SMC®
Networks

SMC7904BRA2/B2
ADSL2 BARRICADE ™

4-Port ADSL2/ 2+ Modem Router

USER GUIDE

Router with built-in ADSL2/2+ Modem

From SMC's line of award-winning connectivity solutions

SMC®
Networks
38 Tesla
Irvine, CA 92618
Phone: (949) 679-8000

August 2006
R.01 F/W 0.11

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

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

Limited Warranty

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

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

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

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

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

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

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

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

SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

COMPLIANCES

Federal Communication Commission Interference Statement

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

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

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

EC Conformance Declaration CE

SMC contact for these products in Europe is:

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

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 55022
EN 55024
EN 61000-3-2
EN 61000-3-3
EN 60950-1

Safety Compliance

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlu ßsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sind beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden. Für einen Nennstrom bis 6 A und einem Gerätegewicht größer 3 kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75 mm^2 einzusetzen.

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

Table of Contents

CHAPTER 1
INTRODUCTION

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

About the Barricade

The Barricade provides Internet access to multiple users by sharing a single-user account.

It is simple to configure and can be up and running in minutes.

Features and Benefits

- Intergrated ADSL modem for connecting to ADSL line
- Local network connection via four 10/100 Mbps Ethernet ports
- DHCP for dynamic IP configuration, and DNS Proxy/Relay for domain name mapping
- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet

services such as web, FTP, e-mail, and Telnet)

- VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP)
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

Applications

Many advanced networking features are provided by the Barricade:

- **Wired LAN**

  The Barricade provides connectivity to 10/100 Mbps 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**

  Using only one ISP account, multiple users on your network can access the Internet at the same time.

- **Virtual Server**

  If you have a fixed IP address, you can set the Barricade to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the Barricade can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **DMZ Host Support**

  Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

- **Security**

  The Barricade supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The Barricade's firewall also blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- **Virtual Private Network (VPN)**

  The Barricade supports three of the most commonly used VPN protocols — PPTP, L2TP, and IPSec. These protocols allow remote users to establish a secure connection to their corporate network. If your service provider supports VPNs, then these protocols can be used to create an authenticated and encrypted tunnel for passing secure data over the Internet (i.e., a traditionally shared data network). The VPN protocols supported by the Barricade are briefly described below.

- Point-to-Point Tunneling Protocol — Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
- L2TP merges the best features of PPTP and L2F — Like PPTP, L2TP requires that the ISP's routers support the protocol.
- IP Security — Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

CHAPTER 2
INSTALLATION

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

Package Contents

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

- ADSL2 Barricade^{TM} (SMC7904BRA2 or SMC7904BRB2)
- Power adapter
- One CAT-5 Ethernet cable (RJ-45)
- One Telephone patch cables (RJ-11)
- Documentation CD
- One Warranty Card
- One Splitter for NE (the Netherlands), UK and FR (France) versions only

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.
- 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 ADSL2+ modem and connects to the Internet or to a remote site using its WAN port. This device can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports.

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

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports.

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

SMC7904BRA2 contains the following ports on the rear panel:

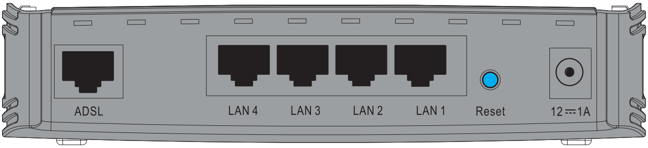


Figure 2-1. SMC7904BRA2 Rear Panel

Item	Description
ADSL Port	Connect your ADSL line to this port (RJ-11 port).
LAN1 to LAN4	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).
Reset Button	Use this button to reset the Barricade and restore the default factory settings. To reset without losing configuration settings, see “Reset” on page 4-70.
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may damage the Barricade.

SMC7904BRB2 contains the following ports on the rear panel:

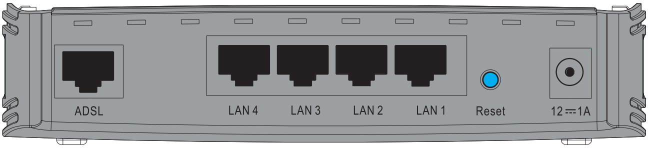


Figure 2-2. SMC7904BRB2 Rear Panel

Item	Description
ADSL Port	Connect your ADSL line to this port (RJ-45 port).
LAN1 to LAN4	Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).
Reset Button	Use this button to reset the Barricade and restore the default factory settings. To reset without losing configuration settings, see "Reset" on page 4-70.
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may damage the Barricade.

LED Indicators (SMC7904BRA2)

The power and port LED indicators on the front panel for SMC7904BRA2 are illustrated in the following figure and table.

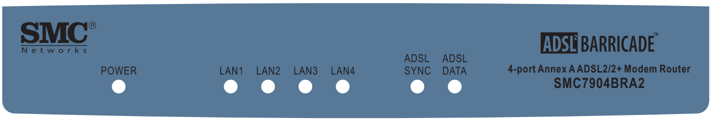


Figure 2-3. SMC7904BRA2 Front Panel

LED	Status	Description
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
LAN (4 LEDs)	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.
ADSL Sync	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL Data	Blinking	ADSL port is sending/receiving data.
	Off	No data is being transferred.

LED Indicators (SMC7904BRB2)

The power and port LED indicators on the front panel for SMC7904BRB2 are illustrated in the following figure and table.

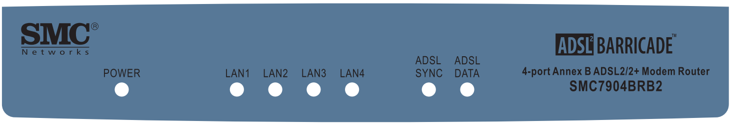


Figure 2-4. SMC7904BRB2 Front Panel

LED	Status	Description
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
LAN (4 LEDs)	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.
ADSL Sync	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL Data	Blinking	ADSL port is sending/receiving data.
	Off	No data is being transferred.

ISP Settings

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

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

Connect the System

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

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

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

Connect the ADSL Line

Connect the supplied ADSL cable from the port labelled ADSL on the Splitter/Microfilter to the ADSL port on your Barricade. When inserting the plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Note: The ADSL port of SMC7904BRA2 is RJ-11. The ADSL port of SMC7904BRB2 is RJ-45.

Attach to Your Network Using Ethernet Cabling

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

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

Warning: Do not plug a phone jack connector into an RJ-45 port. This may damage the Barricade.

Note: Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Category 5 cable is recommended. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).

Connect the Power Adapter

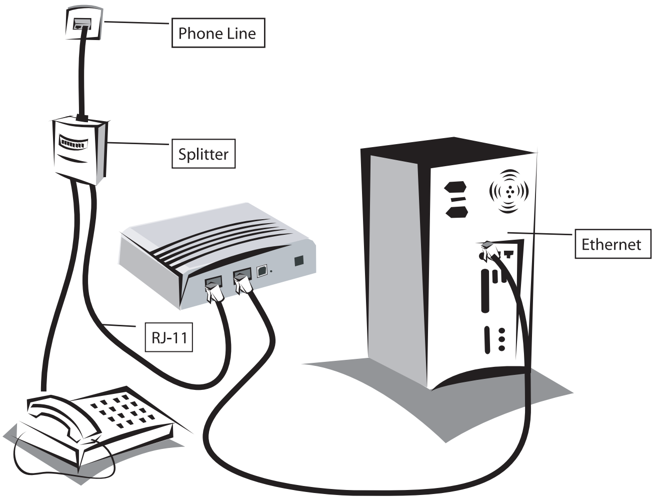
Plug the power adapter into the power socket on the rear of the Barricade, and the other end into a power outlet.

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

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

Connection Illustration

The connection diagram shows how to connect the Barricade.



CHAPTER 3
CONFIGURING CLIENT PC

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

See:

"Windows 2000" on page 3-2

"Windows XP" on page 3-5

"Configuring Your Macintosh Computer" on page 3-7

depending on your operating system.

TCP/IP Configuration

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

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

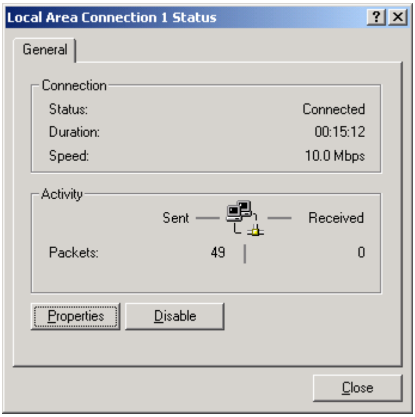
Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade's web configuration interface in order to make the required changes. (See "Configuring the BarricadeTM" on page 4-1 for instruction on configuring the Barricade.)

Windows 2000

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

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

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



Local Area Connection 1 Status

General

Connection

Status: Connected

Duration: 00:15:12

Speed: 10.0 Mbps

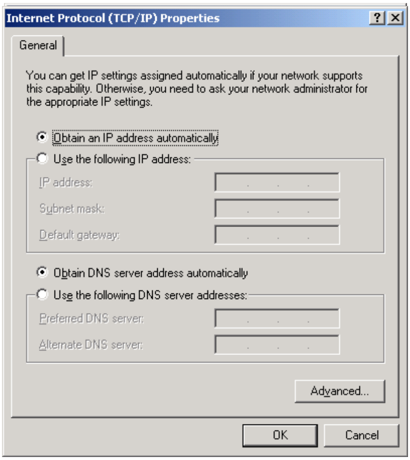
Activity

Sent — Received

Packets: 49 | 0

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

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.



Internet Protocol (TCP/IP) Properties

General

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

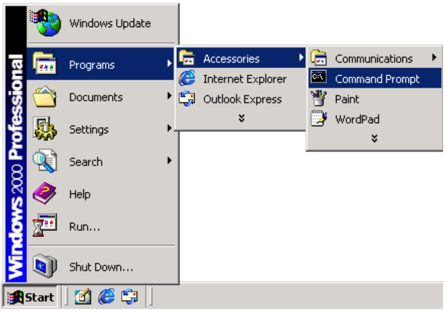
Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the Barricade’s HTML configuration pages. See page 3-5 for details.

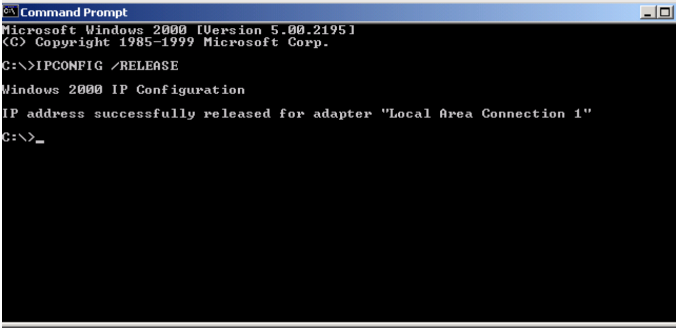
Obtain IP Settings from Your Barricade

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

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

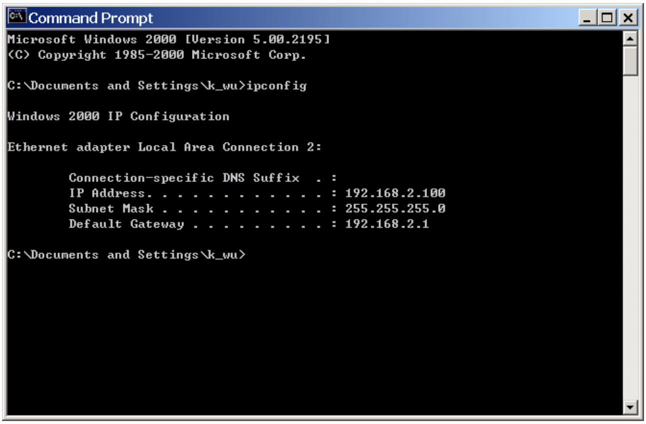


2. In the Command Prompt window, type “**IPCONFIG /RELEASE**” and press the ENTER key.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

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

C:\>_
```

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_wu>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

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

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

4. Close the Command Prompt window.

Your computer is now configured to connect to the Barricade.

Windows XP

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

Disable HTTP Proxy

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

Open your web browser, go to **Tools/Internet Options**, select the **Connections** tab, click **LAN Setting**. Make sure the checkbox for Use a proxy server for your LAN is not checked.

Obtain IP Settings from Your Barricade

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

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

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

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

4. Close the Command Prompt window.

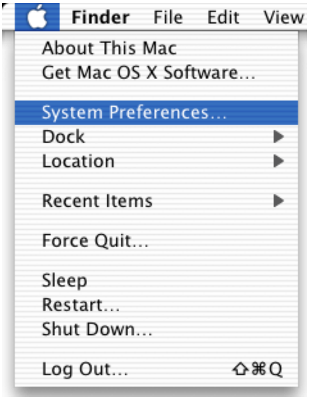
Your computer is now configured to connect to the Barricade.

Configuring Your Macintosh Computer

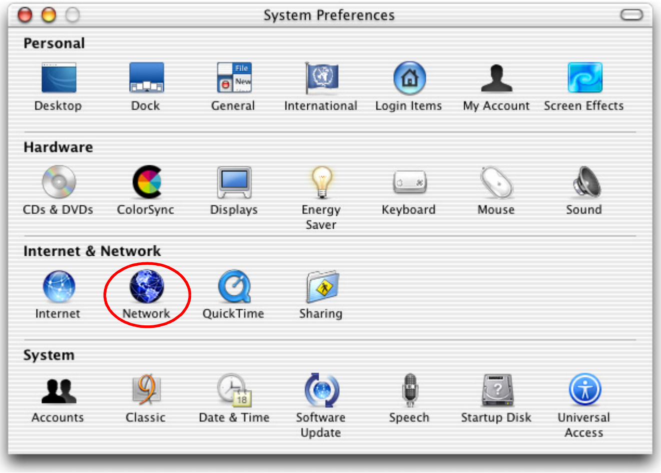
You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

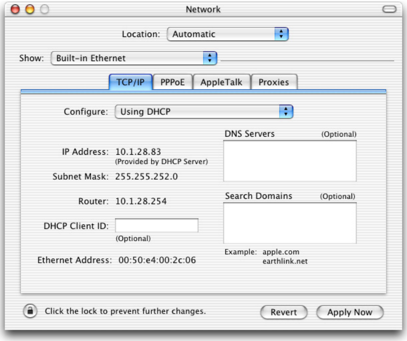
1. Pull down the Apple Menu. Click **System Preferences**.



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



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



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 10.1.28.83
(Provided by DHCP Server)

Subnet Mask: 255.255.252.0

Router: 10.1.28.254

DHCP Client ID:
(Optional)

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

DNS Servers (Optional)

Search Domains (Optional)

Example: apple.com
earthlink.net

Click the lock to prevent further changes.

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

5. Close the Network window.

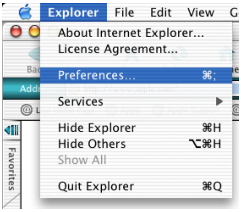
Now your computer is configured to connect to the Barricade.

Disable HTTP Proxy

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

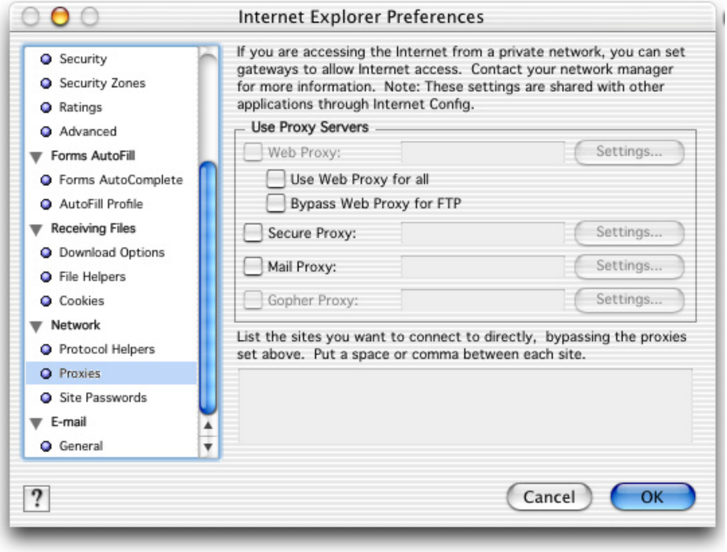
Internet Explorer

1. Open Internet Explorer and click **Explorer/ Preferences**.



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

3. Uncheck all check boxes and click OK.



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

Use Proxy Servers

□ Web Proxy: Settings...

□ Use Web Proxy for all

□ Bypass Web Proxy for FTP

□ Secure Proxy: Settings...

□ Mail Proxy: Settings...

□ Gopher Proxy: Settings...

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

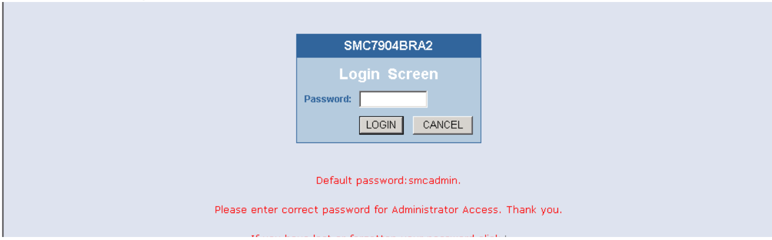
CHAPTER 4
CONFIGURING THE BARRICADE™

After you have configured TCP/IP on a client computer, you can configure the Barricade using your web browser.

To access the Barricade's 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: Password is case sensitive.

This is the login screen for SMC7904BRA2:

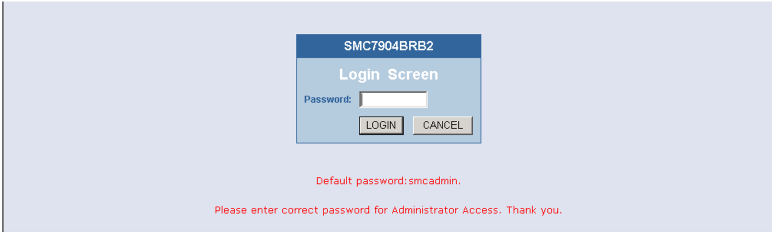


Default password:smcadmin.

Please enter correct password for Administrator Access. Thank you.

If you have lost or forgotten your password click

This is the login screen for SMC7904BRB2:

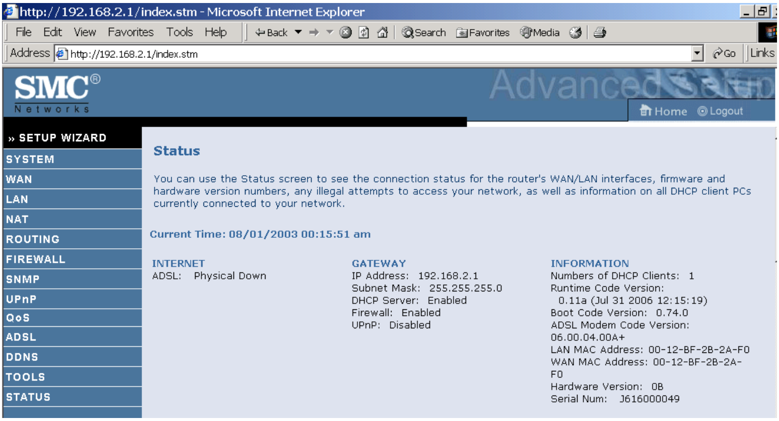


Default password:smcadmin.

Please enter correct password for Administrator Access. Thank you.

Navigating the Management Interface

The first screen of the web management is the Status screen. You can view the device status summary here.



Status

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

Current Time: 08/01/2003 00:15:51 am

```
INTERNET                       GATEWAY                          INFORMATION
ADSL:   Physical Down          IP Address:  192.168.2.1         Numbers of DHCP Clients:  1
                               Subnet Mask:  255.255.255.0      Runtime Code Version:
                               DHCP Server:  Enabled              0.11a (Jul 31 2006 12:15:19)
                               Firewall:  Enabled               Boot Code Version:  0.74.0
                               UPnP:  Disabled                  ADSL Modem Code Version:
                                                                06.00.04.00A+
                                                                LAN MAC Address: 00-12-BF-2B-2A-F0
                                                                WAN MAC Address: 00-12-BF-2B-2A-
                                                                F0
                                                                Hardware Version:  0B
                                                                Serial Num:   J616000049
```

The Barricade’s management interface consists of a Setup Wizard and 13 menu items.

Use the Setup Wizard to quickly set up the Barricade. Go to “SETUP WIZARD” on page 4-4 for details.

For configuration details of the 13 menu items, please refer to “Configuration parameters” on page 4-16.

Making Configuration Changes

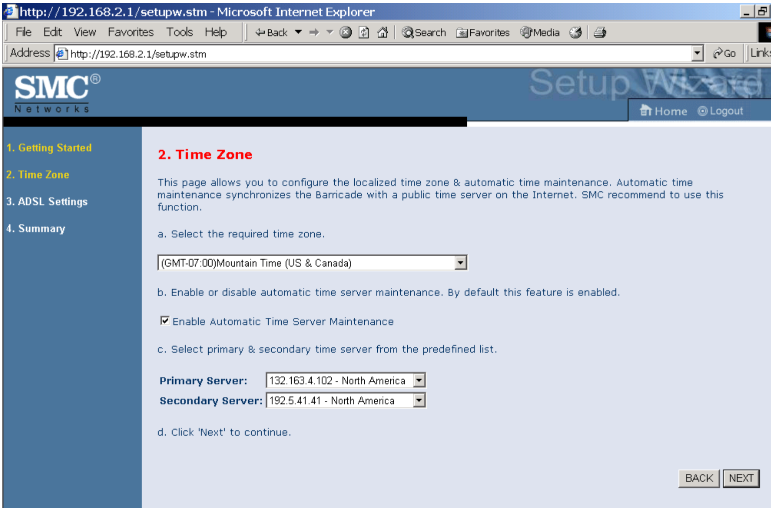
Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click the **APPLY** or **SAVE SETTINGS** or **NEXT** button at the bottom of the screen to enable the new setting.

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

SETUP WIZARD

Time Zone

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



http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. 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-07:00)Mountain Time (US & Canada)

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.

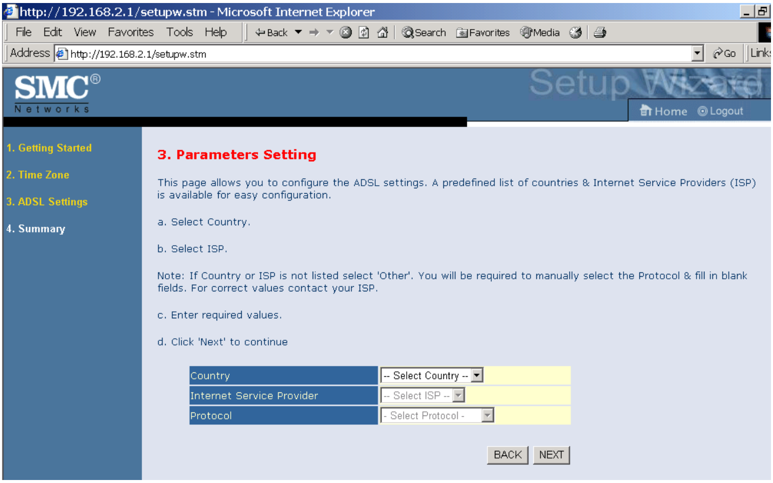
Select your local time zone from the drop down menu. This information is used for log entries and client filtering.

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

Click **NEXT** to continue.

Parameter Setting

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.


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary
BACK NEXT

3. Parameters Setting

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

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

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

If your Country or Internet Service Provider is not listed in this screen, you will need to manually enter settings. Go to “Parameter Setting - Country or ISP Not Listed” on page 4-6 in the manual.

Note: If your ISP has not provided you with a DNS address and the protocol is PPPoA, PPPoE or 1483 Bridging, you can leave this field blank. The Barricade will then automatically obtain the DNS address.

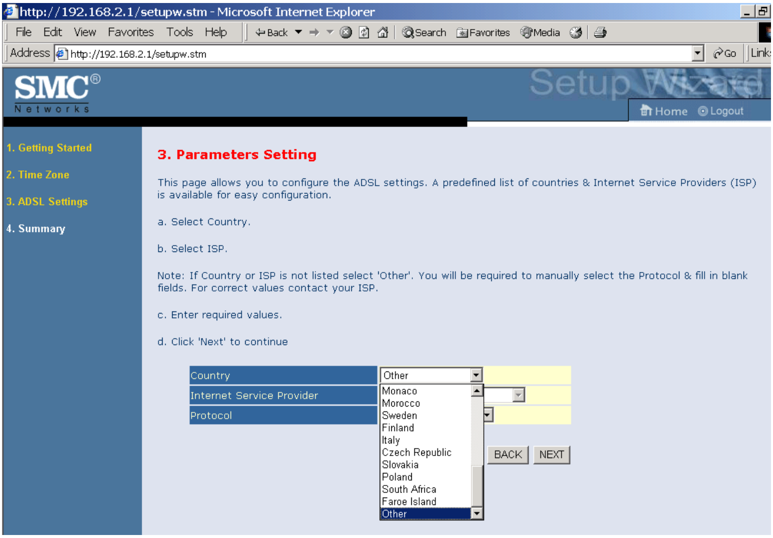
Click **NEXT** to continue.

Parameter Setting - Country or ISP Not Listed

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

For manual configuration you will need to know the Protocol, DNS Server, Encapsulation and VPI/VCI settings used by your ISP. If you have a static IP address you will also need to know the IP address, Subnet Mask and Gateway address. Please contact your ISP for these details if you do not already have them.

After selecting **Other**, then select the **Protocol** that your ISP uses from the drop down menu.


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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.

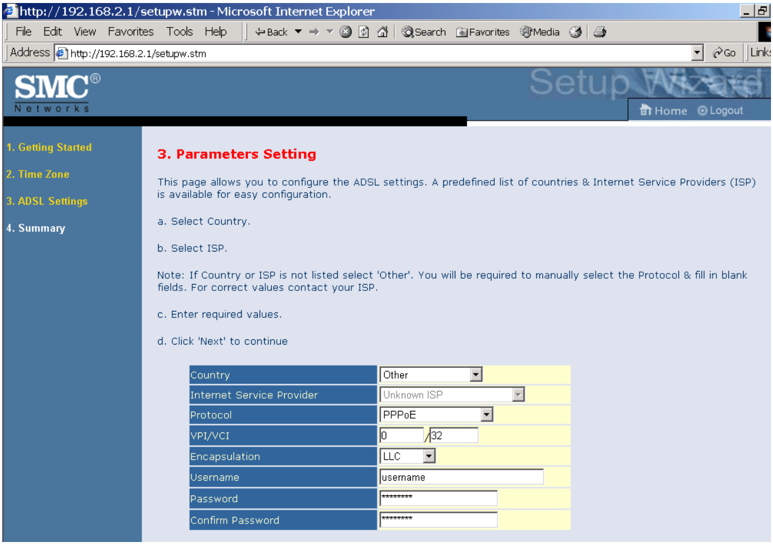
d. Click 'Next' to continue

Country: Other

Internet Service Provider

Protocol

PPPoE


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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

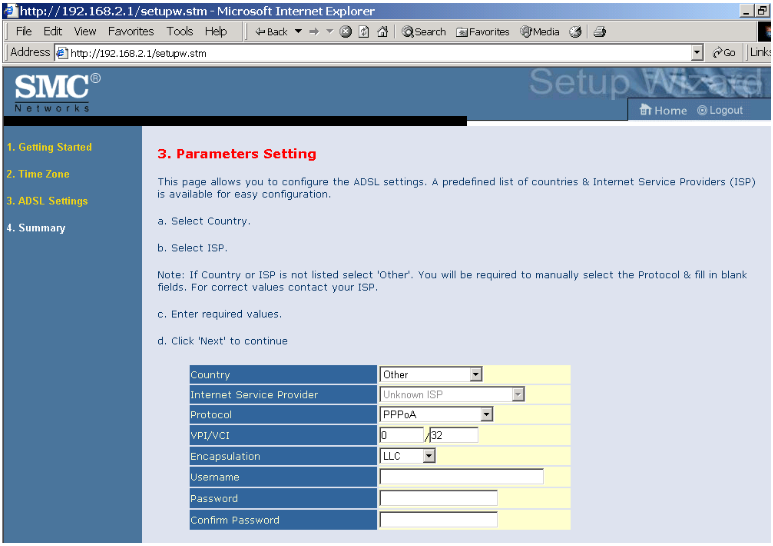
Country	Other
Internet Service Provider	Unknown ISP
Protocol	PPPoE
VPI/VCI	0 / 32
Encapsulation	LLC
Username	username
Password	********
Confirm Password	********

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

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

PPPoA


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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

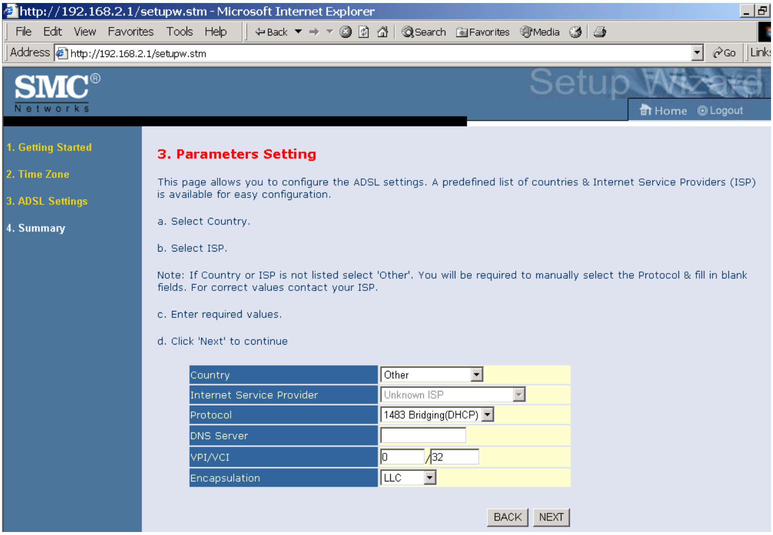
Country	Other
Internet Service Provider	Unknown ISP
Protocol	PPPoA
VPI/VCI	0 / 32
Encapsulation	LLC
Username	
Password	
Confirm Password	

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

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

1483 Bridging (DHCP)


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary
BACK
NEXT

3. Parameters Setting

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

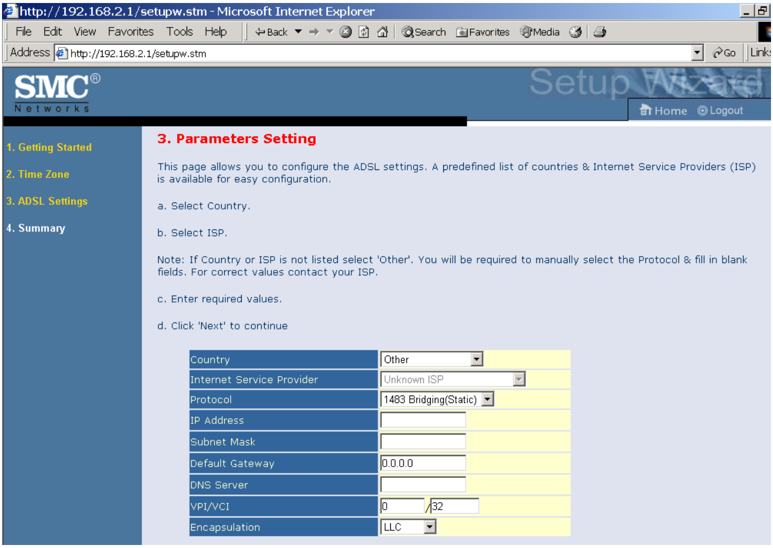
Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Bridging(DHCP)
DNS Server	
VPI/VCI	0 / 32
Encapsulation	LLC

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

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

Go to “Confirm” on page 4-14 in the manual for details about the setting.

1483 Bridging (Static)



http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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

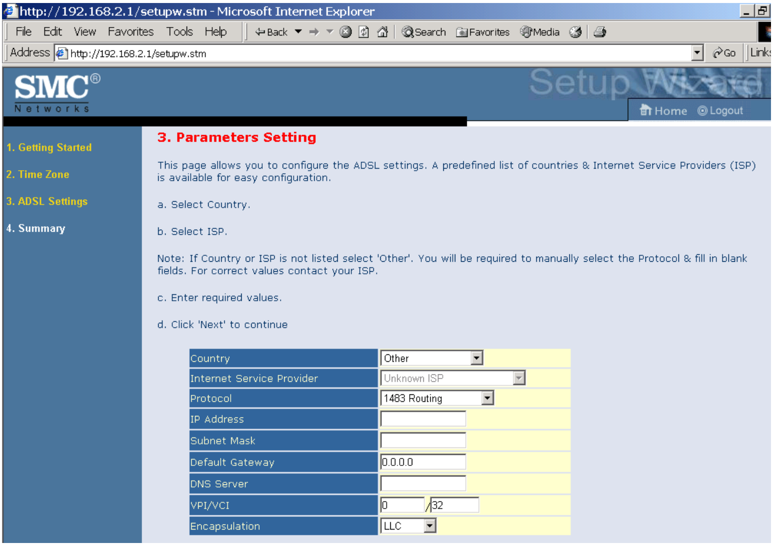
Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Bridging(Static)
IP Address	
Subnet Mask	
Default Gateway	0.0.0.0
DNS Server	
VPI/VCI	0 / 32
Encapsulation	LLC

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

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

1483 Routing


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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

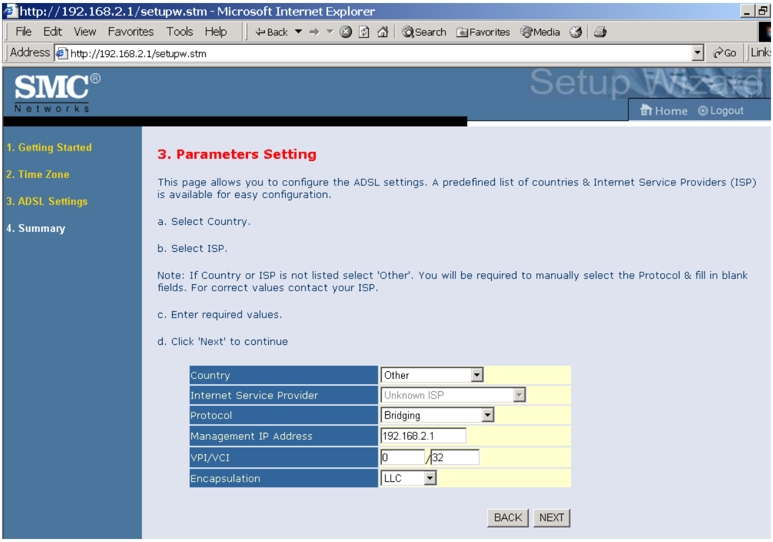
Country	Other
Internet Service Provider	Unknown ISP
Protocol	1483 Routing
IP Address	
Subnet Mask	
Default Gateway	0.0.0.0
DNS Server	
VPI/VCI	0 / 32
Encapsulation	LLC

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

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

Bridging


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

3. Parameters Setting

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

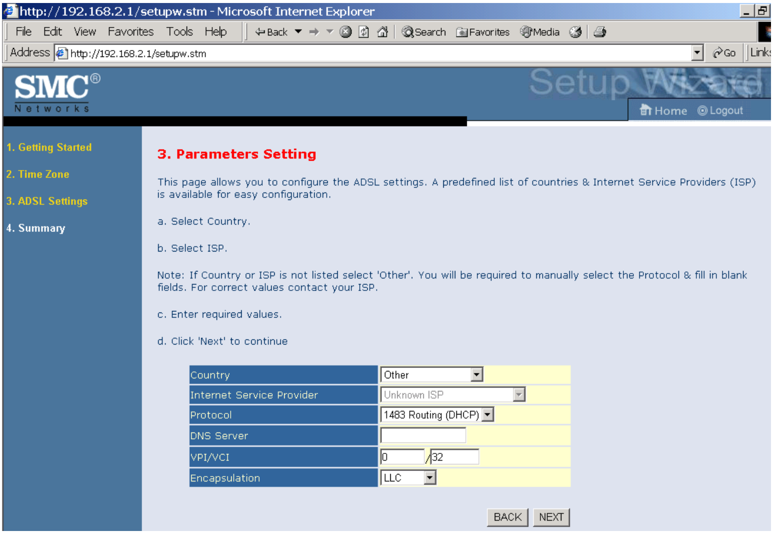
Country	Other
Internet Service Provider	Unknown ISP
Protocol	Bridging
Management IP Address	192.168.2.1
VPI/VCI	0 / 32
Encapsulation	LLC

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

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

1483 Routing (DHCP)


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://192.168.2.1/setupw.stm
Go
Links
SMC Networks
Setup Wizard
Home
Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary
BACK
NEXT

3. Parameters Setting

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 (DHCP)
DNS Server	
VPI/VCI	0 / 32
Encapsulation	LLC

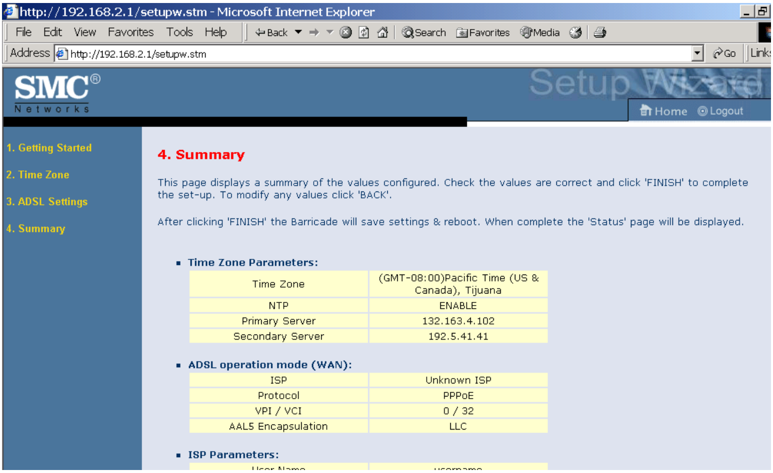
Parameter	Description
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop down menu.

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

Go to “Confirm” on page 4-14 in the manual for details about the settings.

Confirm

The Confirm screen shows a summary of the configuration parameters. Check ADSL operation mode (WAN), Network Layer Parameters (WAN) and ISP parameters are correct.


http://192.168.2.1/setupw.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/setupw.stm
Go Links
SMC® Networks
Setup Wizard
Home Logout
1. Getting Started
2. Time Zone
3. ADSL Settings
4. Summary

4. 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.

- **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	Unknown ISP
Protocol	PPPoE
VPI / VCI	0 / 32
AAL5 Encapsulation	LLC

- **ISP Parameters:**

User Name	username

Parameter	Description
ADSL Operation Mode (WAN)	
ISP	The name of the ISP you have selected from list.
Protocol	The WAN protocol of your ISP. If you are unsure if the selected protocol is correct check with your ISP.
VPI/VCI	Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). If you are unsure the VPI/VCI values are correct check with your ISP.
AAL5 Encapsulation	Shows the packet encapsulation type. If you are unsure the selected Encapsulation is correct check with your ISP. Go to page 4-21 for a detailed description.
Network Layer Parameters (WAN)	
IP Address	WAN IP address (only displayed if you have static IP).
Subnet Mask	WAN subnet mask (only displayed if you have static IP).
Default Gateway	WAN gateway (only displayed if you have static IP).

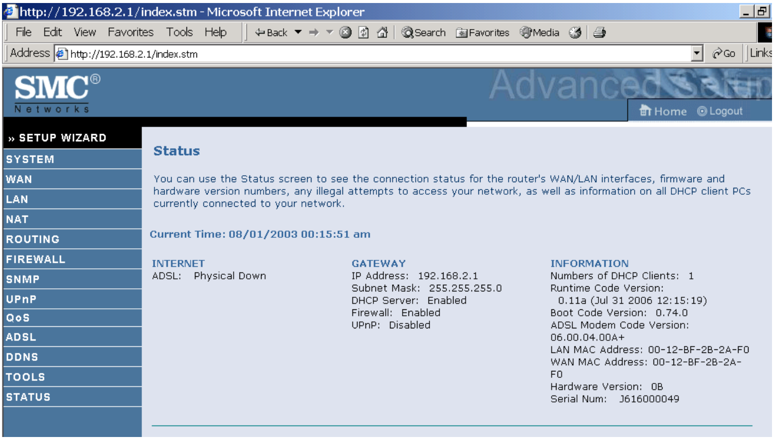
Parameter	Description
DNS Server	The IP address of the DNS server. If the DNS address field was left blank in previous steps the address will be displayed as 0.0.0.0.
ISP Parameters	
Username	The ISP assigned user name.
Password	The password (hidden).

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

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

Configuration parameters

There are 13 main menu items located on the left side of the screen.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

Status

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

Current Time: 08/01/2003 00:15:51 am

```
INTERNET                  GATEWAY                      INFORMATION
ADSL:   Physical Down     IP Address:  192.168.2.1     Numbers of DHCP Clients:  1
                          Subnet Mask:  255.255.255.0  Runtime Code Version:
                          DHCP Server:  Enabled          0.11a (Jul 31 2006 12:15:19)
                          Firewall:  Enabled           Boot Code Version:  0.74.0
                          UPnP:  Disabled              ADSL Modem Code Version:
                                                       06.00.04.00A+
                                                       LAN MAC Address: 00-12-BF-2B-2A-F0
                                                       WAN MAC Address: 00-12-BF-2B-2A-
                                                       F0
                                                       Hardware Version:  0B
                                                       Serial Num:   J616000049
```

Each main menu item is described in the following table.

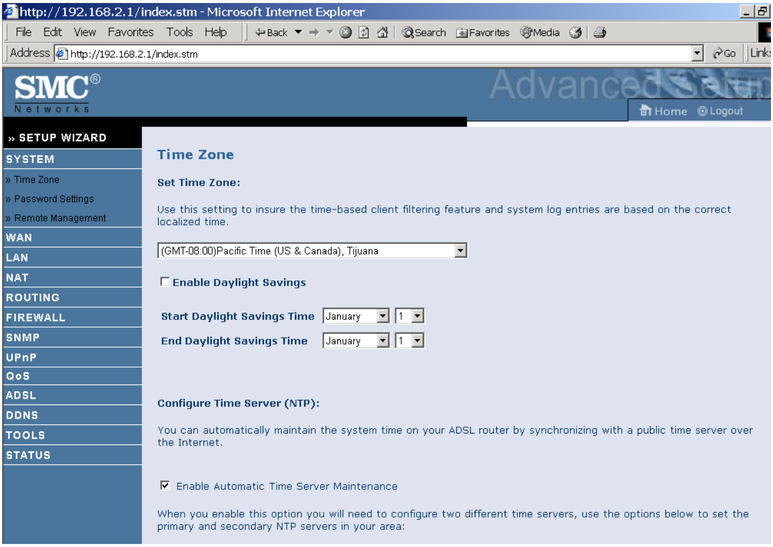
Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.
WAN	Configures the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.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

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

SYSTEM

Time Settings

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



Time Zone

Set Time Zone:

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

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

□ Enable Daylight Savings

Start Daylight Savings Time January 1

End Daylight Savings Time January 1

Configure Time Server (NTP):

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

☑ Enable Automatic Time Server Maintenance

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

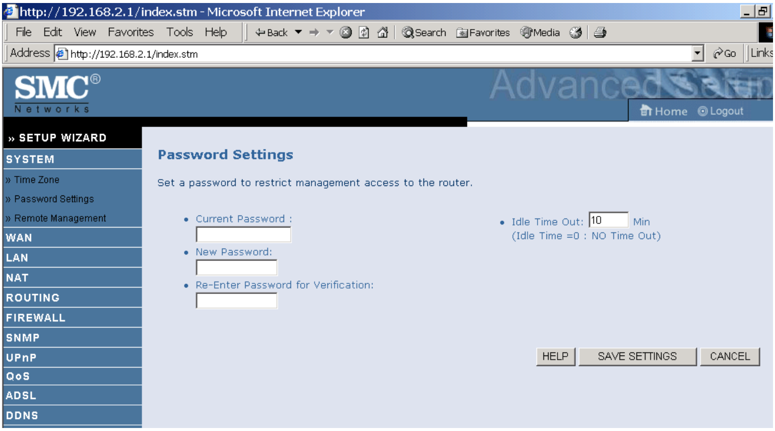
For accurate timing of log entries and system events, you need to set the time zone. Select your time zone from the drop down menu.

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

If you want to automatically synchronize the ADSL router with a public time server, check the 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.



Password Settings

Set a password to restrict management access to the router.

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

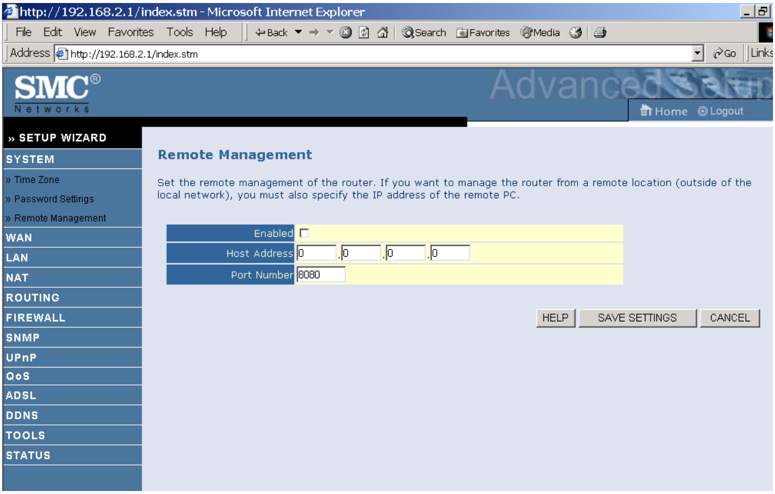
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

Note: If you lost the password, or you cannot gain access to the user interface, press the blue reset button on the rear panel, holding it down for at least 10 seconds to restore the factory defaults. The default password is “smcadmin”.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

Remote Management

By default, management access is only available to users on your local network. However, you can also manage the Barricade from a remote host by entering the IP address of a remote computer on this screen. Check the **Enabled** check box, and enter the IP address of the Host Address and click **Save Settings**.



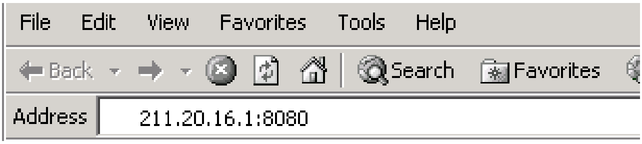
Remote Management

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

Enabled	□
Host Address	0 . 0 . 0 . 0
Port Number	8080

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

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



Address 211.20.16.1:8080

WAN

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

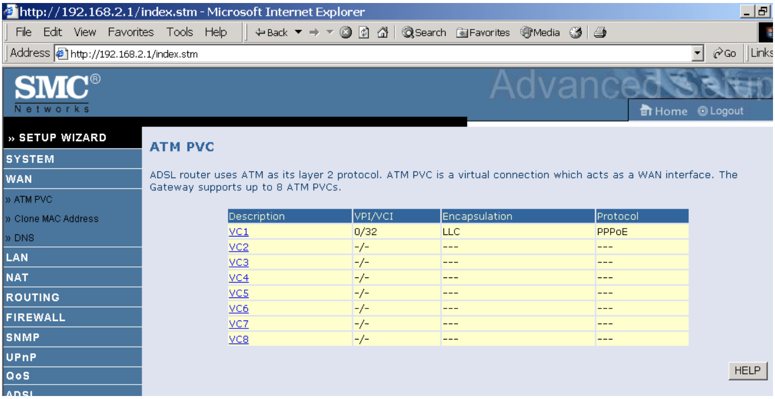
The following three items are configurable:

- ATM PVC
- Clone MAC
- DNS

ATM PVC

To configure your Internet Connection settings, select **ATM PVC**, then **VC1**. Click the VC to set the detailed parameters.

Note: The Barricade can support up to 8 Virtual Circuits (VC's). Multiple VC's, in general, are only used in the case of Triple Play (Internet/Voice/Video) services. Example: VC1 = Internet, VC2 = Voice, VC3 = Video. Unless stated by your ISP, you will use a single VC. In this case "VC1"should be used.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
» ATM PVC
» Clone MAC Address
» DNS
LAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
HELP

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.

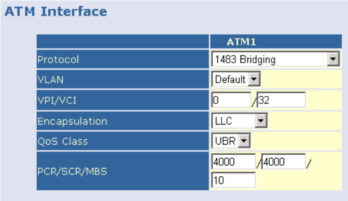
Description	VPI/VCI	Encapsulation	Protocol
VC1	0/32	LLC	PPPoE
VC2	-/-	---	---
VC3	-/-	---	---
VC4	-/-	---	---
VC5	-/-	---	---
VC6	-/-	---	---
VC7	-/-	---	---
VC8	-/-	---	---

Parameter	Description
VC1 to VC8	Click on the desired VC to configure the connection parameters.
VPI/VCI	Displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for the corresponding VC.
Encapsulation	Displays the Encapsulation configured for the corresponding VC. Encapsulation specifies how to handle multiple protocols at the ATM transport layer. • VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. • LLC: Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead).
Protocol	Displays the Protocol configured for the corresponding VC.

ATM Interface

1483 Bridging

Enter the settings provided by your ISP. In Bridging mode the Barricade will act as a bridge passing the IP addressing directly to the attached client PC.

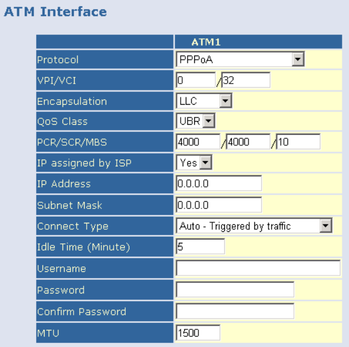


ATM Interface

	ATM1
Protocol	1483 Bridging
VLAN	Default
VPI/VCI	0 / 32
Encapsulation	LLC
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



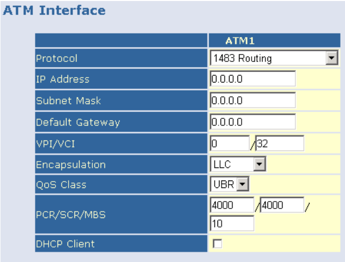
ATM Interface

	ATM1
Protocol	PPPoA
VPI/VCI	0 / 32
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Auto - Triggered by traffic
Idle Time (Minute)	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 the IP address was provided by your ISP
IP Address	Enter the IP address provided by your ISP. For dynamic IP leave this field blank.
Subnet Mask	Enter the subnet mask address provided by your ISP. For dynamic IP leave this field blank.
Connect Type	Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic.
Username	Enter user name.
Password	Enter password.

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

1483 Routing

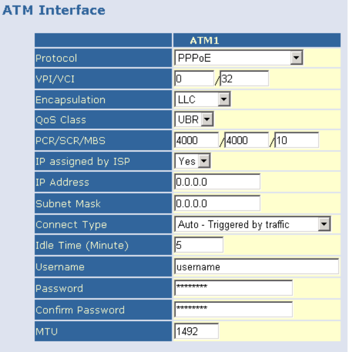


ATM Interface

	ATM1
Protocol	1483 Routing ▾
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
VPI/VCI	0 / 32
Encapsulation	LLC ▾
QoS Class	UBR ▾
PCR/SCR/MBS	4000 / 4000 / 10
DHCP Client	☐

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

PPPoE



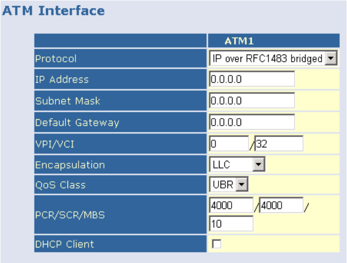
ATM Interface

	ATM1
Protocol	PPPoE
VPI/VCI	0 /32
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 /4000 /10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Auto - Triggered by traffic
Idle Time (Minute)	5
Username	username
Password	********
Confirm Password	********
MTU	1492

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

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

IP Over RFC1483 bridged



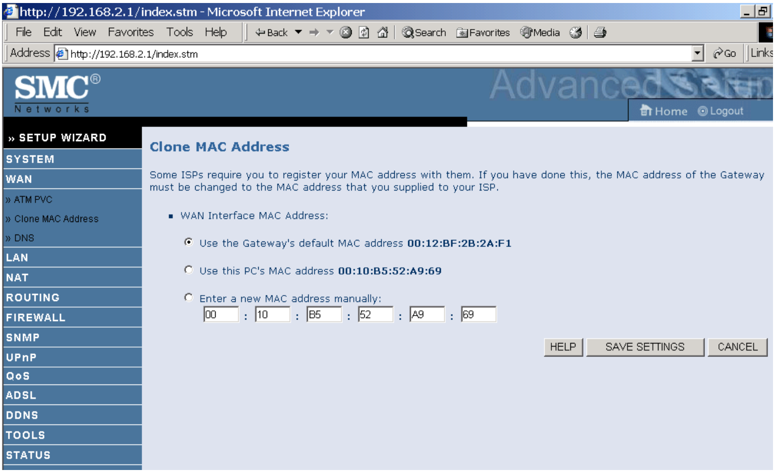
ATM Interface

	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	0 / 32
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 4000 / 10
DHCP Client	□

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

Clone MAC Address

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



Clone MAC Address

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

- WAN Interface MAC Address:

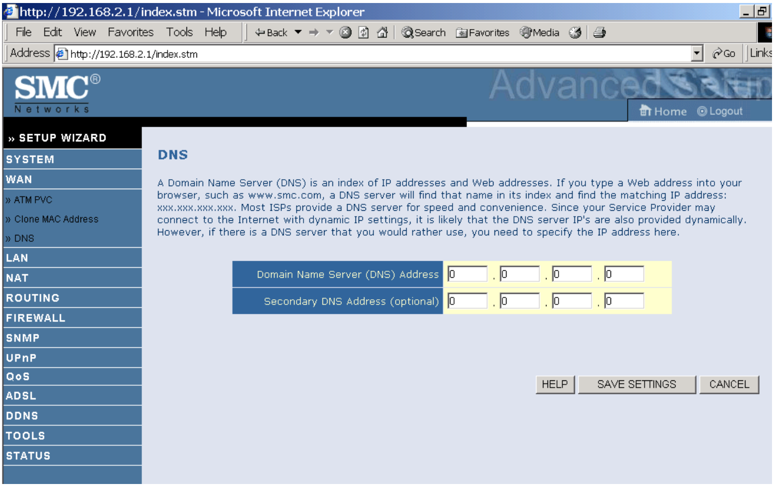
● Use the Gateway's default MAC address **00:12:BF:2B:2A:F1**

○ Use this PC's MAC address **00:10:B5:52:A9:69**

○ Enter a new MAC address manually:
00 : 10 : B5 : 52 : A9 : 69

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.



DNS

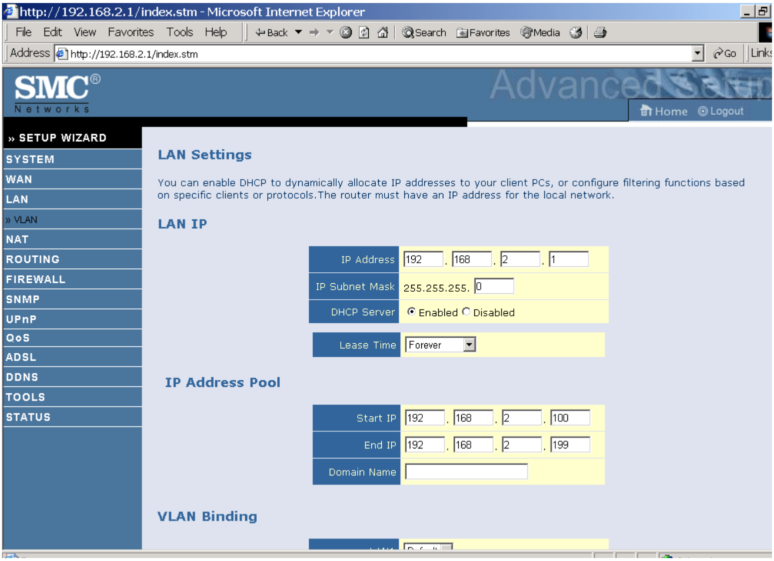
A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

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

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

LAN

The LAN settings menu allows you to change the default IP address of the Barricade, modify the DHCP server settings and create VLAN's.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
» VLAN
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
Lease Time	Forever

IP Address Pool

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

VLAN Binding

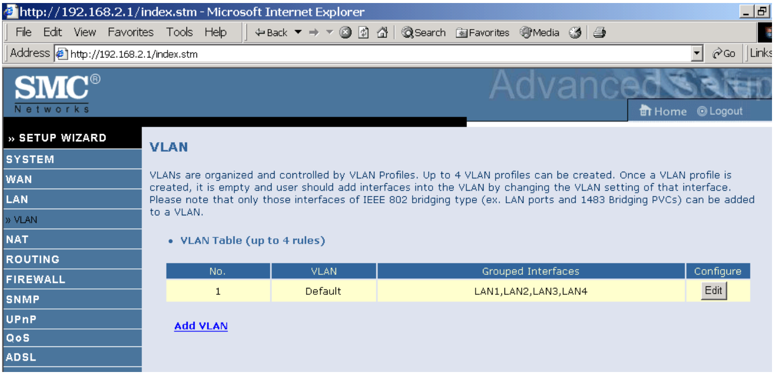
Parameter	Description
LAN IP	
IP Address	The IP address of the Barricade.
IP Subnet Mask	The subnet mask of the Barricade.
DHCP Server	This option allows you to enable or disable the DHCP server function. By default DHCP is enabled.
VLAN Binding	
LAN1 to LAN4	This option allows you to change VLAN membership of LAN ports 1-4. By default all LAN ports are assigned to the "default" VLAN.
DHCP Server	
DHCP Server ID	Allows you to define a name for the DHCP server.

Parameter	Description
Lease Time	Allows you to select a pre-defined lease time for IP addresses assigned using DHCP. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
IP Address Pool	
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the gateway address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.
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

The Barricade's VLAN function can be used to create up to 4 VLAN profiles. Once a VLAN profile is created interfaces can be assigned to the VLAN profile. This is done by setting the VLAN binding.

Notes: Only interfaces of IEEE 802 bridging type (LAN ports 1-4 and 1483 Bridging PVC's) can be assigned to a VLAN.



VLAN

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.

- VLAN Table (up to 4 rules)

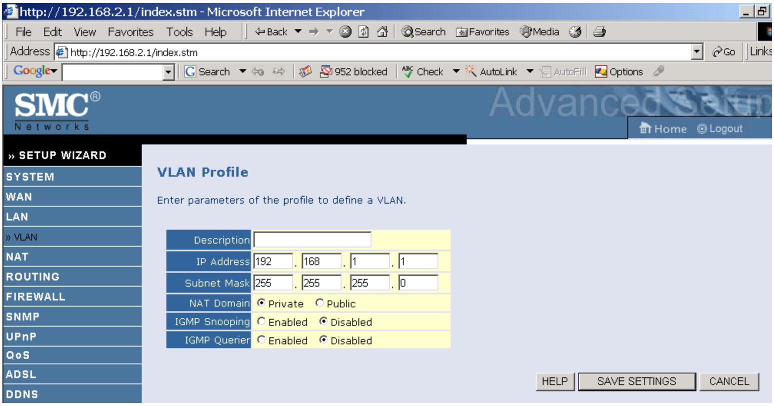
No.	VLAN	Grouped Interfaces	Configure
1	Default	LAN1,LAN2,LAN3,LAN4	Edit

Add VLAN

Click **Add VLAN** to create a profile.

VLAN Profile

Configure the VLAN settings in this screen.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
Google Search 952 blocked Check AutoLink AutoFill Options
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
» VLAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
HELP
SAVE SETTINGS
CANCEL

VLAN Profile

Enter parameters of the profile to define a VLAN.

Description	
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
NAT Domain	● Private ○ Public
IGMP Snooping	○ Enabled ● Disabled
IGMP Querier	○ Enabled ● Disabled

- Description: Enter a description for the VLAN group, for example: Admin PC's

- IP Address: Enter IP address for the VLAN.

- Subnet Mask: Enter Subnet Mask address for the VLAN.

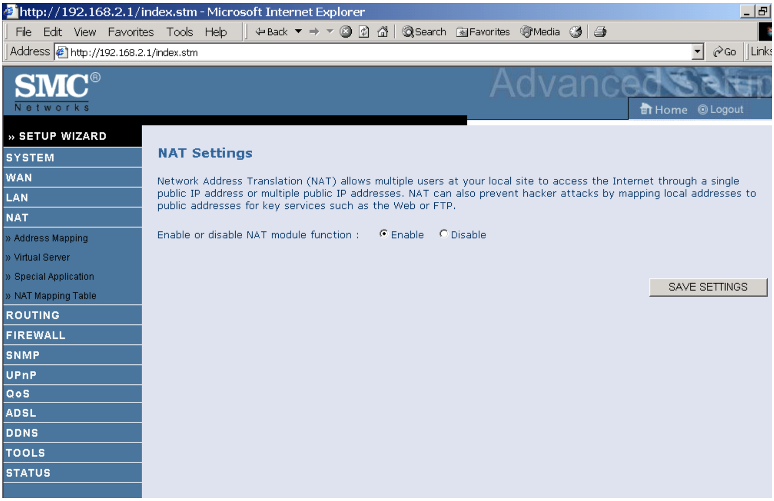
- NAT Domain: Set NAT Domain to private or public.

- IGMP Snooping: 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: IGMP Querier: if the IGMP Querier is enabled, then the router will periodically query all multicast group members on the specified VLAN.

NAT

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



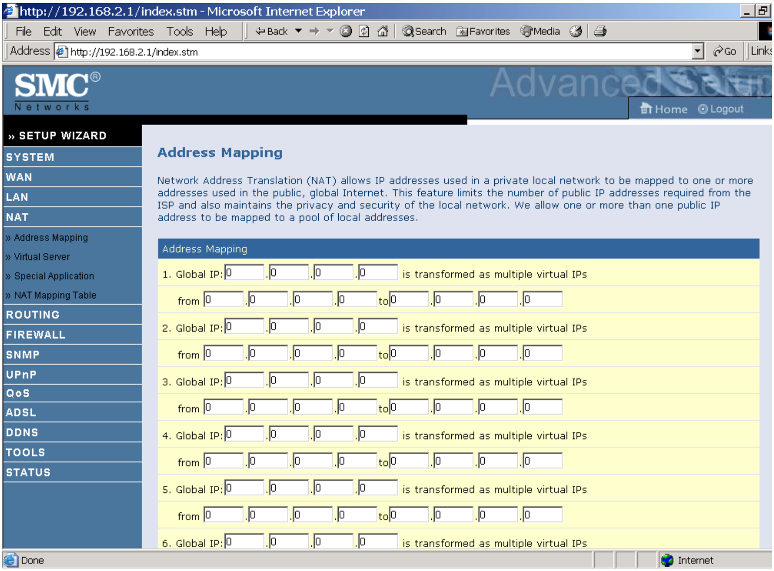
NAT Settings

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

Enable or disable NAT module function : ● Enable ○ Disable

Address Mapping

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



Address Mapping

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

Address Mapping

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

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

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

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

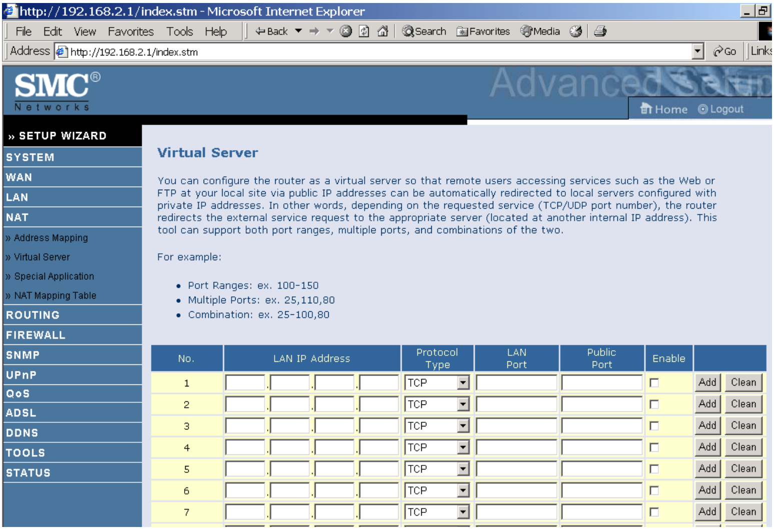
5. Global IP: 0 .0 .0 .0 is transformed as multiple virtual IPs
from 0 .0 .0 .0 to 0 .0 .0 .0

6. Global IP: 0 .0 .0 .0 is transformed as multiple virtual IPs

- Enter the Public IP address you wish to share into the Global IP field.
- Enter a range of internal IPs that will share the global IP into the “from” field.

Virtual Server

If you configure the Barricade as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address).



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	. . .	TCP			□	Add Clean
2	. . .	TCP			□	Add Clean
3	. . .	TCP			□	Add Clean
4	. . .	TCP			□	Add Clean
5	. . .	TCP			□	Add Clean
6	. . .	TCP			□	Add Clean
7	. . .	TCP			□	Add Clean

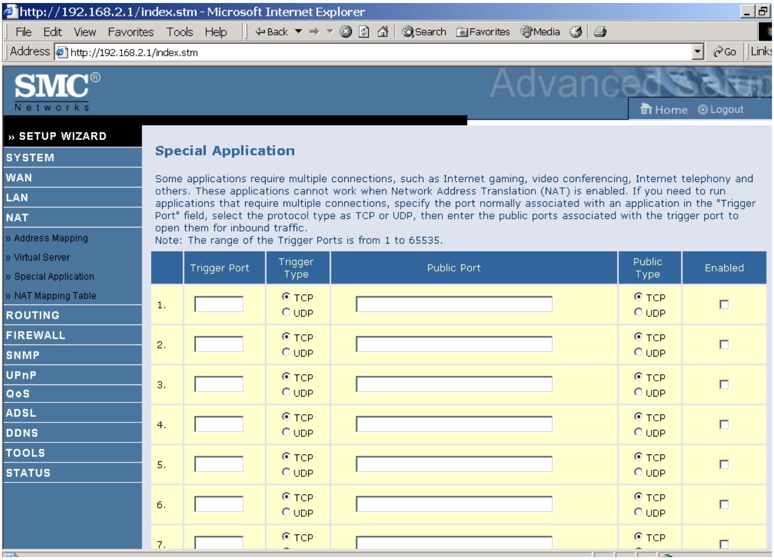
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they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

The more common TCP service ports include:
HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

A list of ports is maintained at the following link:
http://www.iana.org/assignments/port-numbers.

Special Application

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



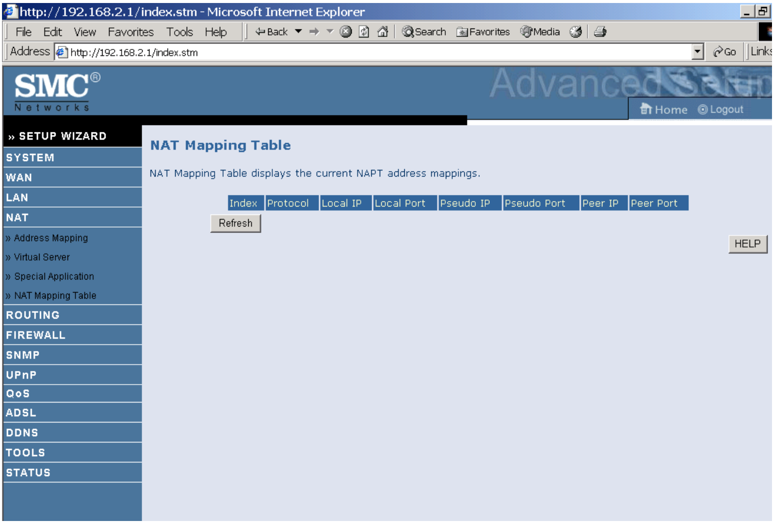
Special Application

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

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.		● TCP ○ UDP		● TCP ○ UDP	□
2.		● TCP ○ UDP		● TCP ○ UDP	□
3.		● TCP ○ UDP		● TCP ○ UDP	□
4.		● TCP ○ UDP		● TCP ○ UDP	□
5.		● TCP ○ UDP		● TCP ○ UDP	□
6.		● TCP ○ UDP		● TCP ○ UDP	□
7.		● TCP		● TCP	□

NAT Mapping Table

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



NAT Mapping Table

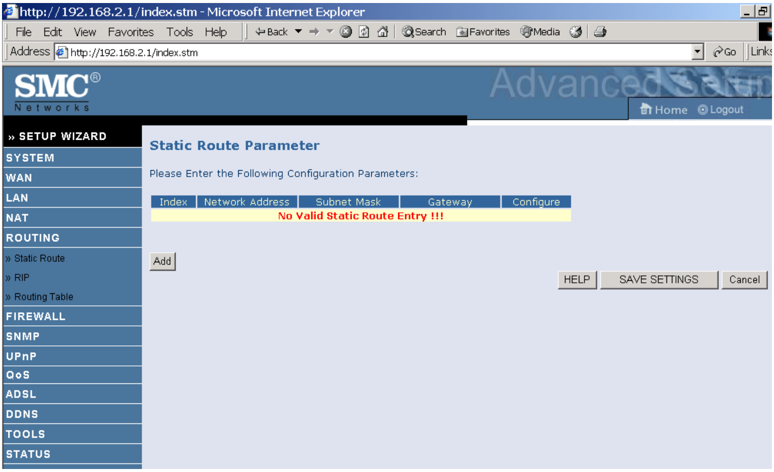
NAT Mapping Table displays the current NAPT address mappings.

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

ROUTING

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

Static Route



Static Route Parameter

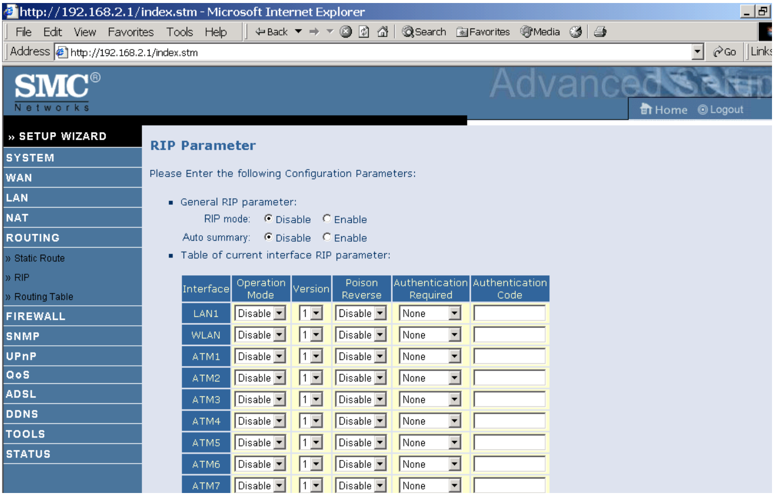
Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
No Valid Static Route Entry !!!				

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


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
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:

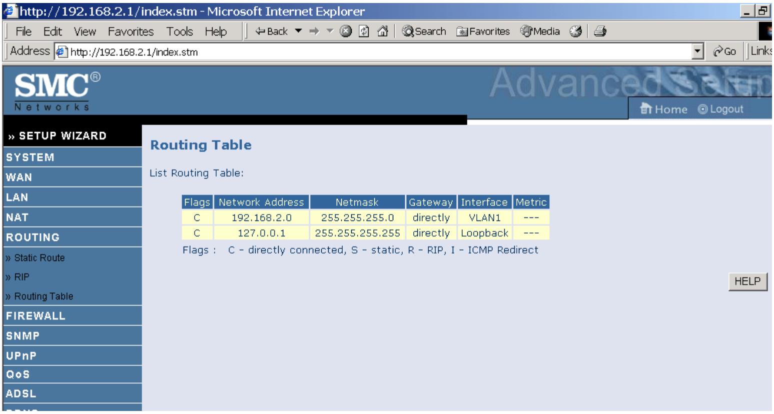
Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
LAN1	Disable	1	Disable	None	
WLAN	Disable	1	Disable	None	
ATM1	Disable	1	Disable	None	
ATM2	Disable	1	Disable	None	
ATM3	Disable	1	Disable	None	
ATM4	Disable	1	Disable	None	
ATM5	Disable	1	Disable	None	
ATM6	Disable	1	Disable	None	
ATM7	Disable	1	Disable	None	

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

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

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

Routing Table



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

Parameter	Description

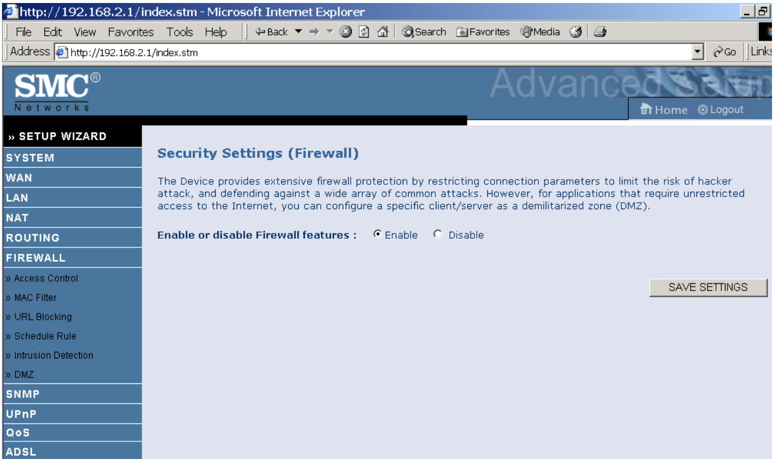
Flags	Indicates the route status:
	C = Direct connection on the same subnet.
	S = Static route.
	R = RIP (Routing Information Protocol) assigned route.
	I = ICMP (Internet Control Message Protocol) Redirect route.

Network Address	Destination IP address.
Netmask	The subnetwork associated with the destination. This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the subnet mask number; each bit that corresponds to “0” is part of the host number.
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

FIREWALL

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

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



Security Settings (Firewall)

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

Enable or disable Firewall features : ● Enable ○ Disable

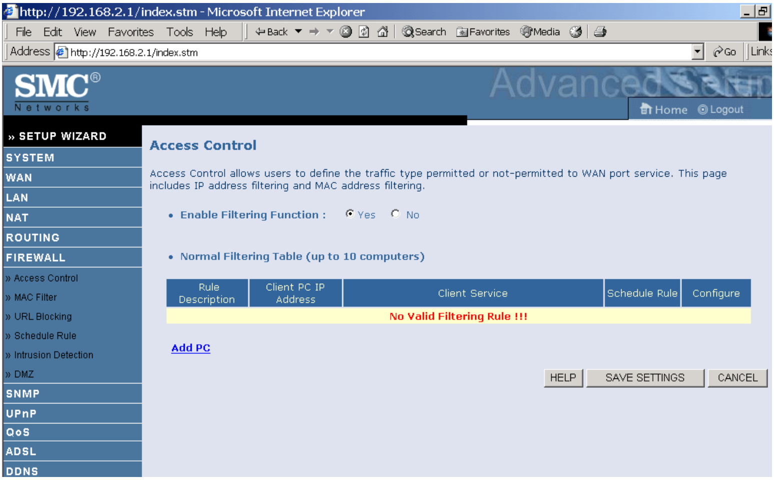
The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (For details see page 4-49.)

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

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

Access Control

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



Access Control

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

- Enable Filtering Function : ● Yes ○ No
- Normal Filtering Table (up to 10 computers)

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

The following items are on the Access Control screen:

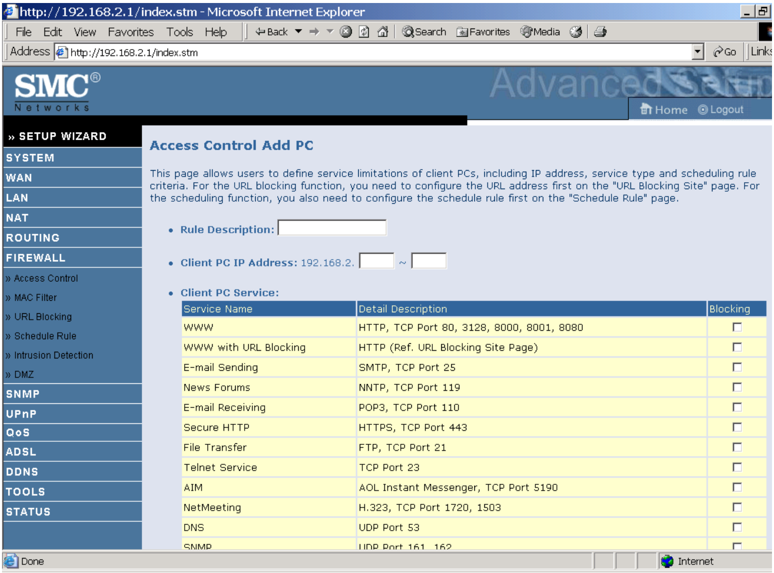
Parameter	Description
Enable Filtering Function	Enable or Disable Access control function.
Normal Filtering Table	Displays descriptive list of filtering rules defined.

To create a new access control rule:

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

2. Define the appropriate settings for client PC services.

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



Access Control Add PC

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

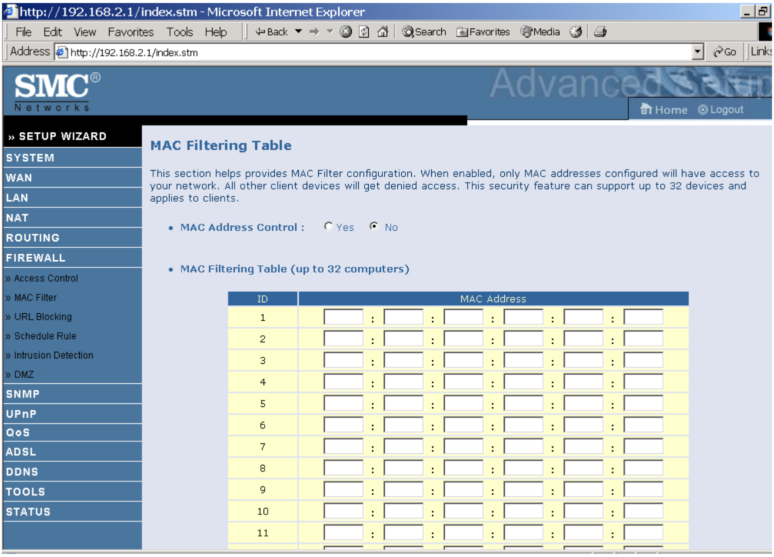
- **Rule Description:**
- **Client PC IP Address:** 192.168.2. ~
- **Client PC Service:**

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

MAC Filter

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

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



MAC Filtering Table

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

- MAC Address Control : ○ Yes ● No

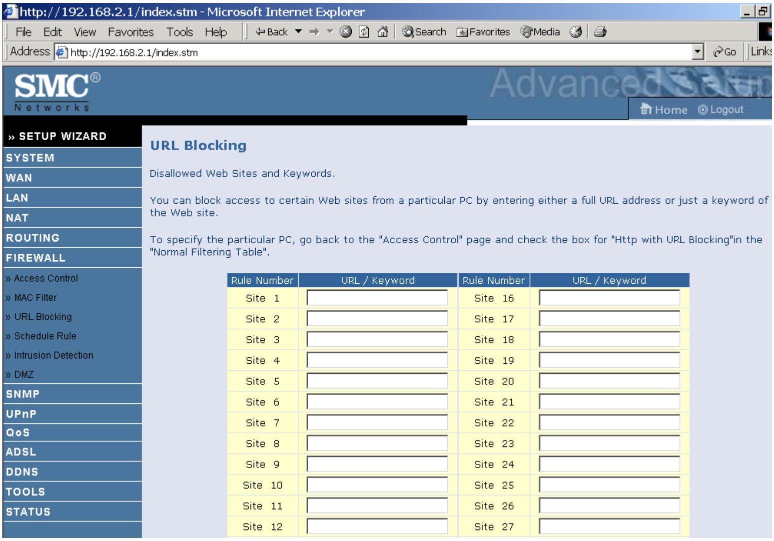
- MAC Filtering Table (up to 32 computers)

ID	MAC Address
1	: : : : :
2	: : : : :
3	: : : : :
4	: : : : :
5	: : : : :
6	: : : : :
7	: : : : :
8	: : : : :
9	: : : : :
10	: : : : :
11	: : : : :

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

URL Blocking

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



URL Blocking

Disallowed Web Sites and Keywords.

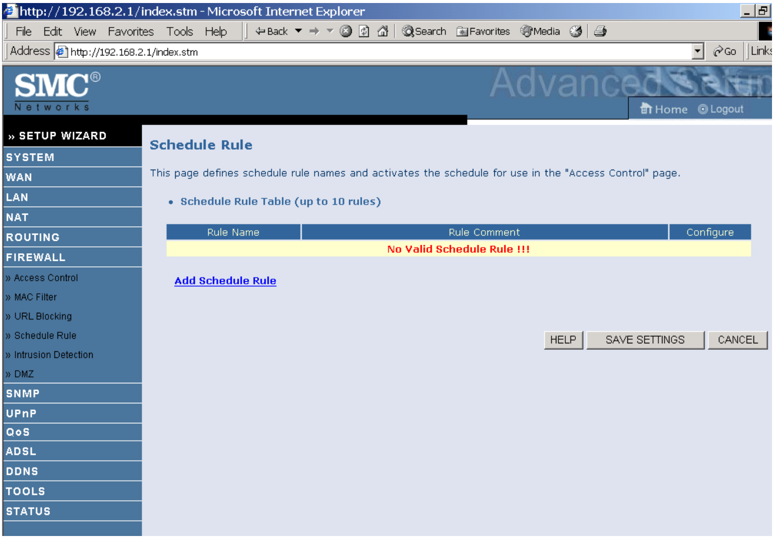
You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

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	

Schedule Rule

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



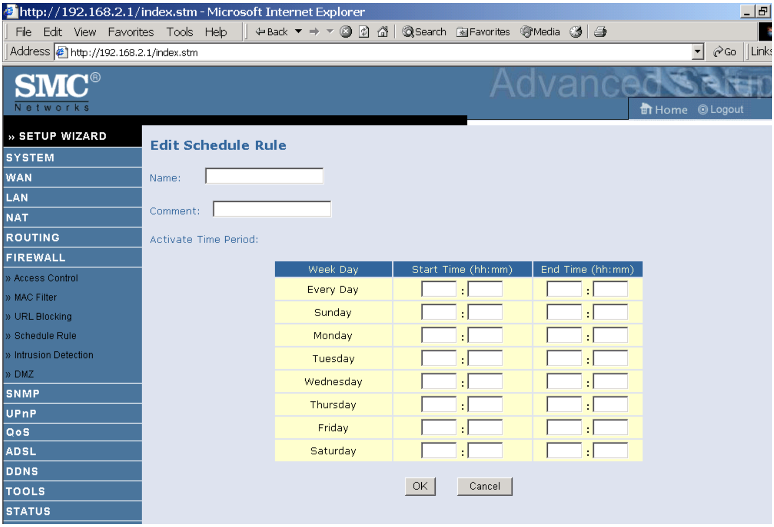
Schedule Rule

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

- Schedule Rule Table (up to 10 rules)

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

Follow these steps to add a schedule rule:



Edit Schedule Rule

Name:

Comment:

Activate Time Period:

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

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

2. Define the appropriate settings for a schedule rule.

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

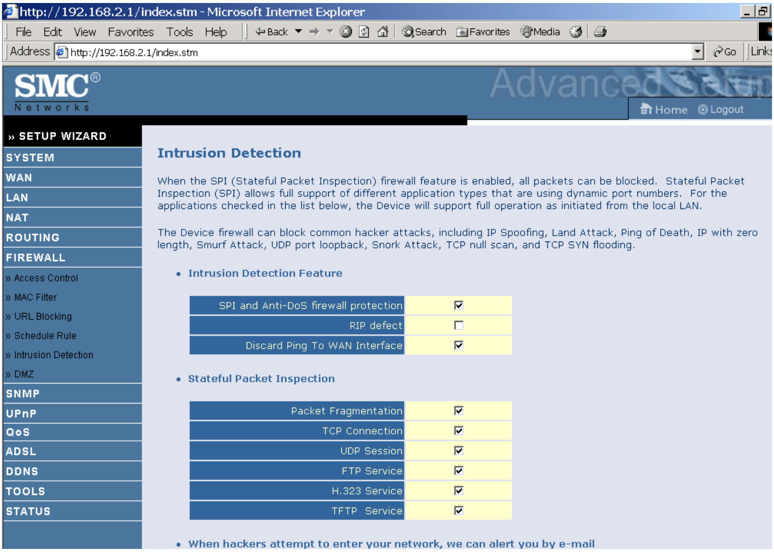
Intrusion Detection

- ### Intrusion Detection Feature

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

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

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



Intrusion Detection

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

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

- Intrusion Detection Feature

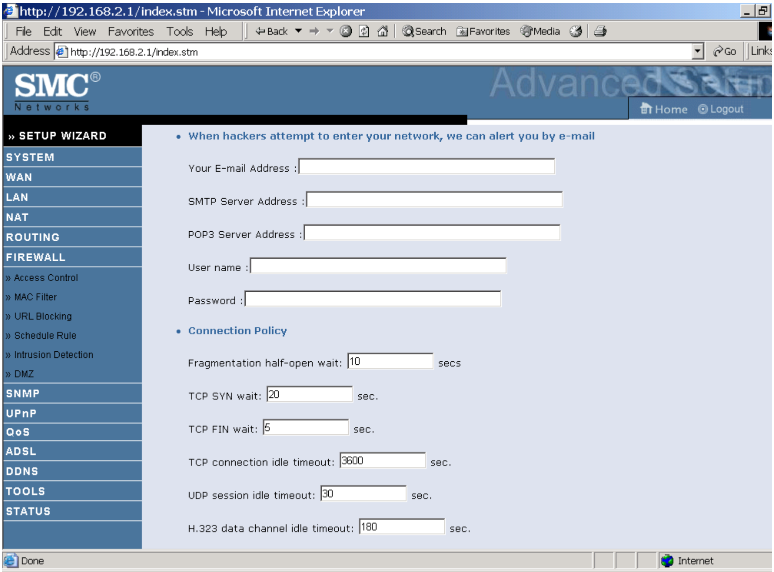
SPI and Anti-DoS firewall protection	☑
RIP defect	☐
Discard Ping To WAN Interface	☑

- Stateful Packet Inspection

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

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

Scroll down to view more information.



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

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :

- Connection Policy

Fragmentation half-open wait: 10 secs

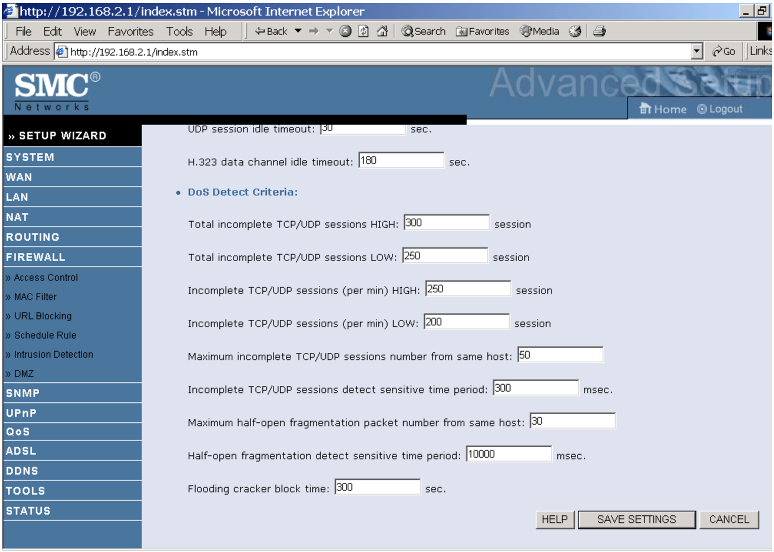
TCP SYN wait: 20 sec.

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.



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.

- **Stateful Packet Inspection**

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

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

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

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

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

- **Connection Policy**

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

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

- **DoS Criteria and Port Scan Criteria**

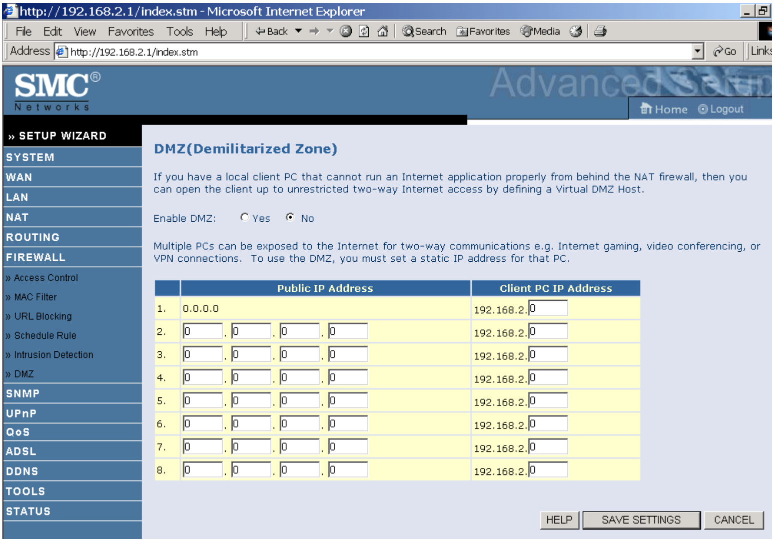
Set up DoS and port scan criteria in the spaces provided (as shown below).

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

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

DMZ

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



DMZ(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.

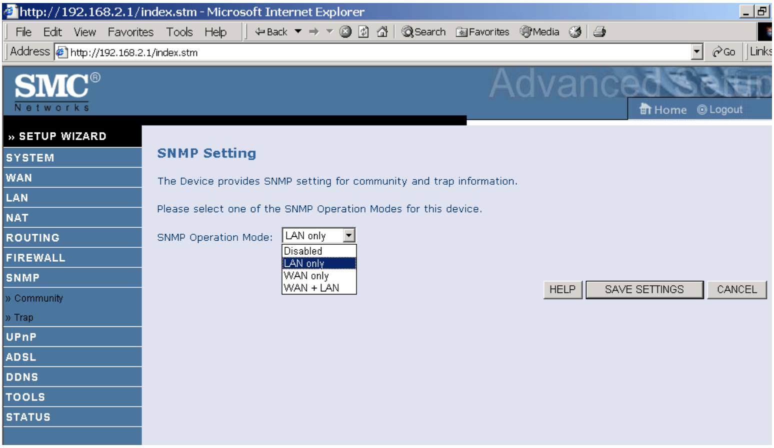
Enable DMZ: ○ Yes ● No

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.	0 . 0 . 0 . 0	192.168.2.0
3.	0 . 0 . 0 . 0	192.168.2.0
4.	0 . 0 . 0 . 0	192.168.2.0
5.	0 . 0 . 0 . 0	192.168.2.0
6.	0 . 0 . 0 . 0	192.168.2.0
7.	0 . 0 . 0 . 0	192.168.2.0
8.	0 . 0 . 0 . 0	192.168.2.0

SNMP

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



SNMP Setting

The Device provides SNMP setting for community and trap information.

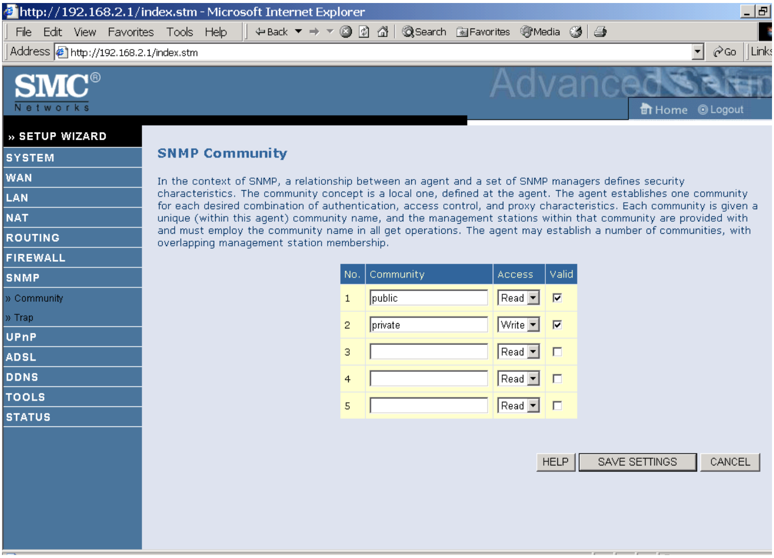
Please select one of the SNMP Operation Modes for this device.

SNMP Operation Mode: LAN only

Select the SNMP Operation mode from the drop down menu.

Community

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



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.

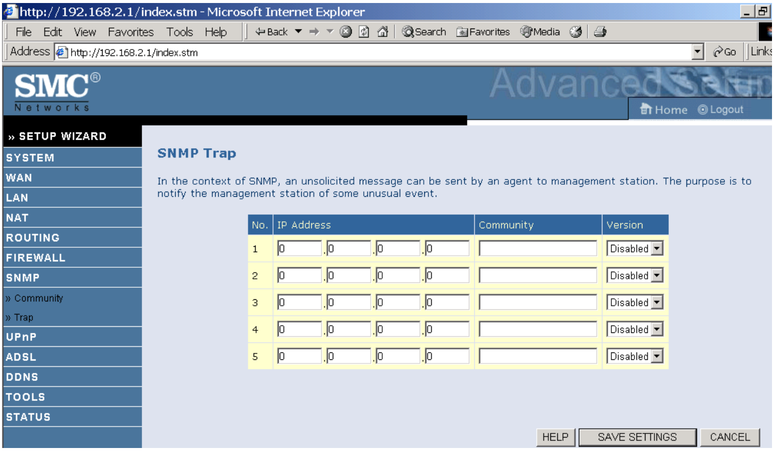
No.	Community	Access	Valid
1	public	Read	☑
2	private	Write	☑
3		Read	□
4		Read	□
5		Read	□

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.



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.

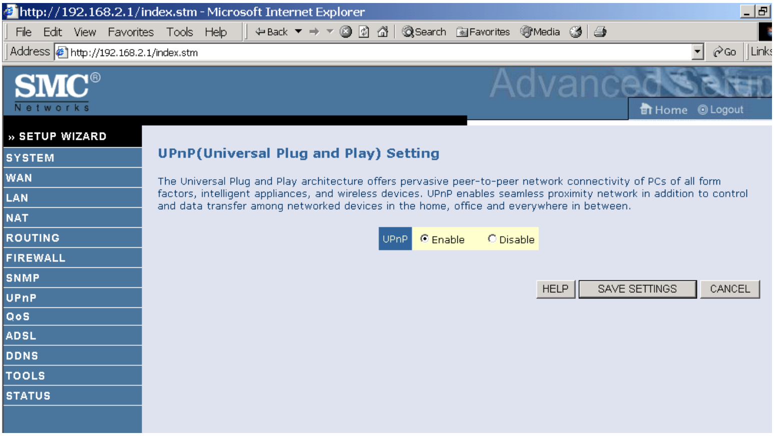
No.	IP Address	Community	Version
1	0 . 0 . 0 . 0		Disabled
2	0 . 0 . 0 . 0		Disabled
3	0 . 0 . 0 . 0		Disabled
4	0 . 0 . 0 . 0		Disabled
5	0 . 0 . 0 . 0		Disabled

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(Universal Plug and Play) Setting

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

UPnP ● Enable ○ Disable

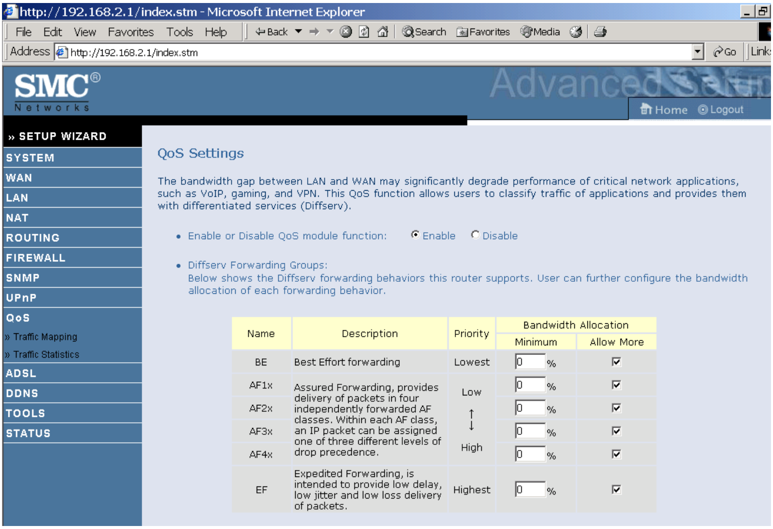
UPnP allows the device to automatically:

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

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

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.



QoS Settings

The bandwidth gap between LAN and WAN may significantly degrade performance of critical network applications, such as VoIP, gaming, and VPN. This QoS function allows users to classify traffic of applications and provides them with differentiated services (Diffserv).

- Enable or Disable QoS module function: ● Enable ○ Disable
- Diffserv Forwarding Groups:
  Below shows the Diffserv forwarding behaviors this router supports. User can further configure the bandwidth allocation of each forwarding behavior.

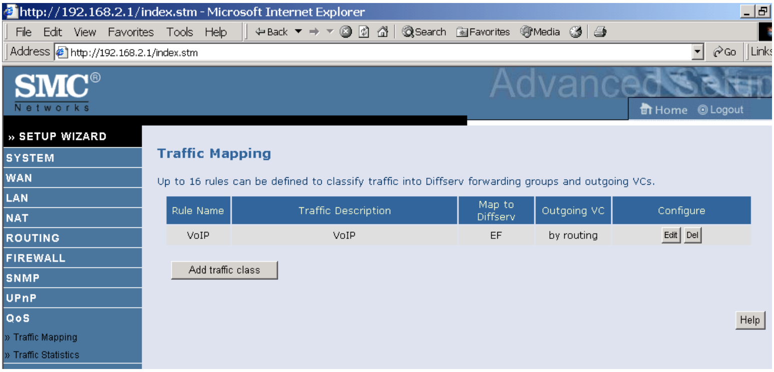
Name	Description	Priority	Bandwidth Allocation	
			Minimum	Allow More
BE	Best Effort forwarding	Lowest	0 %	☑
AF1x	Assured Forwarding, provides delivery of packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence.	Low	0 %	☑
AF2x		↑	0 %	☑
AF3x		↓	0 %	☑
AF4x		High	0 %	☑
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.	Highest	0 %	☑

Parameter	Description
Enable or disable QoS module function	Check to enable or disable this function.
BE	Best Effort, network forwards as many packets as possible in as reasonable a time as possible. This is the default per-hop behavior (PHB) for packet transmission.
AF1x, AF2x AF3x, AF4x	Set the percentage for four different types of Assured Forwarding.
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.

- Assured forwarding, defined in RFC 2597
- Expedited forwarding, defined in RFC 2598

Traffic Mapping

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

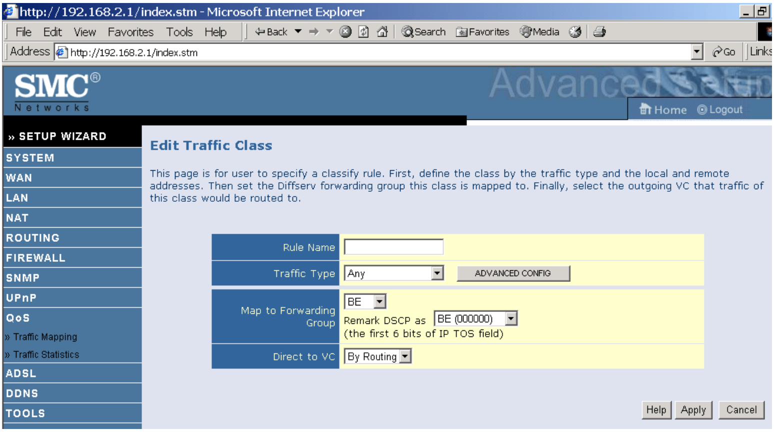


Traffic Mapping

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

Click **Add traffic class** to set the parameter details.



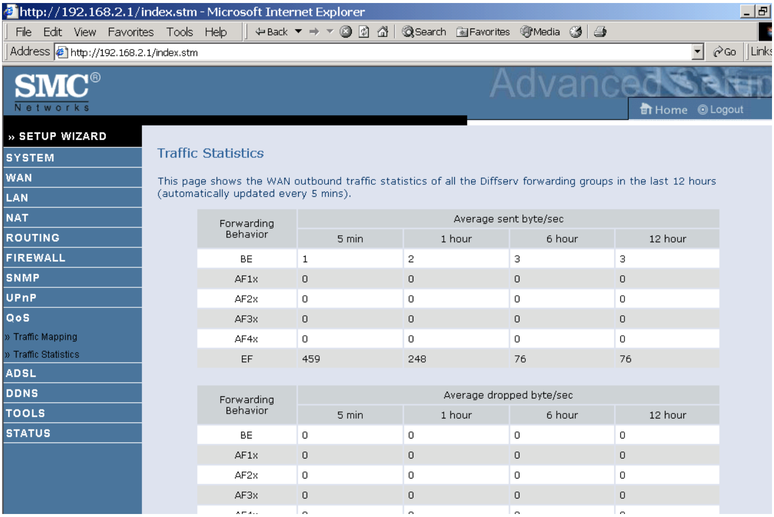
Edit Traffic Class

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	
Traffic Type	Any
Map to Forwarding Group	BE Remark DSCP as BE (000000) (the first 6 bits of IP TOS field)
Direct to VC	By Routing

Traffic Statistics

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



http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
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	1	2	3	3
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	459	248	76	76

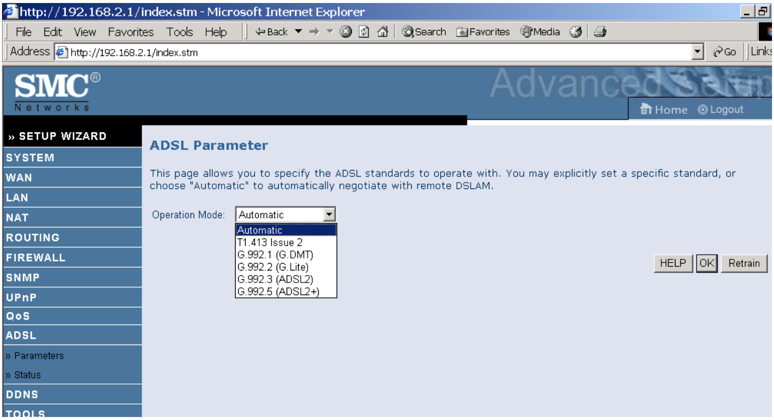
Forwarding Behavior	Average dropped byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0

ADSL

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

ADSL Parameters

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



ADSL Parameter

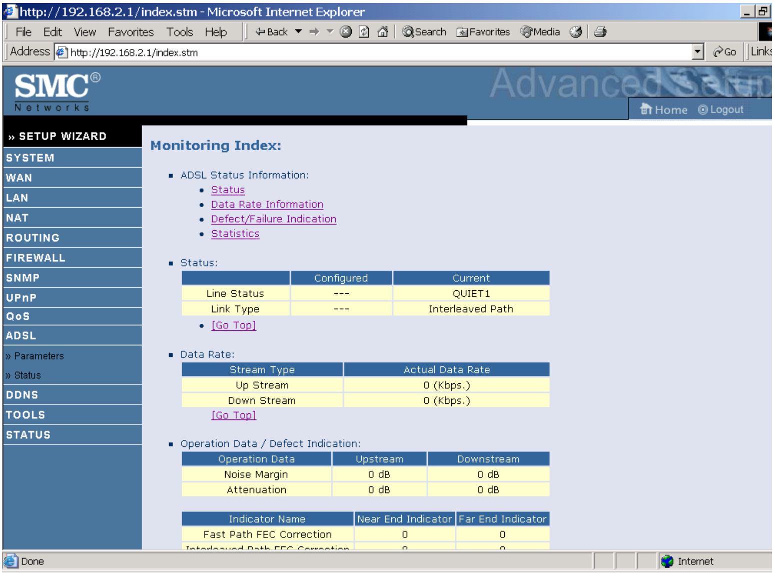
This page allows you to specify the ADSL standards to operate with. You may explicitly set a specific standard, or choose "Automatic" to automatically negotiate with remote DSLAM.

Operation Mode: Automatic

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

ADSL Status

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


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC® Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
» Parameters
» Status
DDNS
TOOLS
STATUS
Done
Internet

Monitoring Index:

- ADSL Status Information:
  - Status
  - Data Rate Information
  - Defect/Failure Indication
  - Statistics

- Status:

	Configured	Current
Line Status	---	QUIET1
Link Type	---	Interleaved Path

  - [Go Top]

- Data Rate:

Stream Type	Actual Data Rate
Up Stream	0 (Kbps.)
Down Stream	0 (Kbps.)

[Go Top]

- Operation Data / Defect Indication:

Operation Data	Upstream	Downstream
Noise Margin	0 dB	0 dB
Attenuation	0 dB	0 dB

Indicator Name	Near End Indicator	Far End Indicator
Fast Path FEC Correction	0	0
Interleaved Path FEC Correction	0	0

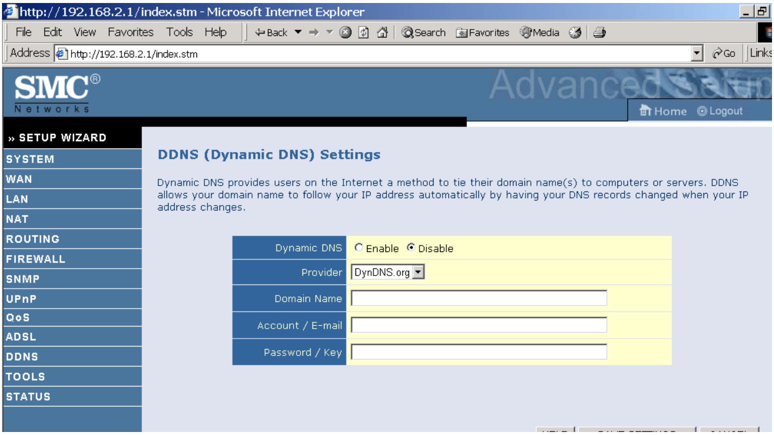
The following items are included on this information screen:

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

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

DDNS

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



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.

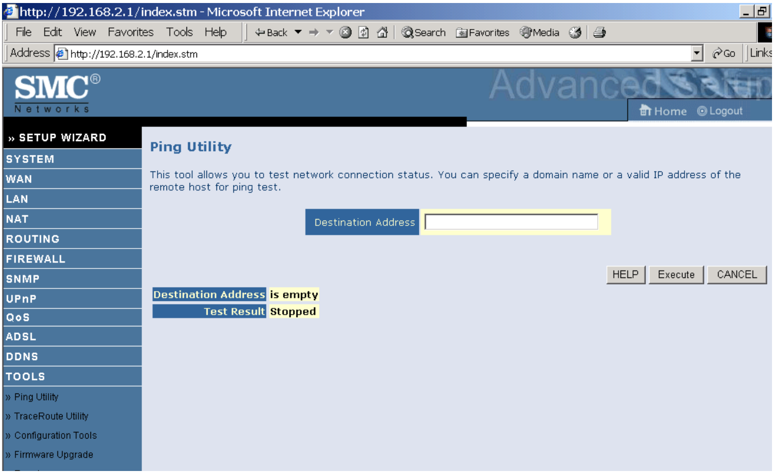
Dynamic DNS	○ Enable ● Disable
Provider	DynDNS.org
Domain Name	
Account / E-mail	
Password / Key	

TOOLS

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

Ping Utility

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



Ping Utility

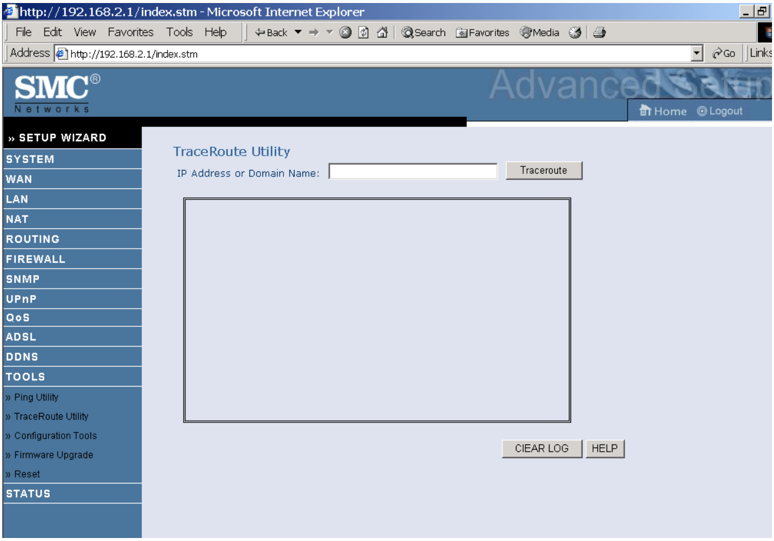
This tool allows you to test network connection status. You can specify a domain name or a valid IP address of the remote host for ping test.

Destination Address

Destination Address	is empty
Test Result	Stopped

Trace Route Utility

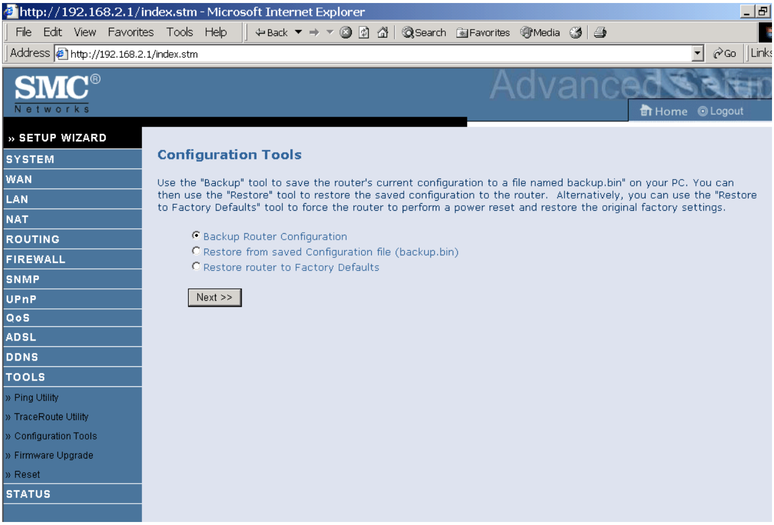
Traceroute is a TCP/IP utility which allows the user to determine the route packets take to reach a particular host.



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

Configuration Tools

Choose a function and click **Next**.



Configuration Tools

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

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

Next >>

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

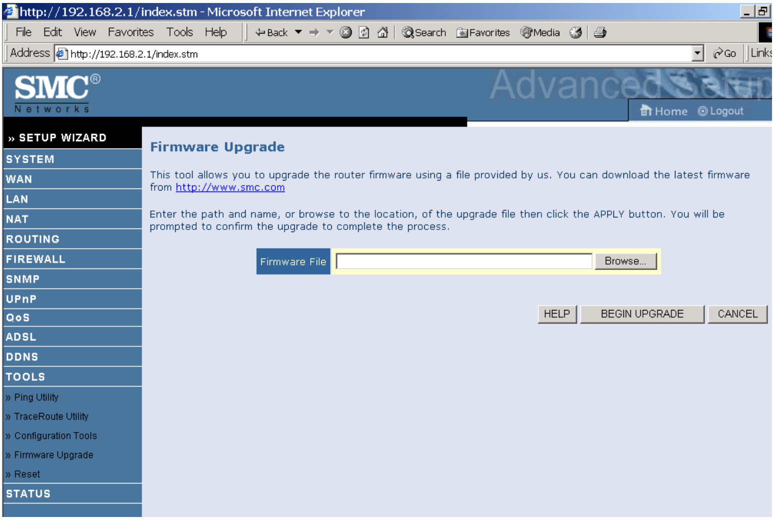
Firmware Upgrade

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

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

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

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



Firmware Upgrade

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

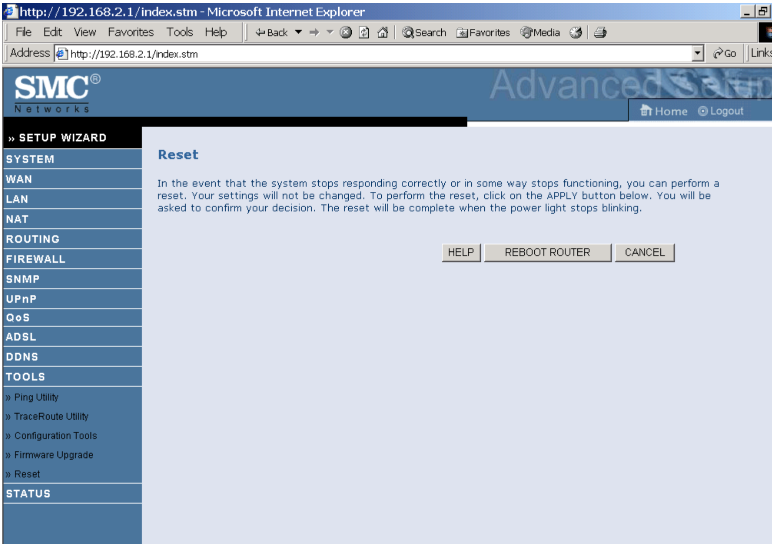
Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.

Firmware File [ ] Browse...

HELP | BEGIN UPGRADE | CANCEL

Reset

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



Reset

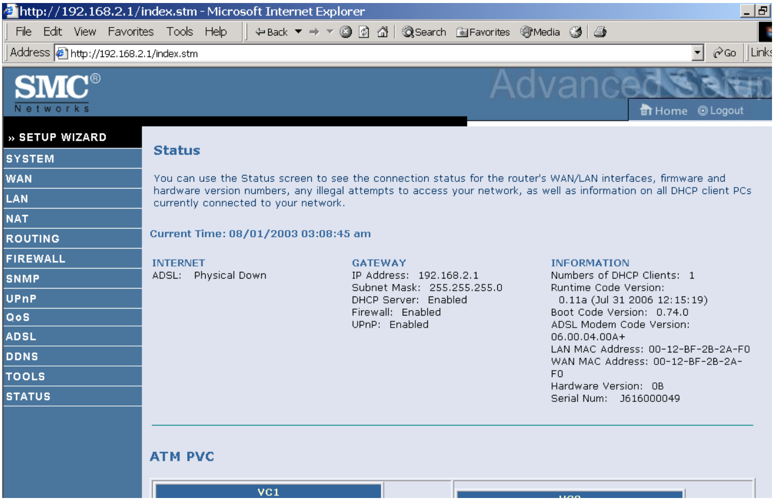
In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The reset will be complete when the power light stops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

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

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

STATUS

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



Status

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

Current Time: 08/01/2003 03:08:45 am

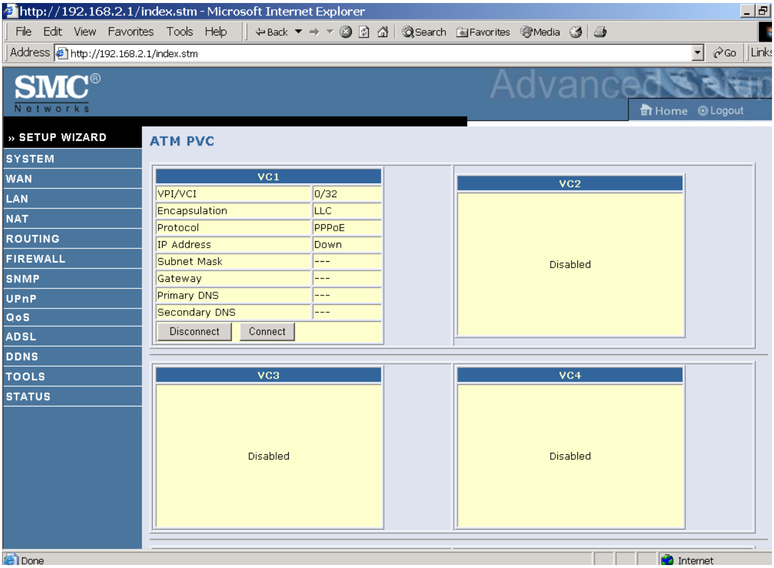
INTERNET
ADSL: Physical Down

GATEWAY
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
Firewall: Enabled
UPnP: Enabled

INFORMATION
Numbers of DHCP Clients: 1
Runtime Code Version:
0.11a (Jul 31 2006 12:15:19)
Boot Code Version: 0.74.0
ADSL Modem Code Version:
06.00.04.00A+
LAN MAC Address: 00-12-BF-2B-2A-F0
WAN MAC Address: 00-12-BF-2B-2A-F0
Hardware Version: 0B
Serial Num: J616000049

ATM PVC

Scroll down to view more information on the Status screen.


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS
Done
Internet

ATM PVC

VC1	
VPI/VCI	0/32
Encapsulation	LLC
Protocol	PPPoE
IP Address	Down
Subnet Mask	---
Gateway	---
Primary DNS	---
Secondary DNS	---

Disconnect Connect

VC2

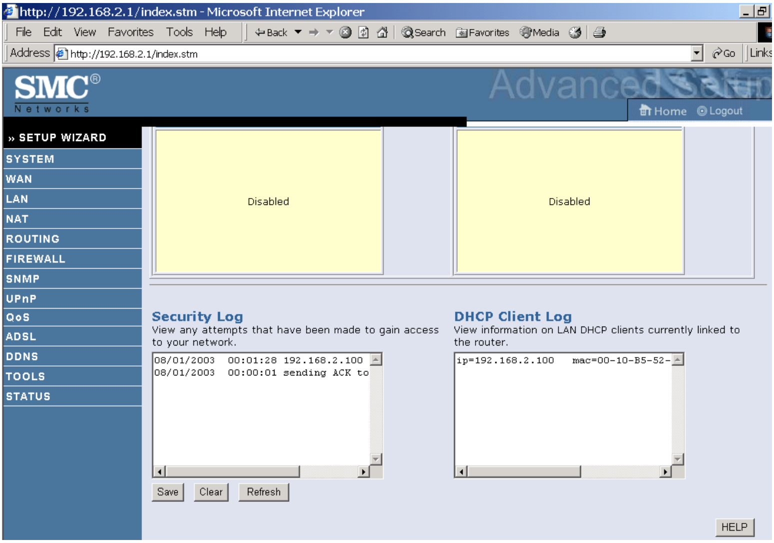
Disabled

VC3

Disabled

VC4

Disabled


http://192.168.2.1/index.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.2.1/index.stm
Go Links
SMC Networks
Advanced Setup
Home Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
NAT
ROUTING
FIREWALL
SNMP
UPnP
QoS
ADSL
DDNS
TOOLS
STATUS

Disabled

Disabled

Security Log

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

```
08/01/2003  00:01:28 192.168.2.100
08/01/2003  00:00:01 sending ACK to
```

Save Clear Refresh

DHCP Client Log

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

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

HELP

The following items are included on the Status screen:

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

Finding the MAC address of a Network Card

WINDOWS NT4/2000/XP

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

The MAC address is listed as the “Physical Address.”

MACINTOSH

Click System Preferences/Network.

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

LINUX

Run the command “/sbin/ifconfig.”

The MAC address is the value after the word “HWaddr.”

Appendix A
Troubleshooting

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

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

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

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

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.

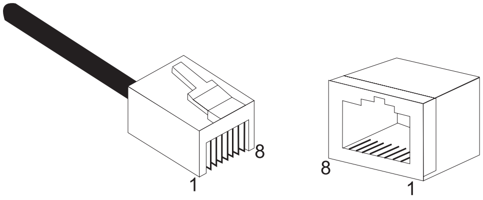


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

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-)

ADSL Cable

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-45 ADSL port on the ADSL Router.

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

Specifications

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

Wiring Conventions

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

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

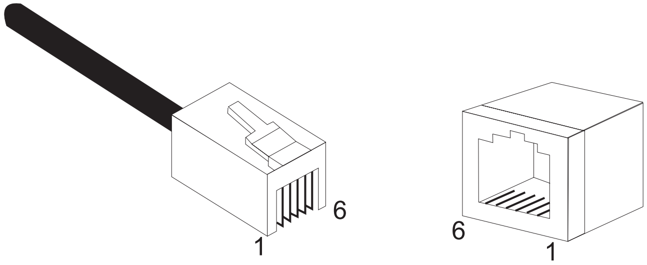
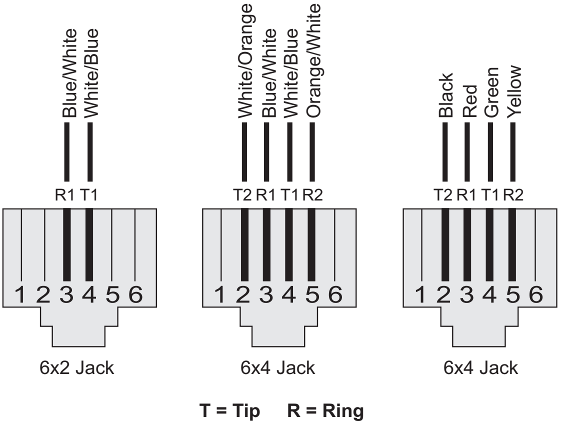


Figure B-2. RJ-11 Connector Pin Numbers



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

Figure B-3. RJ-11 Pinouts

APPENDIX C SPECIFICATIONS

Physical Characteristics

Ports

Four 10/100Mbps RJ-45 ports

One ADSL port (RJ-45 or RJ-11)

ADSL Features

Supports DMT line modulation

Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 &T1.413, Issue 2) and ADSL2 (G.992.3) and ADSl2+ (G.992.5)

Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream

Dying GASP support

ATM Features

RFC1483 Encapsulation (IP, Bridging and encapsulated routing)

PPP over ATM (LLC &VC multiplexing) (RFC2364)

Classical IP (RFC1577)

Traffic shaping (UBR, CBR)

OAM F4/F5 support

PPP over Ethernet Client

Management Features

Firmware upgrade via web based management

web based management (configuration)

Power Indicators

Event and History logging

Network Ping

Traceroute

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

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

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

Humidity
10% to 90% (Non-condensing)

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

Shock: IEC 68-2-29

Drop: IEC 68-2-32

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

Weight: 500 g

Input Power: 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

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

Safety
EN 60950-1

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.

Model Number: SMC7904BRA2/B2 EU

SMC®
Networks
38 Tesla
Irvine, CA 90618
Phone: (943) 679-8000