
Encapsulation	VC MUX
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Auto - Triggered by traffic
Idle Time (Minute)	5
Username	
Password	
Confirm Password	
MTU	1500

Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR.
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
IP assigned by ISP	Select Yes if you have a dynamic IP address. Select No if you have a static IP address.
IP Address	Enter the IP address provided by your ISP. For dynamic IP leave this field blank.
Subnet Mask	Enter the subnet mask address provided by your ISP. For dynamic IP leave this field blank.
Connect Type	Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.

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

1483 Routing

ATM Interface

	ATM1
Protocol	1483 Routing
IP Address	0.0.0
Subnet Mask	0.0.0
Default Gateway	0.0.0
VPI/VCI	8/35
Encapsulation	VC MUX
QoS Class	UBR
PCR/SCR/MBS	4000/4000/10
DHCP Client	<input type="checkbox"/>

Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
DHCP Client	Check the box if your ISP assigns an IP address dynamically.

PPPoE

ATM Interface	
	ATM1
Protocol	PPPoE
VPI/VCI	8 / 35
Encapsulation	VC MUX
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Auto - Triggered by traffic
Idle Time (Minute)	5
Username	userjoe
Password	*****
Confirm Password	*****
MTU	1492

Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR.
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
IP assigned by ISP	Select Yes if you have a dynamic IP address. Select No if you have a static IP address.
IP Address	Enter the IP address provided by your ISP. For dynamic IP leave this field blank.
Subnet Mask	Enter the Subnet Mask address provided by your ISP. For dynamic IP leave this field blank.
Connect Type	Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic.
Username	Enter user name provided by your ISP.

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

IP over RFC 1483 bridged

ATM Interface

	ATM1
Protocol	IP over RFC1483 bridged ▾
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
VPI/VCI	8 / 35
Encapsulation	VC MUX ▾
QoS Class	UBR ▾
PCR/SCR/MBS	4000 / 4000 / 10
DHCP Client	<input type="checkbox"/>

Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
QoS Class	ATM QoS classes including CBR, UBR and VBR.
PCR/SCR/MBS	QoS Parameters - PCR, SCR and MBS are configurable.
DHCP Client	Check the box if your ISP assigns an IP address dynamically.

Clone MAC Address

Some ISPs require you to register your MAC address with them. If this is the case, the MAC address of the Barricade must be changed to the MAC address that you have registered with your ISP.

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with the following items: SETUP WIZARD, SYSTEM, WAN, ATM PVC, Clone MAC Address (highlighted), DNS, LAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The main content area is titled 'Clone MAC Address' and contains the following text: '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.' Below this text are three radio button options for the 'WAN Interface MAC Address': 'Use the Gateway's default MAC address 00:06:4E:00:00:02' (selected), 'Use this PC's MAC address 00:10:B5:52:A9:69', and 'Enter a new MAC address manually:'. The manual entry option has six input fields for the MAC address bytes: 00, 10, B5, 52, A9, and 69. At the bottom right of the main area are three buttons: HELP, SAVE SETTINGS, and CANCEL.

DNS

Domain Name Servers (DNS) are used to map a domain name (e.g, www.smc.com) with the IP address (e.g, 64.147.25.20). Your ISP should provide the IP address of one or more Domain Name Servers. Enter those addresses on this screen, and click **SAVE SETTINGS**.

SMC®
Networks

» SETUP WIZARD

SYSTEM

WAN

» ATM PVC

» Clone MAC Address

» DNS

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

Advanced

Home Logout

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

Secondary DNS Address (optional)

HELP

SAVE SETTINGS

CANCEL

LAN

Use the LAN menu to configure the LAN IP address, VLAN binding and to enable the DHCP server for dynamic client address allocation.

SMC® Networks Advanced Setup [Home](#) [Logout](#)

» SETUP WIZARD

SYSTEM

WAN

LAN

» VLAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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

VLAN Binding

LAN1: Default

LAN2: Default

LAN3: Default

LAN4: Default

Lease Time: Forever

IP Address Pool

Start IP: 192 . 168 . 2 . 100

End IP: 192 . 168 . 2 . 199

Domain Name:

Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	The subnet mask of the network.
DHCP Server	Enable or Disable the DHCP server function. By default the DHCP server is enabled for automatic IP address assignment to client devices.
VLAN Binding	
LAN1 to LAN4	Select VLAN group for the corresponding LAN port. By default all ports members of the Default VLAN.
Lease Time	Set the IP lease time. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.

Parameter	Description
IP Address Pool	
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the ip address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.
End IP Address	Specify the end IP address of the DHCP pool.
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.

VLAN

VLANs are organized and controlled by VLAN Profiles. Up to 4 VLAN profiles can be created. Once a VLAN profile is created, you should add interfaces into the VLAN by changing the VLAN setting of that interface. Please note that only those interfaces of IEEE 802 bridging type (ex. LAN ports and 1483 Bridging PVCs) can be added to a VLAN.

The screenshot shows the SMC Networks Advanced Setup Wizard. On the left is a sidebar menu with options: SETUP WIZARD, SYSTEM, WAN, LAN, VLAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The main area is titled 'VLAN' and contains the following text: 'VLANs are organized and controlled by VLAN Profiles. Up to 4 VLAN profiles can be created. Once a VLAN profile is created, it is empty and user should add interfaces into the VLAN by changing the VLAN setting of that interface. Please note that only those interfaces of IEEE 802 bridging type (ex. LAN ports and 1483 Bridging PVCs) can be added to a VLAN.'

Below the text is a section titled 'VLAN Table (up to 4 rules)' with a table:

No.	VLAN	Grouped Interfaces	Configure
1	Default	LAN1, LAN2, LAN3, LAN4, WLAN	Edit

Below the table is a link 'Add VLAN'. At the bottom right are 'HELP' and 'CANCEL' buttons.

Click **Add VLAN** to setup the profile.

VLAN Profile

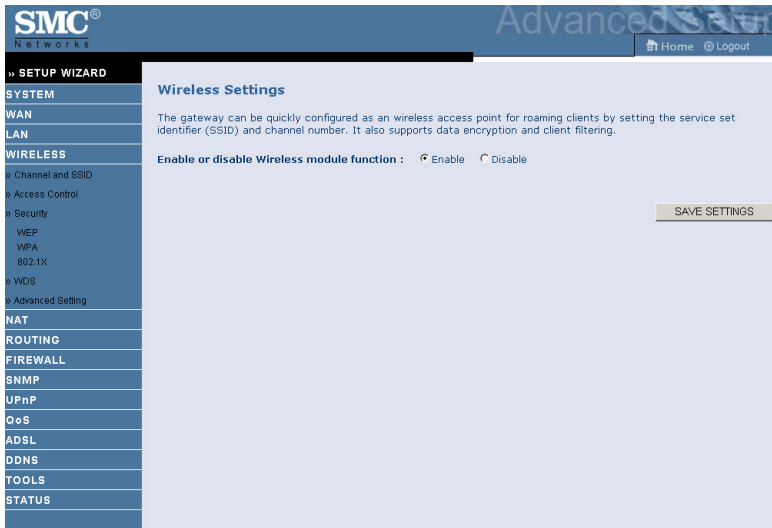
Enter parameters of the profile to define a VLAN.

Description	<input type="text"/>											
IP Address	<input type="text" value="192"/>	<input type="text" value="."/>	<input type="text" value="168"/>	<input type="text" value="."/>	<input type="text" value="1"/>	<input type="text" value="."/>	<input type="text" value="1"/>					
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="."/>	<input type="text" value="255"/>	<input type="text" value="."/>	<input type="text" value="255"/>	<input type="text" value="."/>	<input type="text" value="0"/>					
NAT Domain	<input checked="" type="radio"/> Private <input type="radio"/> Public											
IGMP Snooping	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled											
IGMP Querier	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled											

- Description: enter a name or description for the VLAN.
- IP Address: enter the IP address.
- Subnet Mask: enter the subnet mask.
- NAT Domain: select private or public.
- IGMP Snooping: Internet Group Management Protocol (IGMP) snooping is a method by which Layer 2 devices can “listen in” on IGMP conversations between hosts and routers. When a switch hears a group join message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a group leave message or a response timer expires, the switch will remove that host’s switch interface from the group.
- IGMP Querier: if the IGMP Querier is enabled, then the router will periodically query all multicast group members on the specified VLAN.

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

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with options: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS (selected), NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The WIRELESS section is expanded, showing sub-options: Channel and SSID (selected), Access Control, Security, WEP, WPA, 802.1X, WDS, and Advanced Setting. The main content area is titled 'Channel and SSID' and includes a descriptive paragraph: '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.' Below this is a configuration form with four fields: SSID (text input with 'SMC'), SSID Broadcast (radio buttons for ENABLE and DISABLE, with DISABLE selected), Wireless Mode (dropdown menu with 'Mixed (11b+11g)' selected), and Channel (dropdown menu with '11' selected). At the bottom right of the form are three buttons: HELP, SAVE SETTINGS, and CANCEL.

Parameter	Description
SSID	Service Set ID (SSID) is the name given to the wireless network. The SSID must be the same on the Barricade and all of its wireless clients.
SSID Broadcast	Enable or disable the broadcasting of the SSID. Disabling broadcasting of the SSID provides added security by hiding your wireless network.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have.
Channel	<p>The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients.</p> <p>The Barricade will automatically assign itself a radio channel, or you may select one manually.</p>

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 Address Filtering List**

Wireless DHCP Client List
- **MAC Filtering Table (up to 32 stations)**

ID	MAC Address
1	00 : 00 : 00 : 00 : 00 : 00
2	00 : 00 : 00 : 00 : 00 : 00
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

- **Enable MAC Filtering:** select to turn on/off this feature.
- **Access Rule for registered MAC address:** select to allow/deny access for the registered MAC addresses. Selecting Allow means only MAC addresses registered here will be able to connect to the router. Selecting Deny means only the MAC addresses registered here will be denied access to the router.
- **MAC Address Filtering List:** you can use the drop-down menu to select and quickly copy the entry to the MAC Filtering table.

Security

To make your wireless network safe, you should turn on the security function. The Barricade supports WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected) and WPA2 security mechanisms.



Three options are available:

- No WEP, No WPA
- WEP only
- WPA only

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.

The screenshot shows the SMC Advanced Router configuration interface. On the left is a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The 'WIRELESS' section is expanded, showing sub-items: Channel and SSID, Access Control, Security (selected), WEP (selected), WPA, 802.1X, WDS, and Advanced Setting. The main content area is titled 'WEP' and contains the following settings:

- WEP Mode:** Radio buttons for 64-bit (selected) and 128-bit.
- Key Entry Method:** Radio buttons for Hex (selected) and ASCII.
- Key Provisioning:** Radio buttons for Static (selected) and Dynamic.
- Static WEP Key Setting:** A section titled '10/26 hex digits for 64-WEP/128-WEP' containing:
 - Default Key ID:** A dropdown menu with '1' selected.
 - Passphrase:** A text input field with a 'GENERATE' button next to it. Below the field is the text '(1~32 characters)'.
 - Key 1, Key 2, Key 3, Key 4:** Four text input fields, each preceded by a label and followed by a series of asterisks to indicate masked characters.
 - Clear:** A button located below the key input fields.

At the bottom right of the configuration area are three buttons: 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1X function first.

You can automatically generate encryption keys using the passphrase or manually enter the keys. To generate the keys automatically enter a passphrase and click **GENERATE**. Select the default key from the drop-down menu and click **SAVE SETTINGS**.

Note: Before saving settings the key is shown in clear text. If you wireless client does not have a passphrase utility make a note of the default

key before saving settings. This is so you can configure your wireless client with the correct key.

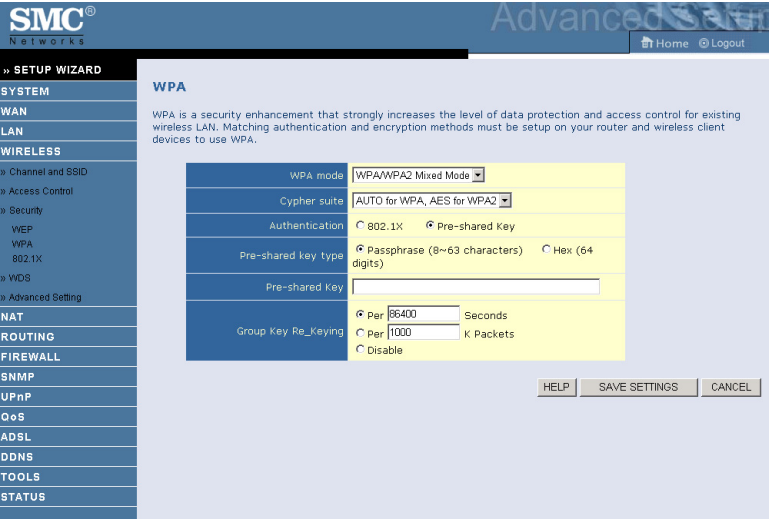
To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F)

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

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

WPA

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



Parameter	Description
WPA mode	Select WPA or WPA2 or mixed mode.
Cypher suite	The security mechanism used in WPA for encryption.
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. •802.1X: for the enterprise network with a RADIUS server. •Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.
Group Key Re_Keying	The period of renewing broadcast/multicast key.

802.1X

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

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

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	<input type="radio"/> Enable <input checked="" type="radio"/> 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	192 . 168 . 2 . 1
Server Port	1812
Secret Key	
NAS-ID	

HELP SAVE SETTINGS CANCEL

Parameter	Description
802.1X Authentication	Enable or disable this authentication function.
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re-Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the Barricade will wait between failed authentications.
Server Type	Select RADIUS as the authentication server.
RADIUS Server Parameters	
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.

Parameter	Description
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

WDS

The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and to allow stations to roam freely within the area covered by the WDS.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

» Channel and SSID

» Access Control

» Security

WEP

WPA

802.1X

» WDS

» Advanced Setting

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

WDS

The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and to allow stations to roam freely within the area covered by the WDS.

• Enable or disable WDS features : ☐ Enable ☒ Disable

Rescan

o AP MAC Address Table (up to 4 APs)

	SSID	MAC Address						Mode
<input checked="" type="checkbox"/>	SMC	00	: 0F	: CB	: AF	: 23	: 68	11g
<input type="checkbox"/>	HomeNet727864838b	00	: 04	: E2	: C2	: 66	: B8	11g

HELP SAVE SETTINGS CAN

To refresh the list of available access points, Click **Rescan**.

Available access points will show up on the AP MAC Address Table, check the box to add that particular access point to the WDS.

Advanced Setting

To change the settings on this screen is recommended for experienced user only. It is advised to leave the parameters at the default value.

SMC® Networks Advanced Setting

Home Logout

Advanced Setting

This page allows you to config advanced settings in the wireless driver.

Beacon Interval	100	(Default: 100, Range: 1-65535)
DTIM Interval	1	(Default: 1, Range: 1-255)
Fragmentation Threshold	2346	(Default: 2346, Range: 256-2346)
RTS Threshold	2347	(Default: 2347, Range: 0-2347)
CTS Protection Mode	Auto	(Default: Auto)
WMM Mode	Enable	(Default: Enable)

HELP SAVE SETTINGS CANCEL

- **Beacon Interval:** this represents the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
- **DTIM Interval:** Delivery Traffic Indication Message, indicates when the DTIM occurs. A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For example, a DTIM interval of one means that the multicast frames are sent after each beacon frame. A DTIM interval of two indicates that multicast frames are sent after every two beacon frames, and so on. Because each beacon frame includes a field that identifies the DTIM interval, all stations know when to wake up and receive multicast frames if they're implementing power saving.

- **Fragmentation Threshold:** this is the maximum size for directed data packets transmitted. Larger frames fragment into several packets this size or smaller before transmission. The receiving station then reassembles the transmitted fragments.
- **RTS Threshold:** RTS stands for “Request to Send”. This parameter controls what size data packet the low level RF protocol issues to an RTS packet. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, therefore reducing the apparent throughput of the network packet. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions.
- **CTS Protection Mode:** CTS stands for “Clear to Send”. If this value is set to Auto. The AP will automatically use CTS Protection Mode when the 802.11g products are experiencing severe problems and are not able to transmit to the AP in an environment with heavy 802.11b traffic. This function boosts the AP’s ability to catch all 802.11g transmissions but will decrease the performance.
- **WMM Mode:** Wireless Multimedia support. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort, and background. However, it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

NAT

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

SMC[®]
Networks

Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

» Address Mapping

» Virtual Server

» Special Application

» NAT Mapping Table

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

NAT Settings

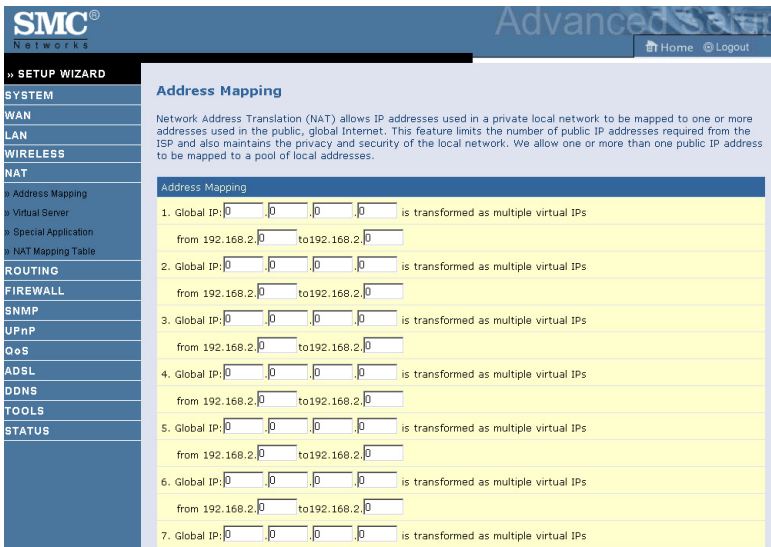
Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP.

Enable or disable NAT module function : ☒ Enable ☐ Disable

SAVE SETTINGS

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.



SMC® Networks Advanced Router

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

» Address Mapping

» Virtual Server

» Special Application

» NAT Mapping Table

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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 192.168.2.0 to 192.168.2.0
2. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0
3. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0
4. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0
5. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0
6. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0
7. Global IP: 0.0.0.0	is transformed as multiple virtual IPs from 192.168.2.0 to 192.168.2.0

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 IP Address	Protocol Type	LAN Port	Public Port	Enable		
1	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
2	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
3	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
4	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
5	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
6	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
7	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
8	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
9	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
10	192.168.2.1	TCP			<input type="checkbox"/>	Add	Clean
11	192.168.2.1	TCP			<input type="checkbox"/>	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.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

» Address Mapping

» Virtual Server

» Special Application

» NAT Mapping Table

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

Special Applications

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.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
8.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
9.	<input type="text"/>	<input type="radio"/> TCP	<input type="text"/>	<input type="radio"/> TCP	<input type="checkbox"/>

NAT Mapping Table

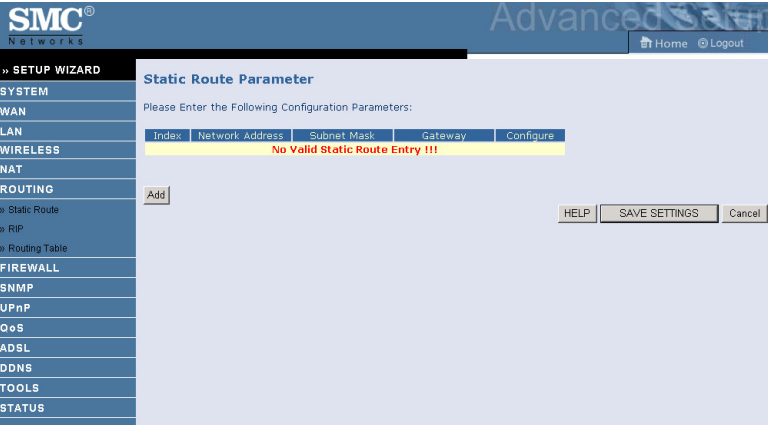
This screen displays the current NAPT (Network Address Port Translation) address mappings.

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with the following items: » SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, » Address Mapping, » Virtual Server, » Special Application, » NAT Mapping Table, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The main content area is titled "NAT Mapping Table" and includes the text "NAT Mapping Table displays the current NAPT address mappings." Below this text is a table with the following headers: Index, Protocol, Local IP, Local Port, Pseudo IP, Pseudo Port, Peer IP, and Peer Port. A "Refresh" button is located to the left of the table, and a "HELP" button is in the top right corner of the main area. The top of the interface features the SMC Networks logo and "Advanced Setup" text, along with "Home" and "Logout" links.

ROUTING

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

Static Route



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

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

RIP

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.

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

Static Route

RIP

Routing Table

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

RIP Parameter

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
LAN1	Disable	1	Disable	None	
WLAN	Disable	1	Disable	None	
ATM1	Disable	1	Disable	None	
ATM2	Disable	1	Disable	None	
ATM3	Disable	1	Disable	None	
ATM4	Disable	1	Disable	None	
ATM5	Disable	1	Disable	None	
ATM6	Disable	1	Disable	None	
ATM7	Disable	1	Disable	None	
ATM8	Disable	1	Disable	None	
PPPoE1	Disable	1	Disable	None	
PPPoE2	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.

Parameter	Description
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	<ul style="list-style-type: none">• None: No authentication.• Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.• MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.
Authentication Code	Password or MD5 Authentication key.

Routing Table

SMC Networks Advanced Setup

Home Logout

» SETUP WIZARD

Routing Table

List Routing Table:

Flags	Network Address	Netmask	Gateway	Interface	Metric
C	192.168.2.0	255.255.255.0	directly	VLAN1	---
C	127.0.0.1	255.255.255.255	directly	Loopback	---

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

HELP

Parameter Description

Flags	<p>Indicates the route status:</p> <p>C = Direct connection on the same subnet.</p> <p>S = Static route.</p> <p>R = RIP (Routing Information Protocol) assigned route.</p> <p>I = ICMP (Internet Control Message Protocol) Redirect route.</p>
Network Address	Destination IP address.
Netmask	<p>The subnetwork associated with the destination.</p> <p>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.</p>
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

FIREWALL

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

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



The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (For details see page 4-61.)

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select **Enable** and click the **SAVE SETTINGS** button to open the Firewall submenus.

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.

SMC® Networks Advanced Setup Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

- » Access Control
- » MAC Filter
- » URL Blocking
- » Schedule Rule
- » Intrusion Detection
- » DMZ
- SNMP
- UPnP
- QoS
- ADSL
- DDNS
- TOOLS
- STATUS

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 : ☒ Yes ☐ No
- Normal Filtering Table (up to 10 computers)

Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				

[Add PC](#)

HELP SAVE SETTINGS CANCEL

Parameter	Description
Enable Filtering Function	Click Yes to turn on the filtering function.
Normal Filtering Table	Displays a summary of the filtering rules configured.

To add the PC to the filtering table:

1. Click **Add PC** on the Access Control screen.
2. Define the appropriate settings for client PC services.
3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

SMC® Networks Advanced Router

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

» Access Control

» MAC Filter

» URL Blocking

» Schedule Rule

» Intrusion Detection

» DMZ

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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.

- Rule Description:
- Client PC IP Address: 192.168.2. ~
- Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

User Define Service

MAC Filter

The Barricade can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the Barricade to enter up to 32 MAC addresses that are not allowed access to the WAN port. Please note that this filter only applies to ethernet clients.

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, and FIREWALL. Under FIREWALL, several options are listed: Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, DMZ, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The 'MAC Filter' option is selected. The main content area is titled 'MAC Filtering Table'. It contains a description: '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.' Below this, there are two radio buttons for 'MAC Address Control': 'Yes' (unselected) and 'No' (selected). A bullet point indicates 'MAC Filtering Table (up to 32 computers)'. Below this is a table with 15 rows and 7 columns. The first column is 'ID' (1-15). The next six columns are for the MAC address, separated by colons. Each cell contains a small input box for a single digit or colon. The table is currently empty.

ID	MAC Address					
1		:		:		:
2		:		:		:
3		:		:		:
4		:		:		:
5		:		:		:
6		:		:		:
7		:		:		:
8		:		:		:
9		:		:		:
10		:		:		:
11		:		:		:
12		:		:		:
13		:		:		:
14		:		:		:
15		:		:		:

Click **Yes** to enable, or **No** to disable this function.

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.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

» Access Control

» MAC Filter

» URL Blocking

» Schedule Rule

» Intrusion Detection

» DMZ

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		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	
Site 12		Site 27	
Site 13		Site 28	
Site 14		Site 29	
Site 15		Site 30	

Clear All

HELP

SAVE SETTINGS

CANCEL

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.

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories like SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, and STATUS. The FIREWALL section is expanded, showing sub-items like Access Control, MAC Filter, URL Blocking, Schedule Rule, and DMZ. The 'Schedule Rule' sub-item is selected. The main content area is titled 'Schedule Rule' and contains a description: 'This page defines schedule rule names and activates the schedule for use in the "Access Control" page.' Below this is a section for the 'Schedule Rule Table (up to 10 rules)' which is currently empty, displaying a red error message: 'No Valid Schedule Rule !!!'. A link 'Add Schedule Rule' is provided. At the bottom right are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

SMC® Networks Advanced Setup Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

» Access Control

» MAC Filter

» URL Blocking

» **Schedule Rule**

» DMZ

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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 !!!		

[Add Schedule Rule](#)

Follow these steps to add a schedule rule:

- 1. Click **Add Schedule Rule** on the Schedule Rule screen.
 - 2. Define the appropriate settings for a schedule rule.
- Click **OK** and then click **SAVE SETTINGS** to save your settings.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

» Access Control

» MAC Filter

» URL Blocking

» Schedule Rule

» Intrusion Detection

» DMZ

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

Edit Schedule Rule

Name:

Comment:

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

OK Cancel

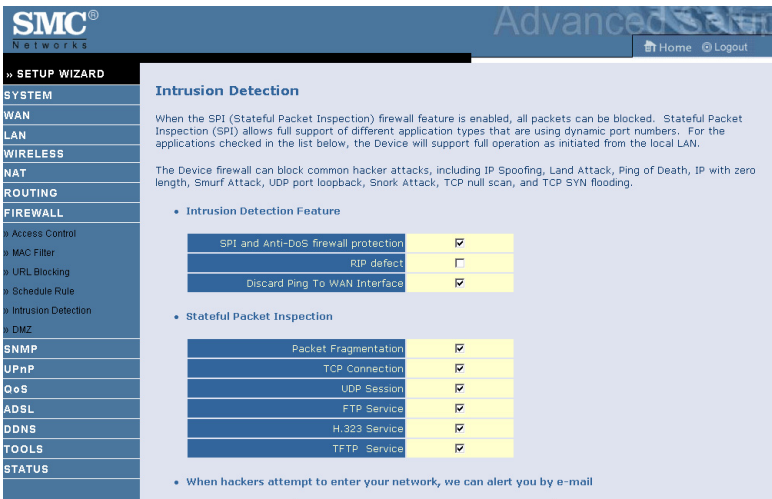
Intrusion Detection

- 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.



The screenshot shows the SMC Networks Advanced Setup Wizard. On the left is a sidebar with a 'SETUP WIZARD' menu and various system categories: SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, DMZ, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, and STATUS. The 'FIREWALL' category is expanded, showing sub-items like Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, and DMZ. The main content area is titled 'Intrusion Detection' and contains the following text:

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.

Below this text are two sections of configuration options:

- Intrusion Detection Feature**

SPI and Anti-DoS firewall protection	<input checked="" type="checkbox"/>
RIP defect	<input type="checkbox"/>
Discard Ping To WAN Interface	<input checked="" type="checkbox"/>
- Stateful Packet Inspection**

Packet Fragmentation	<input checked="" type="checkbox"/>
TCP Connection	<input checked="" type="checkbox"/>
UDP Session	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>

At the bottom, there is a note: "When hackers attempt to enter your network, we can alert you by e-mail".

Scroll down to view more information.

CONFIGURING THE ADSL ROUTER

SMC® Networks Advanced Setup

Home Logout

» **SETUP WIZARD**

SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

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

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :

• Connection Policy

Fragmentation half-open wait: 10 sec.

TCP SYN wait: 20 sec.

TCP FIN wait: 5 sec.

TCP connection idle timeout: 3600 sec.

UDP session idle timeout: 30 sec.

H.323 data channel idle timeout: 180 sec.

SMC® Networks Advanced Setup

Home Logout

» **SETUP WIZARD**

SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

TCP SYN wait: 20 sec.

TCP FIN wait: 5 sec.

TCP connection idle timeout: 3600 sec.

UDP session idle timeout: 30 sec.

H.323 data channel idle timeout: 180 sec.

• DoS Detect Criteria:

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: 50

Incomplete TCP/UDP sessions detect sensitive time period: 300 msec.

Maximum half-open fragmentation packet number from same host: 30

Half-open fragmentation detect sensitive time period: 10000 msec.

Flooding cracker block time: 300 sec.

HELP SAVE SETTINGS CANCEL

- **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 <i>start</i> 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 <i>stop</i> 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, and leaving them at the default settings 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.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

» Access Control

» MAC Filter

» URL Blocking

» Schedule Rule

» Intrusion Detection

» DMZ

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

DMZ(Demilitarized 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: ☐ Yes ☒ No

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.	0000	192.168.2.0
3.	0000	192.168.2.0
4.	0000	192.168.2.0
5.	0000	192.168.2.0
6.	0000	192.168.2.0
7.	0000	192.168.2.0
8.	0000	192.168.2.0

HELP SAVE SETTINGS CANCEL

SNMP

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

Community

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

SNMP Community

In the context of SNMP, a relationship between an agent and a set of SNMP managers defines security characteristics. The community concept is a local one, defined at the agent. The agent establishes one community for each desired combination of authentication, access control, and proxy characteristics. Each community is given a unique (within this agent) community name, and the management stations within that community are provided with and must employ the community name in all get operations. The agent may establish a number of communities, with overlapping management station membership.

No.	Community	Access	Valid
1	public	Read	<input checked="" type="checkbox"/>
2	private	Write	<input checked="" type="checkbox"/>
3		Read	<input type="checkbox"/>
4		Read	<input type="checkbox"/>
5		Read	<input type="checkbox"/>

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

Note: Up to five community names may be entered.

Trap

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

SMC®
Networks

Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

» Community

» Trap

UPnP

ADSL

DDNS

TOOLS

STATUS

SNMP Trap

In the context of SNMP, an unsolicited message can be sent by an agent to management station. The purpose is to notify the management station of some unusual event.

No.	IP Address	Community	Version
1	0.0.0.0		Disabled
2	0.0.0.0		Disabled
3	0.0.0.0		Disabled
4	0.0.0.0		Disabled
5	0.0.0.0		Disabled

HELP SAVE SETTINGS CANCEL

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

UPNP

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the office, home and everywhere within your network.



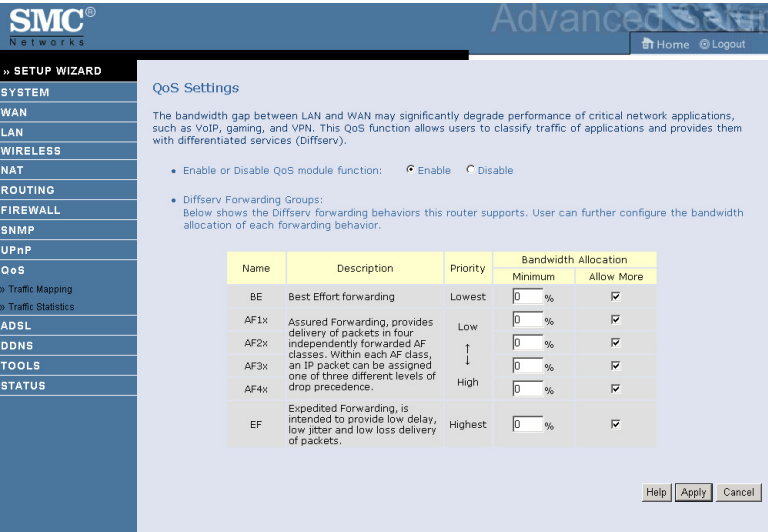
UPnP allows the device to automatically:

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

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

QoS

The QoS (Quality of Service) function allows you to differentiate traffic types and provide high-priority forwarding service for applications such as VoIP or gaming.



Parameter	Description
Enable or disable QoS module function	Check to enable or disable this function.
Diffserv Forwarding Groups	
BE	Best Effort forwarding, set the percentage for this type of QoS.
AF1x	Set the percentage for four different types of
AF2x	Assured Forwarding.
AF3x	
AF4x	
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.

Traffic Mapping

Use this screen to classify traffic into Diffserv forwarding groups and outgoing VCs.

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

» Traffic Mapping

» Traffic Statistics

ADSL

DDNS

TOOLS

STATUS

Traffic Mapping

Up to 16 rules can be defined to classify traffic into Diffserv forwarding groups and outgoing VCs.

Rule Name	Traffic Description	Map to Diffserv	Outgoing VC	Configure
VoIP	VoIP	EF	by routing	Edit Del

[Add traffic class](#)

[Help](#)

Click **Add traffic class** to add traffic class.

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

» Traffic Mapping

» Traffic Statistics

ADSL

DDNS

TOOLS

STATUS

Edit Traffic Class

This page is for user to specify a classify rule. First, define the class by the traffic type and the local and remote addresses. Then set the Diffserv forwarding group this class is mapped to. Finally, select the outgoing VC that traffic of this class would be routed to.

Rule Name	<input type="text"/>		
Traffic Type	<input type="text" value="Any"/>	ADVANCED CONFIG	
Map to Forwarding Group	<input type="text" value="BE"/>	Remark DSCP as <input type="text" value="BE (000000)"/> (the first 6 bits of IP TOS field)	
Direct to VC	<input type="text" value="By Routing"/>		

[Help](#) [Apply](#) [Cancel](#)

Traffic Statistics

This screen shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours.

SMC®
Networks

Advanced

Home Logout

» SETUP WIZARD

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

» Traffic Mapping

» Traffic Statistics

ADSL

DDNS

TOOLS

STATUS

Traffic Statistics

This page shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours (automatically updated every 5 mins).

Forwarding Behavior	Average sent byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

Forwarding Behavior	Average dropped byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

Help Refresh

Click **Refresh** to renew the list.

ADSL

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

ADSL Parameters

SMC® Networks Advanced Setup Wizard

Home Logout

SETUP WIZARD

- SYSTEM
- WAN
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
- SNMP
- UPnP
- QoS
- ADSL
- Parameters
- Status
- DDNS
- TOOLS
- STATUS

ADSL Parameter

This page allows you to specify the ADSL standards to operate with. You may explicitly set a specific standard, or choose "Automatic" to automatically negotiate with remote DSLAM.

Operation Mode:

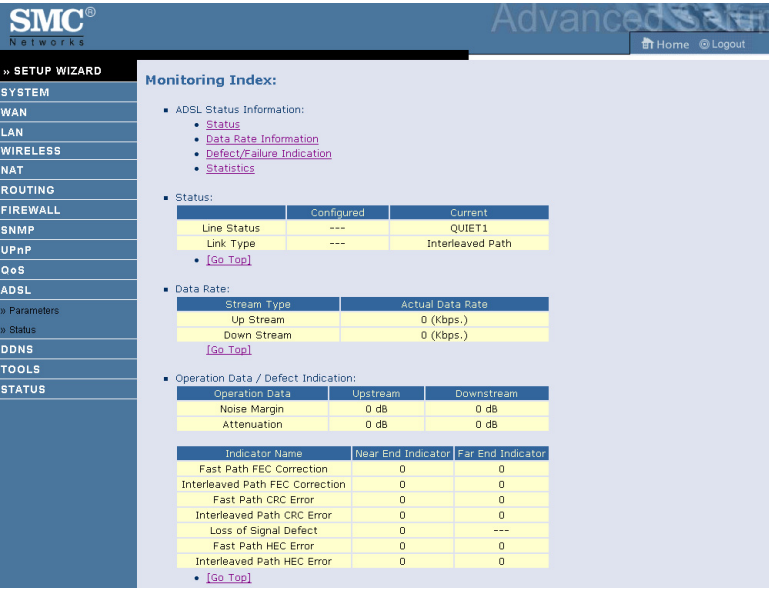
HELP OK Retrain

Parameter	Description
Operation Mode	<ul style="list-style-type: none"> Automatic T1.413 Issue 2 G.992.1 (G.DMT) G.992.2 (G.Lite) G.992.3 (ADSL2) G.992.5 (ADSL2+)

This screen allows you to specify the ADSL standards to operate with. You may explicitly set a specific standard, or choose "Automatic" to automatically negotiate with remote DSLAM.

ADSL Status

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



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

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

DDNS

Dynamic Domain Name Service (DDNS) provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

SMC® Advanced

Home Logout

» **SETUP WIZARD**

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

STATUS

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.

Dynamic DNS ☐ Enable ☒ Disable

Provider DynDNS.org

Domain Name

Account / E-mail

Password / Key

HELP SAVE SETTINGS CANCEL

This DDNS feature is powered by:

- DynDNS.org
- TZO.com
- NO-IP.com

With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

TOOLS

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

Ping Utility

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

SMC® Networks Advanced Setup

Home Logout

» SETUP WIZARD

Ping Utility

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

Destination Address

Destination Address is empty
Test Result Stopped

HELP Execute CANCEL

SYSTEM

WAN

LAN

WIRELESS

NAT

ROUTING

FIREWALL

SNMP

UPnP

QoS

ADSL

DDNS

TOOLS

» Ping Utility

» TraceRoute Utility

» Configuration Tools

» Firmware Upgrade

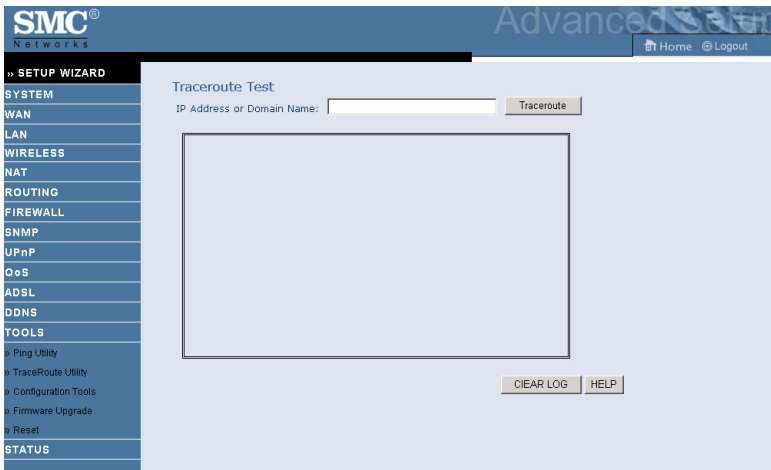
» Reset

STATUS

Enter the destination domain name or the IP address in the **Destination Address** field, and click **Execute**.

Trace Route Utility

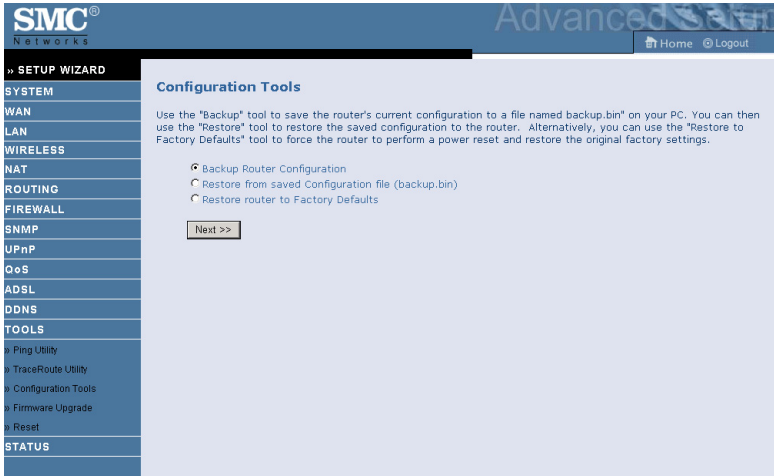
Traceroute is the program that shows you the route over the network between two systems, listing all the intermediate routers that a connection must pass through to get to its destination. It can help you determine why your connections to a given server might be poor, and can often help you figure out where exactly the problem is. It also shows you how systems are connected to each other.



Enter the domain name or IP address in the IP Address or Domain Name field, and click **Traceroute**.

The Router keeps a log of the traceroute test, click **Clear Log** to delete the records.

Configuration Tools



- Backup allows you to save the Barricade's configuration to a file.
- Restore can be used to restore the previously saved backup configuration file.
- Restore to Factory Defaults resets the Barricade back to the original settings.

Choose a function and click **Next**.

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. In the Firmware file field, click “**Browse...**” to look for the downloaded file. Click **BEGIN UPGRADE**.
3. Check the Status screen Information section to confirm that the upgrade process was successful.

The screenshot shows the SMC Networks Advanced Router configuration interface. On the left is a navigation menu with the following items: » SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, SNMP, UPnP, QoS, ADSL, DDNS, TOOLS, » Ping Utility, » TraceRoute Utility, » Configuration Tools, » Firmware Upgrade, » Reset, and STATUS. The main content area is titled "Firmware Upgrade". It contains the following text: "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>". Below this, it says: "Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process." There is a text input field labeled "Firmware File" with a "Browse..." button next to it. At the bottom right of the main area are three buttons: "HELP", "BEGIN UPGRADE", and "CANCEL".

Reset

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



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

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

STATUS

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



Scroll down to view more information.

SMC®

Networks

Advanced

[Home](#)
[Logout](#)

SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

ATM PVC

VC1	
VPI/VCI	8/35
Encapsulation	VC MUX
Protocol	PPPoA
IP Address	Down
Subnet Mask	---
Gateway	---
Primary DNS	---
Secondary DNS	---
<input type="button" value="Disconnect"/> <input type="button" value="Connect"/>	

VC2

Disabled

VC3

Disabled

VC4

Disabled

VC5

Disabled

VC6

Disabled

VC7

Disabled

VC8

Disabled

SMC®

Networks

Advanced

[Home](#)
[Logout](#)

SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

Security Log

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

08/01/2003 00:42:56 192.168.2.100

08/01/2003 00:00:03 sending ACK to

DHCP Client Log

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

ip=192.168.2.100 mac=00-10-B5-52-

The following items are included on the Status screen:

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

Finding the MAC address of a Network Card

WINDOWS 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	<ul style="list-style-type: none">• 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. <p>If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.</p>

Troubleshooting Chart	
Symptom	Action
LED Indicators	
Link LED is Off	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.

Troubleshooting Chart	
Symptom	Action
Wireless Problems	
A wireless PC cannot associate with the Barricade.	<ul style="list-style-type: none"> • Make sure the wireless PC has the same SSID settings as the Barricade. See “Channel and SSID” on page 4-35. • You need to have the same security settings on the clients and the Barricade. See “Security” on page 4-37.
The wireless network is often interrupted.	<ul style="list-style-type: none"> • 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 a microwave ovens or wireless phones. Change the location of the interference sources or of the Barricade. • Change the wireless channel on the Barricade. See “Channel and SSID” on page 4-35. • Check that the antenna, connectors, and cabling are firmly connected.
The Barricade cannot be detected by a wireless client.	<ul style="list-style-type: none"> • 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 Barricade. See “Channel and SSID” on page 4-35 and “Security” on page 4-37.

APPENDIX B

CABLES

Ethernet Cable

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

Specifications

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

Wiring Conventions

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

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

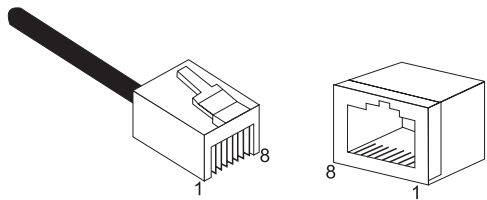


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Connection

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

AttachedDevicePortType	Connecting Cable Type
MDI-X	Straight-through
MDI	Crossover

Pin Assignments

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

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

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

Straight-Through Wiring

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

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

Crossover Wiring

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

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

APPENDIX C

SPECIFICATIONS

Physical Characteristics

Ports

Four 10/100Mbps RJ-45 Ports
One ADSL RJ-11
One external dipole antenna

ADSL Features

Supports DMT line modulation
Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 & T1.413, Issue 2)
Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream
Supports ADSL2/2+: up to 24Mbps downstream, up to 1Mbps upstream
Dying GASP support

ATM Features

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

Management Features

Firmware upgrade via WEB Based Management
WEB Based Management (configuration)
Power Indicators
Event and History logging
Network Ping

Security Features

Password protected configuration access
User authentication (PAP/CHAP) with PPP
Firewall NAT NAPT
VPN pass through

LAN Features

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

Applications

Netmeeting, ICQ, Real Player, QuickTime, DialPad, PC Anywhere, Telnet,
SNTP, NNTP

Radio Features

Wireless RF module Frequency Band

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 802.11b compliant:

11 channels (US, Canada)

13 channels (ETSI)

14 channels (Japan)

Operating Channels IEEE 802.11g compliant:

13 channels (Europe, Japan)

11 channels (US, Canada)

RF Output Power Modulation Rate-Output Power (dBm)

802.11b - 1Mbps 16

802.11b - 2Mbps 16

802.11b - 5.5Mbps 16

802.11b - 11Mbps 16

Modulation Rate-Output Power (dBm)

802.11g - 6Mbps 15

802.11g - 9Mbps 15

802.11g - 12Mbps 15

802.11g - 18Mbps 15

802.11g - 24Mbps 15

802.11g - 36Mbps 15

802.11g - 48Mbps 15

802.11g - 54Mbps 15

Sensitivity Modulation Rate-Receiver 2.412 ~ 2.484 HGz

Sensitivity (dBm)

802.11b - 1Mbps -90

802.11b - 2Mbps -88

802.11b - 5.5Mbps -85

802.11b - 11Mbps -84

Modulation Rate-Receiver Sensitivity Typical (dBm)

802.11g - 6Mbps -88
802.11g - 9Mbps -87
802.11g - 12Mbps -84
802.11g - 18Mbps -82
802.11g - 24Mbps -79
802.11g - 36Mbps -75
802.11g - 48Mbps -68
802.11g - 54Mbps -68

Environmental

SMC7904WBRA2 complies with the following standards:

Temperature: IEC 68-2-14
0 to 40 degrees C (Standard Operating)
-20 to 70 degree C (Non-operation)
Humidity: 10% to 95% (Noncondensing)

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

Shock: IEC 68-2-29

Drop: IEC 68-2-32

Dimensions

159.3 x 133.4 x 32.1 (mm)

Weight

290 g

Input Power

12 V 1 A

IEEE Standards

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

ELECTROMAGNETIC COMPATIBILITY

CE

R&TTE

ETSI

FCC part 15 Class B

FCC part 68

RoHS

Safety

UL 60950-1

CSA 22.2 No. 60950-1

EN 60950-1 & IEC 60950-1

Internet Standards

RFC 826 ARP

RFC 791 IP

RFC 792 ICMP

RFC 768 UDP

RFC 793 TCP

RFC 783 TFTP

RFC 1483 AAL5 Encapsulation

RFC 1661 PPP

RFC 1866 HTML

RFC 2068 HTTP

RFC 2364 PPP over ATM

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)

(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481

From Europe : Contact details can be found on

www.smc-europe.com or www.smc.com

INTERNET

E-mail addresses:

techsupport@smc.com

european.techsupport@smc-europe.com

Driver updates:

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

World Wide Web:

<http://www.smc.com/>

<http://www.smc-europe.com/>

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 8712 779802	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 3355708602	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Eastern Europe:	34-93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	216-712-36616	Fax 216-71751415
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	7 (095) 7893573	Fax 7 (095) 789 357
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

If you are looking for further contact information, please visit www.smc.com or www.smc-europe.com.

SMC[®]
Networks

38 Tesla

Irvine, CA 90618

Phone: (943) 679-8000