SMC Networks

USER GUIDE

SMC7908VoWBRA2

Barricade™ VoIP

Wireless 4-port VoIP ADSL2/2+ Modem Router

Wireless 4-port VoIP ADSL2/2+ Modem Router

From SMC's line of award-winning connectivity solutions

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

April 2007
R01 F/W 0.3 (SIP)

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.
20 Mason
Irvine, CA 92618

COMPLIANCES

EC Conformance Declaration

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 300 328

EN 301 489-1

EN 301 489-17

EN 60950-1

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Congratulations on your purchase of the Barricade™ g Voice ADSL Router, 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. The VoIP Router also enables service providers to provide their residential and small office home office (SOHO) customers with high-quality VoIP service using traditional analog telephones and fax machines.

About the Barricade

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

VoIP (Voice over IP)

Using Voice over IP (VoIP), instead of making calls over the regular telephone network, calls are made over computer (IP) networks, either through your Internet Service Provider's connection or through your local network. Calls made to another Internet telephone, anywhere in the world, are generally free, while calls made to a regular telephone are generally much cheaper than traditional long distance calls. The basic steps involved in VoIP include the conversion of an analog voice signal to digital, the

encoding and then compression of the signal into Internet Protocol (IP) packets. The VoIP Router is equipped with a digital signal processor (DSP), which segments the voice signal into frames and stores them in voice packets. These packets are encoded using the industry standard CODECs, G.711, G.723.3 and G.729.

Features and Benefits

- Intergrated ADSL modem for connecting to ADSL line
- Local network connection via four 10/100 Mbps Ethernet ports
- On-board IEEE 802.11b/g wireless access point
- 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:

- **Wireless and Wired LAN**

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

- **Internet Access**

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

- **Shared IP Address**

  The Barricade provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can 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™ g Voice ADSL Router, 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 Voice ADSL Router" on page 4-1.

Package Contents

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

- Barricade Voice ADSL Router (SMC7908VoWBRA2)
- Power adapter
- One CAT-5 Ethernet cable (RJ-45)
- Two Telephone patch cables (RJ-11)
- Documentation CD
- One Warranty Card

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

System Requirements

To install and connect to the Barricade, you must have:

- An ADSL line installed by your ISP.
- An ADSL splitter (at least one).
- A computer with a CD-ROM drive
- Windows 2000 or later, or Mac OS 9.x.
- An up to date web browser: Internet Explorer 6.0 or later, or Mozilla 1.7 /Firefox 1.0 or later.

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 1.2 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 and 54 Mbps over the built-in wireless network adapter.

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

SMC7908VoWBRA2 contains the following ports on the rear panel:

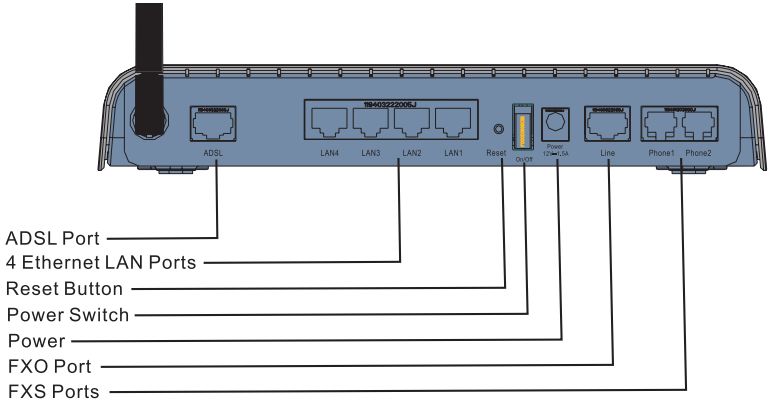


Figure 2-1. SMC7908VoWBRA2 Rear Panel

Item	Description
ADSL Port	Connect your ADSL line to this port.
LAN Ports	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 4-97.
On/Off Switch	Use this switch to turn the Router on and off.
Power Inlet	Connect the included power adapter to this inlet. **Warning**: Using the wrong type of power adapter may damage the Barricade.
Line (FXO)	Connect the telephone line directly to this port.
Phone1 and Phone2 (FXS)	Connect your regular telephone sets to these ports for VoIP connectivity.

LED Indicators

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

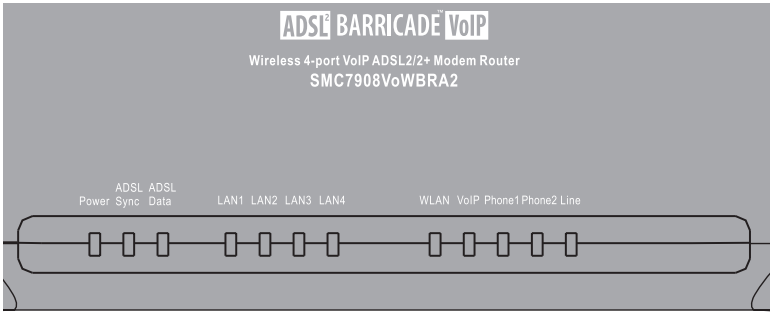


Figure 2-2. SMC7908VoWBRA2 Front Panel

LED	Status	Description
Power	On	The Barricade is receiving power. Normal operation.
	Off	Power off or failure.
ADSL Sync	On	ADSL connection is functioning correctly.
	Flashing	The Barricade is establishing an ADSL link.
	Off	ADSL connection is not established.
ADSL Data	Flashing	Indicates ADSL port is sending or receiving data.
	Off	No data is being transferred.
LAN1-4 (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.
WLAN	Flashing	Indicates WLAN port is sending or receiving data.
	Off	WLAN disabled.

LED	Status	Description
VoIP	On	The VoIP connection is up and connected.
	Off	VoIP connection down.
Phone1/ Phone2 (2 LEDs)	On	The phone is OFF-Hook talking on a call.
	Flashing	Incoming call.
	Off	No call in progress.
Line	On	PSTN call in progress.
	Flashing	Incoming PSTN call.
	Off	No call in progress.

ISP Settings

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

- ISP account user name and password
- VoIP setting details
- 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. It can also be wall-mounted. 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.

Phone/FAX Connection

Connect a standard telephone set or fax machine to the Phone (FXS) port on the rear panel.

Connect the ADSL Line

Connect the supplied ADSL (RJ-11) 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.

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.

Wall-Mount Installation

There are two wall-mount holes at the bottom of the Barricade. Before drilling two holes into the wall, make sure the holes are 175 mm apart.

1. Choose a suitable location for the Barricade.

Note: It should be accessible for installing, cabling and maintaining the device.

2. Measure the distance of the two wall-mount holes.
3. Drill two holes into the wall.
4. Insert a screw into each hole.

Note: Leave 5 mm exposed of the screw head.

5. Attach the Barricade to the wall with two wall-mount slots, and then slide the device down until the screws fit firmly into the slots of the device.

Connection Illustration

The connection diagram shows how to connect the Barricade.For SMC7908VoWBRA2, please refer to the following diagram.

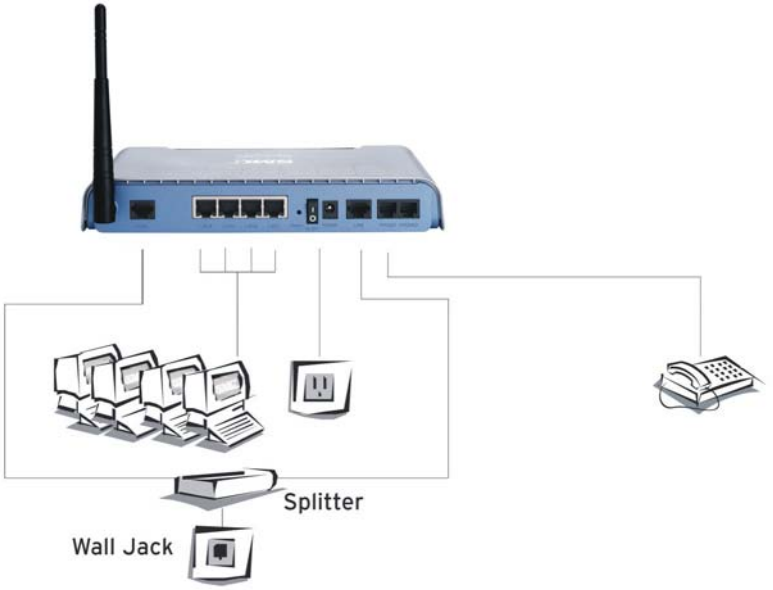


Figure 2-3. SMC7908VoWBRA2 Installation Diagram

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 3-3

"Windows XP" on page 3-6

or

"Configuring Your Macintosh Computer" on page 3-8

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

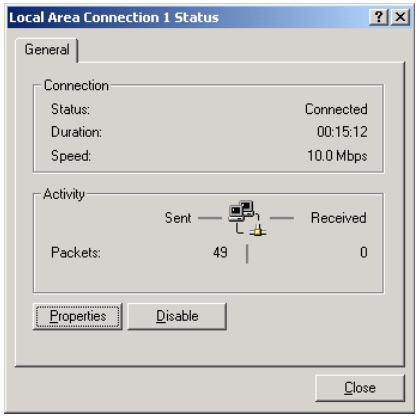
Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the Barricade's web configuration interface in order to make the required changes. (See "Configuring the Voice ADSL Router" on page 4-1 for instruction on configuring the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

Windows 2000

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

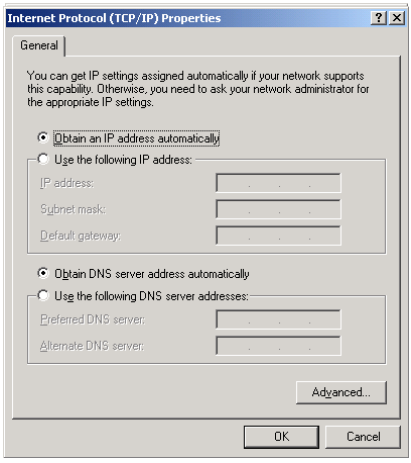
2. Click the icon that corresponds to the connection to your Barricade.

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



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

5. If **Obtain an IP address automatically** and **Obtain DNS server address automatically** are already selected, your computer is already configured for DHCP. If not, select this option.



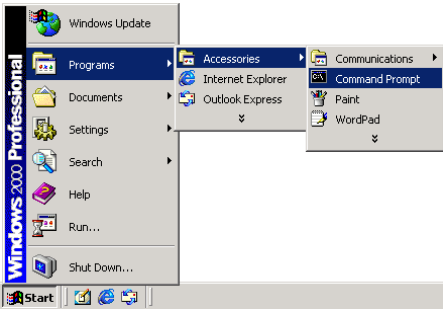
Disable HTTP Proxy

You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. See page 3-6 for details.

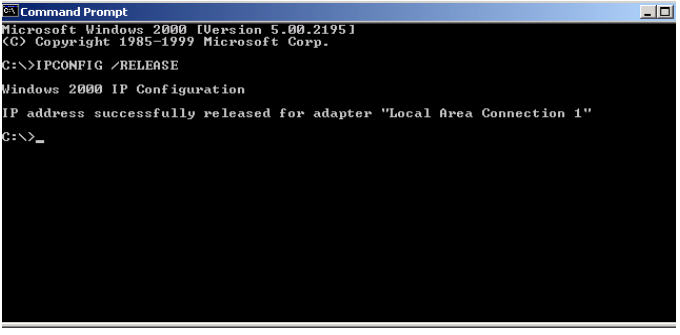
Obtain IP Settings from Your Barricade

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

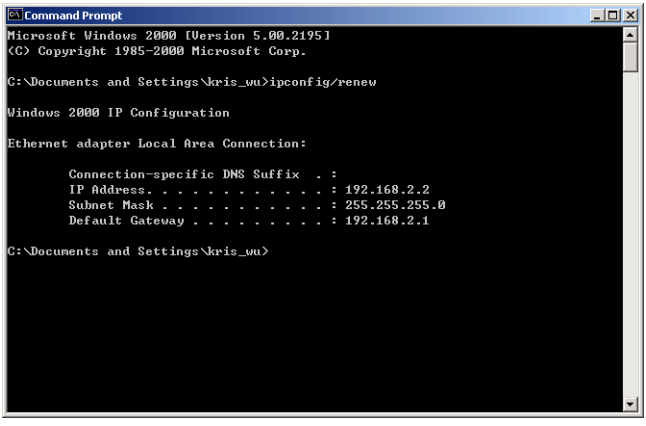
1. On the Windows desktop, click **Start/Programs/Accessories/Command Prompt**.



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



3. Type **ipconfig /renew** and press the **ENTER** key. Verify that your IP address is now **192.168.2.xxx**, your subnet mask is **255.255.255.0** and your default gateway is **192.168.2.1**.
   These values confirm that your Barricade is functioning.



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

Your computer is now configured to connect to the Barricade.

Windows XP

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

Disable HTTP Proxy

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

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

Your computer is now configured to connect to the Barricade.

Configuring Your Macintosh Computer

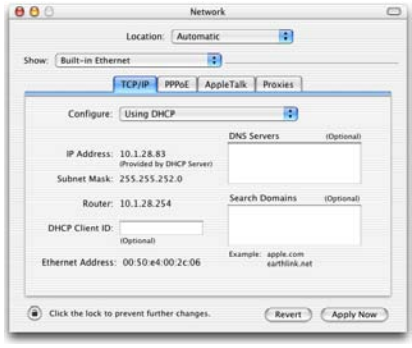
You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

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

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

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



4. Your new settings are shown on the TCP/IP tab. Verify that your IP address is now **192.168.2.xxx**, your subnet mask is **255.255.255.0** and your default gateway is **192.168.2.1**. These values confirm that your Barricade is functioning.

5. Close the **Network** window.

Now your computer is configured to connect to the Barricade.

Disable HTTP Proxy

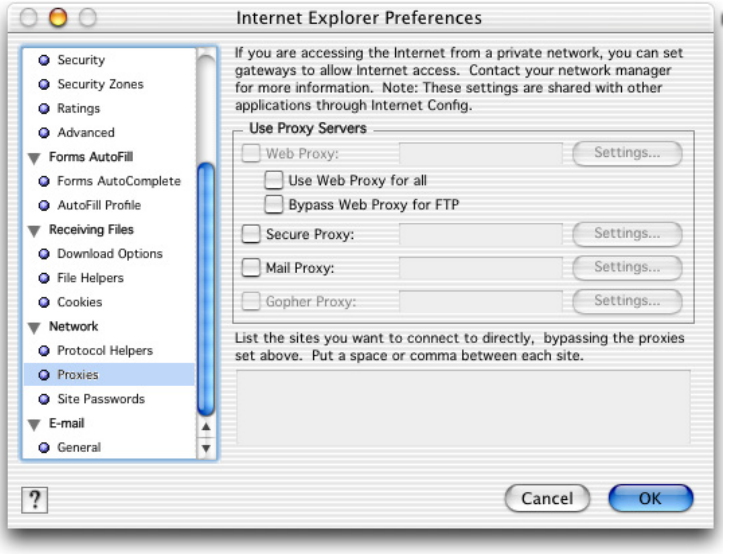
You need to verify that the "HTTP Proxy" feature of your web browser is disabled. This is so that your browser can view the Barricade's HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

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

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

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



CHAPTER 4
CONFIGURING THE VOICE ADSL ROUTER

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**.

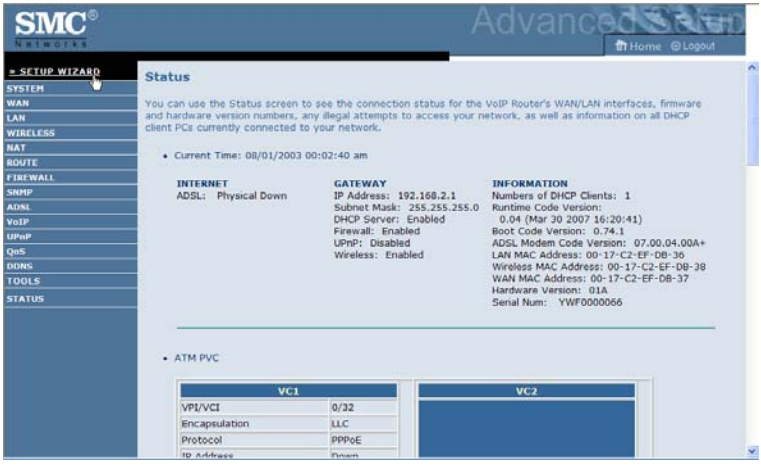
Note: Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

Navigating the Management Interface

The first screen of the web management is Country Selection. You need to select your country before accessing the management interface. Click **OK** to confirm your selection.

Click **Apply** to continue.

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



Setup Wizard: Use the Setup Wizard if you want to quickly set up the Barricade. Go to "SETUP WIZARD" on page 4-4.

Advanced Setup: Advanced Setup supports more advanced functions like VoIP, Firewall, IP and MAC address filtering, virtual server setup, virtual DMZ host, as well as other functions. Go to "Advanced Setup" on page 4-17.

Making Configuration Changes

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

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

SETUP WIZARD

Channel and SSID

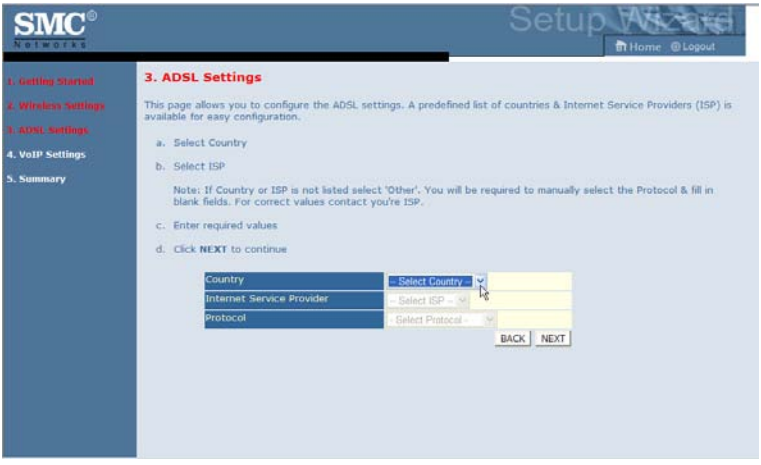
Click on **SETUP WIZARD** and **NEXT**, then you will see the Channel and SSID screen.

Parameter	Description
SSID	Service Set ID. The SSID must be the same on the Barricade and all of its wireless clients.
SSID Broadcast	Enable or disable the broadcasting of the SSID. Disabling SSID broadcast will provide increased security by hiding the SSID of your wireless network.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. SMC recommend using "Mixed (11b+11g)" to provide compatibility with both 11b and 11g wireless clients.
Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients. The Barricade will automatically assign itself a radio channel, or you may select one manually.

Click **NEXT** to continue.

ADSL 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.



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 4-10 in the manual.

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

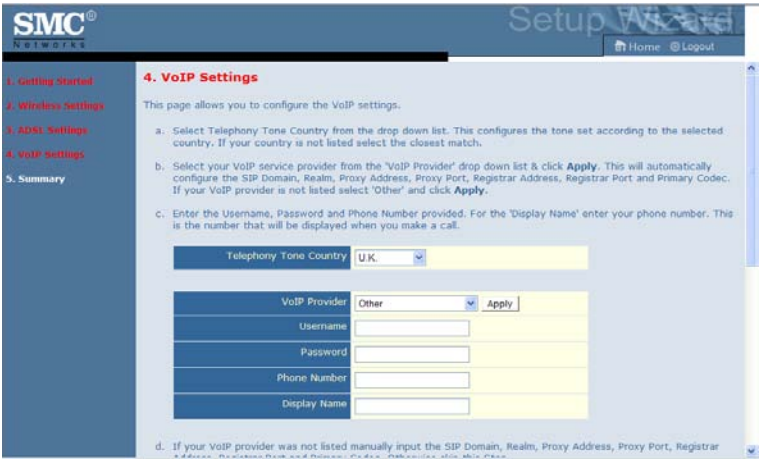
If your ISP uses Protocol RFC1483 Routed you will need to enter the IP address, Subnet Mask, Default Gateway and DNS Server address supplied by your ISP.

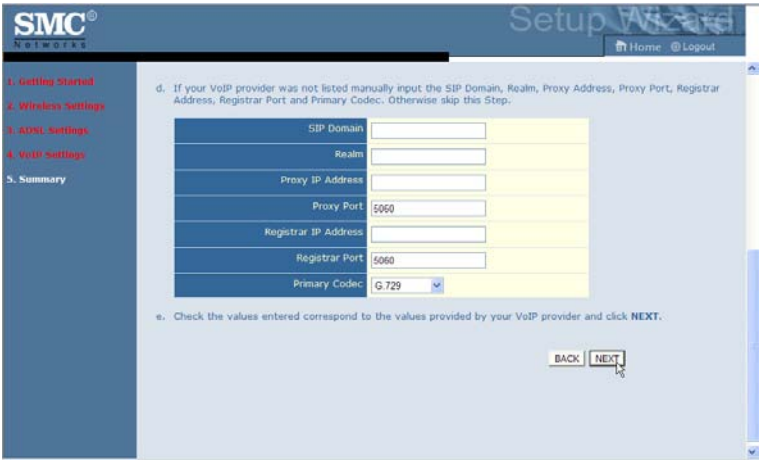
Note: If your ISP has not provided you with a DNS address and the protocol is PPPoA, PPPoE or 1483 Bridging, you can leave this field blank. The Barricade will then automatically obtain the DNS address.

Click **NEXT** to continue.

VoIP Setting

Configure your VoIP account settings on this screen.



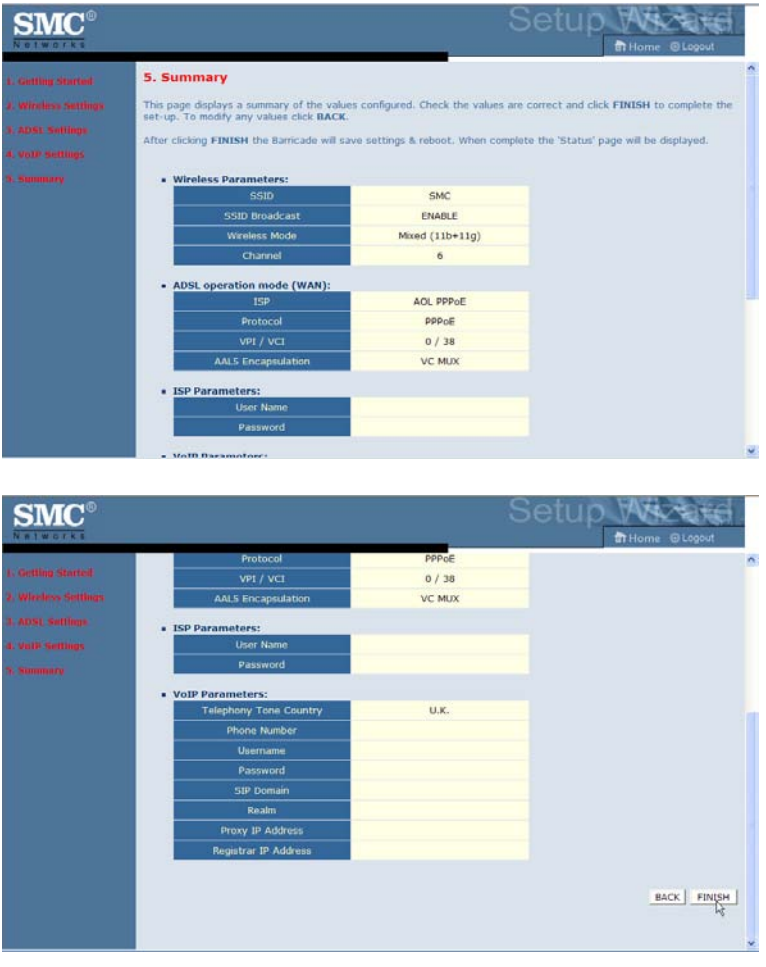


Parameter	Description
Telephony Tone Country	Select your Country. This will automatically configure the Barricade with the correct telephony tone set for the selected country.
VoIP Provider	Select your VoIP provider form the VoIP Provider drop-down menu. This automatically configures the SIP Domain, Realm, Proxy Address, Proxy Port, Registrar Address and Registrar Port settings. If your VoIP provider is not listed select Other.
Username	Input the VoIP provider assigned user name.
Password	Input the Password.
Phone Number	Input the VoIP phone number.
Display Name	This is the number that will be displayed when you make a call. To hide your phone number, enter "Anonymous".
SIP Domain	Enter the SIP domain provided by your VoIP provider.
Realm	Enter the Realm provided by your VoIP provider.
Proxy IP Address	Enter the IP address/domain name of the SIP Proxy Server.
Proxy Port	Enter the port number for connecting to the SIP Proxy Server.
Registrar IP Address	Enter the IP address/domain name of the Registrar Server.
Registrar Port	Enter the port number for connecting to the Registrar Server.
Primary Codec	Specify which audio coding process you would like to use.

Click **NEXT** to continue.

Confirm

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



Parameter	Description
Wireless Parameters	
SSID	The SSID must be the same on the Barricade and all of its wireless clients.
SSID Broadcast	The status of enabling or disabling the broadcasting of the SSID.
Wireless Mode	This device supports both 11g and 11b wireless networks.
Channel	This channel must be the same on the Barricade and all of its wireless clients.
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.
ISP Parameters	
Username	The ISP assigned user name.
Password	The password (hidden).
VoIP Parameters	
Telephony Tone Country	The selected country of your telephony tone set.
Phone Number	The VoIP phone number.
Username	The VoIP provider assigned user name.
Password	The assigned user name.
SIP Domain	The SIP domain provided by your VoIP provider.
Realm	The Realm provided by your VoIP provider
Proxy IP Address	The IP address/domain name of the SIP Proxy Server.
Registrar IP Address	The IP address/domain name of the Registrar Server

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

Your Barricade is now set up. Go to "Troubleshooting" if you cannot make a connection to the Internet.

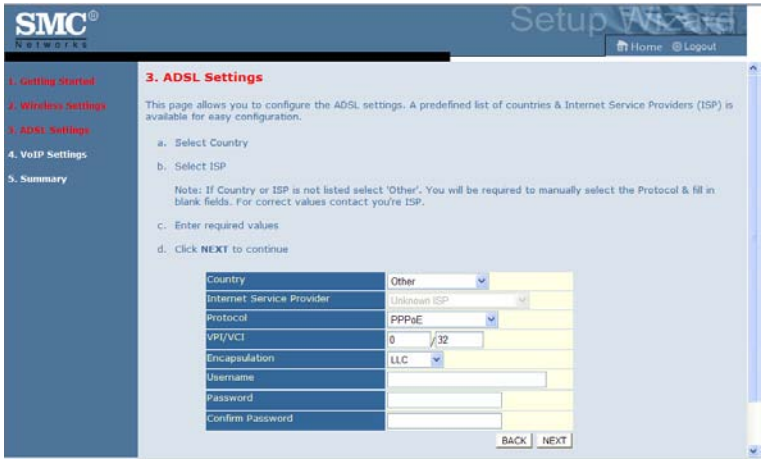
Parameter Setting - Country or ISP Not Listed

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

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

After selecting **Other** you will be required to select the **Protocol** that your ISP uses from the drop-down list.

PPPoE



Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down 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 4-8 in the manual for details about the settings.

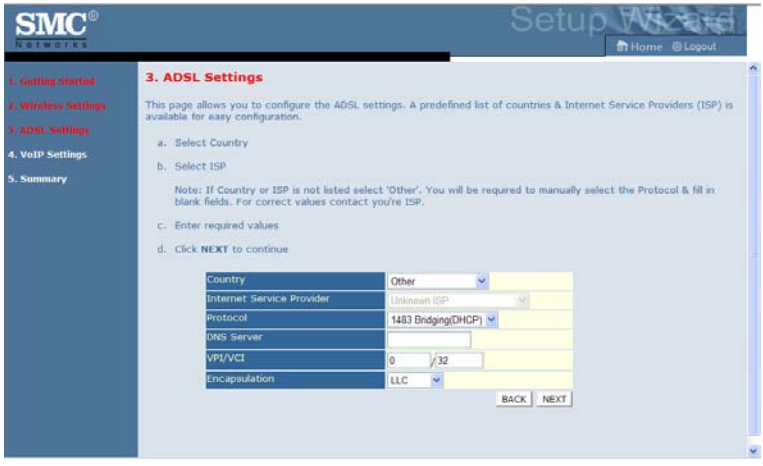
PPPoA

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

Click **NEXT** to continue to the "Confirm" settings page.

Go to "Confirm" on page 4-8 in the manual for details about the settings.

1483 Bridging (DHCP)



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

Click **NEXT** to continue to the "Confirm" settings page.

Go to "Confirm" on page 4-8 in the manual for details about the setting.

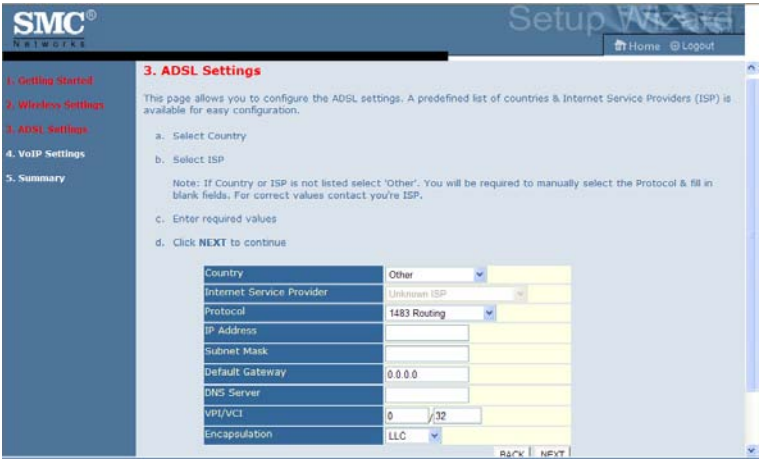
1483 Bridging (Static)

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

Click **NEXT** to continue to the "Confirm" settings page.

Go to "Confirm" on page 4-8 in the manual for details about the settings.

1483 Routing



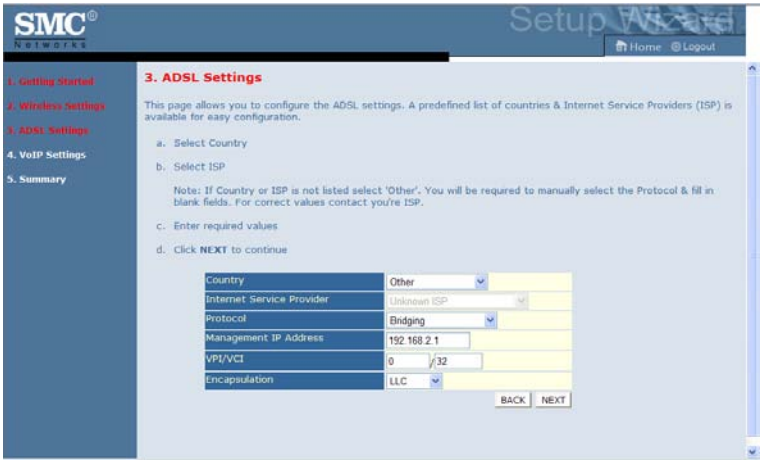
Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
DNS Server	Enter the DNS Server IP address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier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

Click **NEXT** to continue to the "Confirm" settings page.

Go to "Confirm" on page 4-8 in the manual for details about the settings.

Bridging

Enter the Bridging settings provided by your ISP.



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 list.

Click **NEXT** to continue to the "Confirm" settings page.

Go to "Confirm" on page 4-8 in the manual for details about the settings.

Advanced Setup

The left-hand side displays the main menu and the right-hand side shows descriptive information. The advanced management interface contains 16 main menu items as described in the following table.

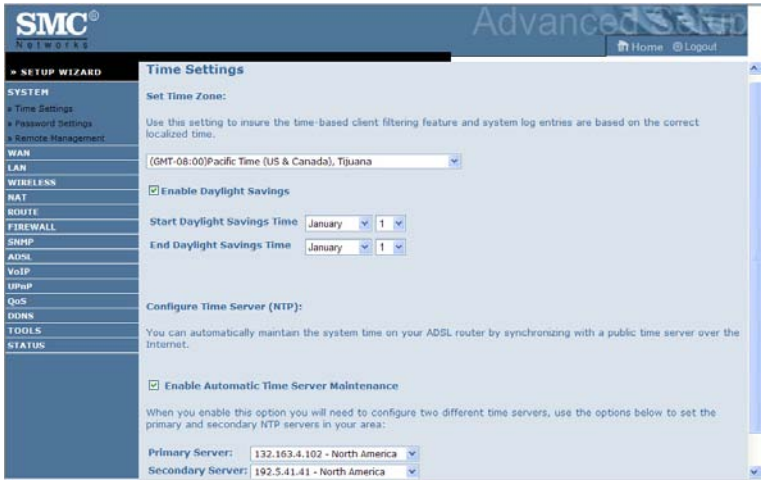
Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade remotely.
WAN	Configures the Internet connection settings.
LAN	Sets the TCP/IP configuration for the Barricade LAN interface and DHCP clients.
Wireless	Configures the radio frequency, SSID, and security for wireless communications.
NAT	Configures Address Mapping, virtual server and special applications.
Route	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.
ADSL	Sets the ADSL operation type and shows the ADSL status.
VoIP	Configures VoIP settings for the VoIP function, and view VoIP Status and Call logs.
UPnP	Enable/disable the Universal Plug and Play function.
QoS	Allows you to optimize voice quality by prioritizing voice over data traffic.
DDNS	Configures Dynamic DNS function.

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

SYSTEM

Time Settings

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



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

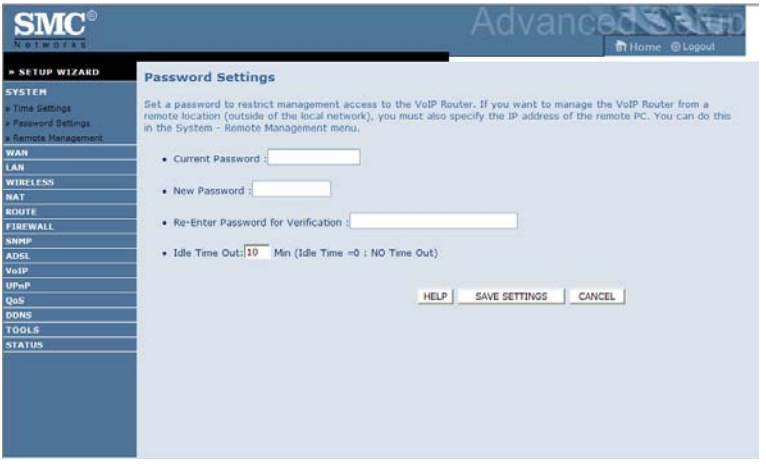
If daylight savings is used in your area, check the box to enable the function, and select the start/end dates.

If you want to automatically synchronize the 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 **Save Settings**.

Password Settings

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



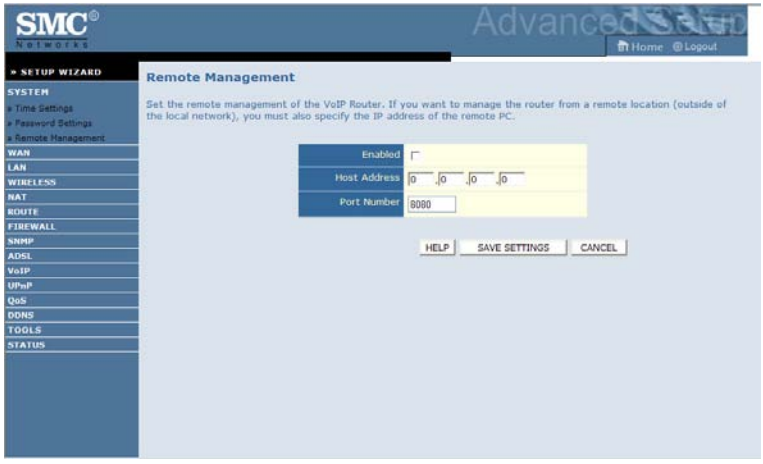
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

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

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

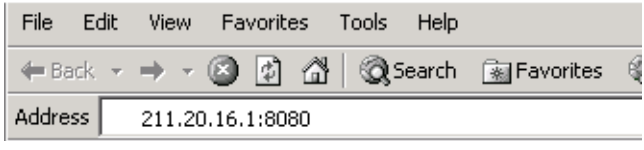
Remote Management

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



Note: If you 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.



WAN

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

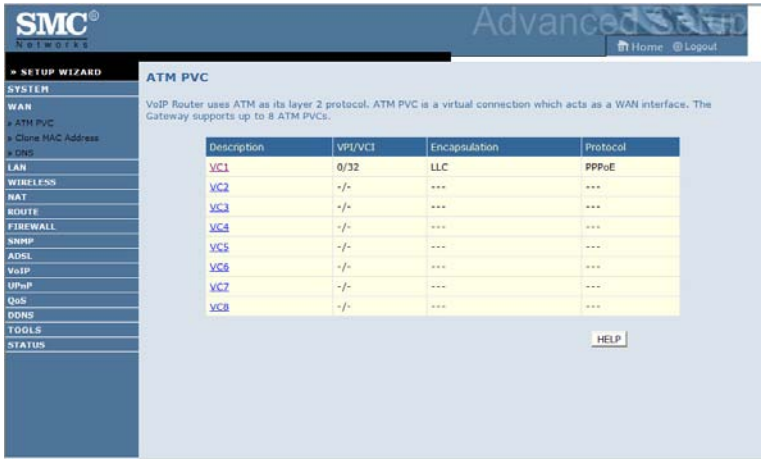
The Barricade supports the following modes:

- 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.

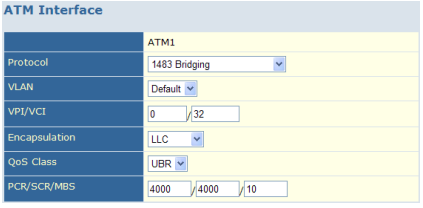


Parameter	Description
VC1 to VC8	Click on the desired VC to configure the connection parameters.
VPI/VCI	Displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) configured for the corresponding VC.
Encapsulation	Displays the Encapsulation configured for the corresponding VC. Encapsulation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

ATM Interface

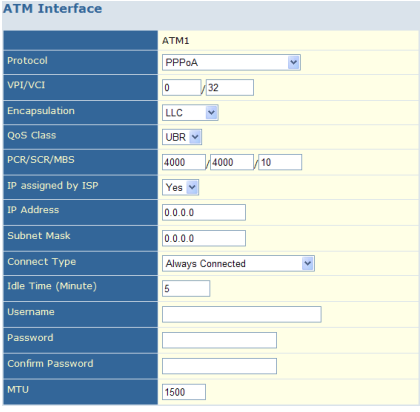
1483 Bridging

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



Parameter	Description
VPI/VCI	Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. When data needs to be transmitted, it is immediately inserted into the cell flows.
Encapsulation	Select the packet encapsulation type. Packet encapsulation specifies how to handle multiple protocols at the ATM transport layer. • VC-MUX: Point-to-Point Protocol over ATM VirtualCircuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead. • LLC: Point-to-Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit (using slightly more overhead).
QoS Class	ATM QoS classes including CBR, UBR and VBR
PCR/SCR/MBS	QoS Parameters - PCR (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) are configurable.

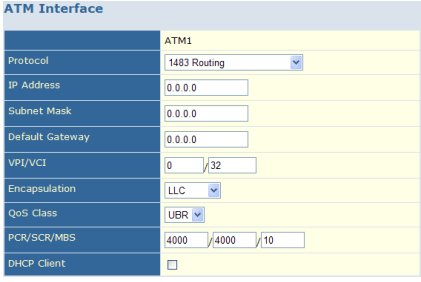
PPPoA



Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down list.
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.
Subnet Mask	Enter the subnet mask provided by your ISP.
Connect Type	Sets connection mode to always connected, automatic or manual connection.
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated.
Username	Enter user name.
Password	Enter password.

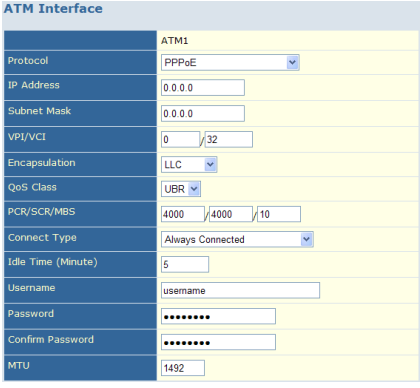
Parameter	Description
Confirm Password	Confirm password
MTU	Leave the Maximum Transmission Unit (MTU) at the default value (1500) unless you have a particular reason to change it.

1483 Routing



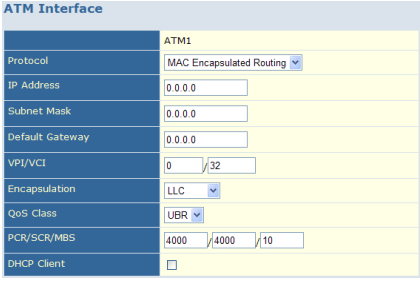
Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask address provided by your ISP.
Default Gateway	Enter the gateway address provided by your ISP.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by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

PPPoE



Parameter	Description
IP Address	Enter the IP address provided by your ISP.
Subnet Mask	Enter the subnet mask 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.
Connect Type	Sets connection mode to always connected, automatic or manual connection.
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated.
Username	Enter user name.
Password	Enter password.
Confirm Password	Confirm password
MTU	Leave the Maximum Transmission Unit (MTU) at the default value (1500) unless you have a particular reason to change it.

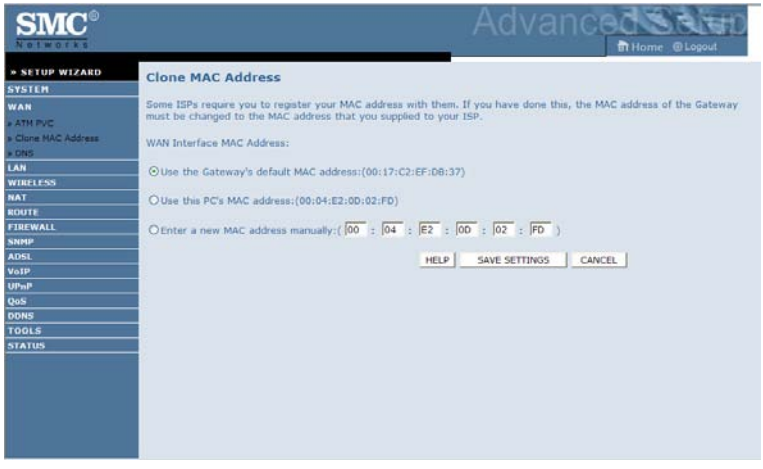
MAC Encapsulated Routing



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

Clone MAC Address

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

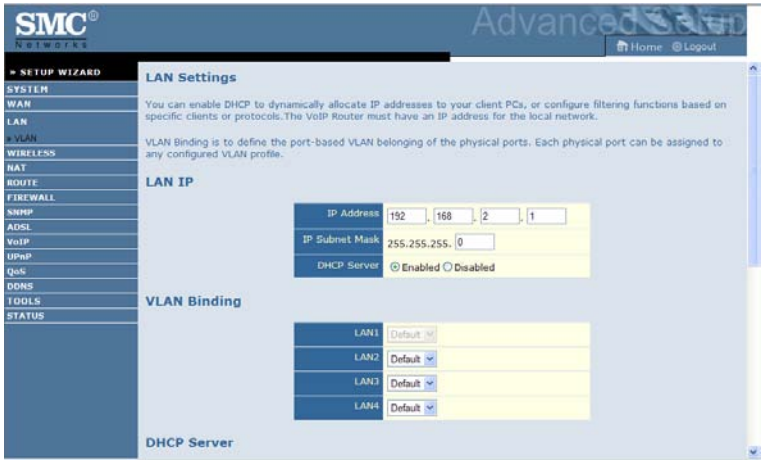


DNS

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

LAN

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



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.
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.

Parameter	Description
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.

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

VLAN Profile

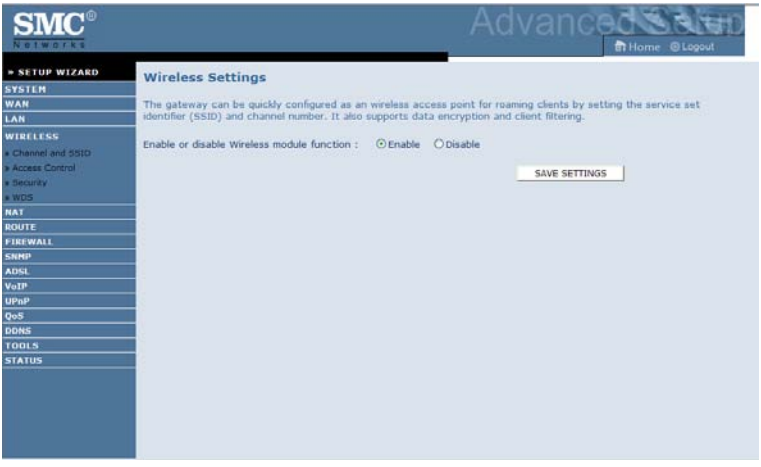
Configure the VLAN settings in this screen.

- 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: Enabling it will turn on the feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers.
- IGMP Querier: Enabling this function will send out periodic IGMP queries.

WIRELESS

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

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



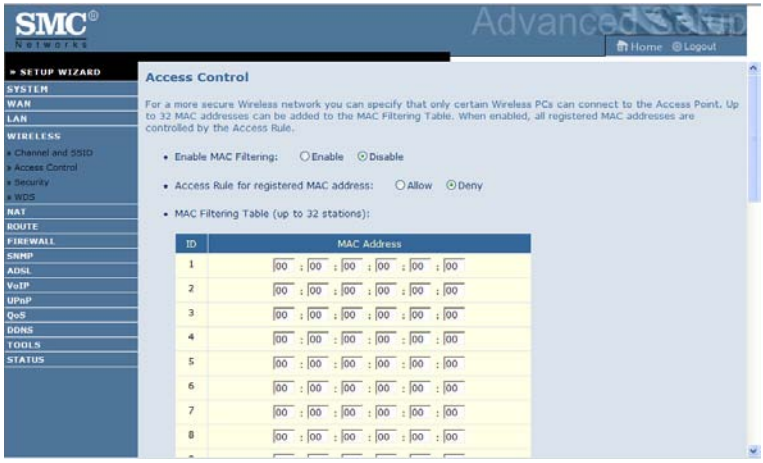
Channel and SSID

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

Parameter	Description
SSID	Service Set ID. The SSID must be the same on the Barricade and all of its wireless clients.
SSID Broadcast	Enable or disable the broadcasting of the SSID. Disabling SSID broadcast will provide increased security by hiding the SSID of your wireless network.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. SMC recommend using "Mixed (11b+11g)" to provide compatibility with both 11b and 11g wireless clients.
Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the Barricade and all of its wireless clients. The Barricade will automatically assign itself a radio channel, or you may select one manually.

Access Control

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



Security

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

- WPA/WPA2
- WPA2 Only
- WPA Only
- WEP

WPA/WPA2

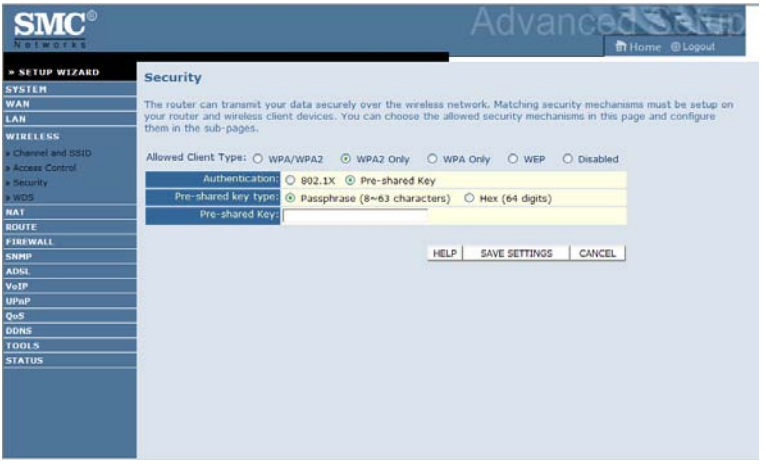
Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.

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

Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. •802.1X: for the enterprise network with a RADIUS server. •Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.

WPA2 Only

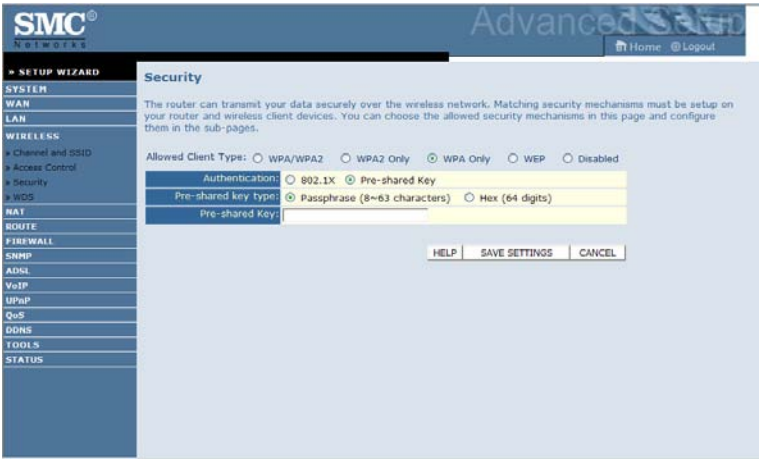
WPA2 is a product certification that is available through the Wi-Fi Alliance. WPA2 certifies that wireless equipment is compatible with the IEEE 802.11i standard. The WPA2 product certification formally replaces Wired Equivalent Privacy (WEP) and the other security features of the original IEEE 802.11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



Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. • Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.

WPA Only

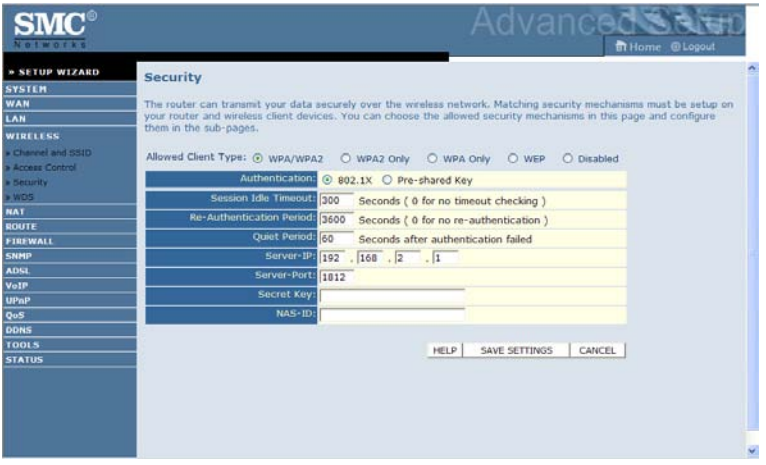
Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service.



Parameter	Description
Authentication	Choose 802.1X or Pre-shared Key to use as the authentication method. • 802.1X: for the enterprise network with a RADIUS server. • Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.

802.1X

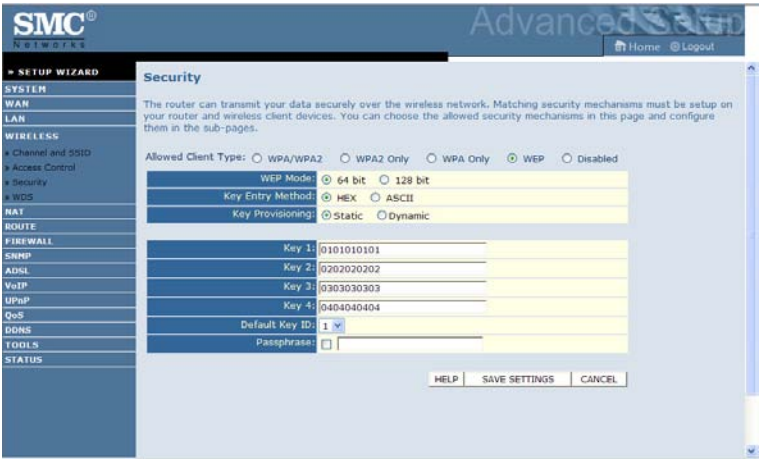
If 802.1x is used in your network, then you should enable this function for the Barricade.



Parameter	Description
Authentication	Choose 802.1X authentication option.
Session Idle timeout	Defines a maximum period of time for which the connection is maintained during inactivity.
Re-Authentication Period	Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client.
Quiet Period	Defines a maximum period of time for which the Barricade will wait between failed authentications.
Server IP	The IP address of your authentication server.
Server Port	The port used for the authentication service.
Secret Key	The secret key shared between the authentication server and its clients.
NAS-ID	Defines the request identifier of the Network Access Server.

WEP

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



Parameter	Description
WEP Mode	Select 64 bit or 128 bit key to use for encryption.
Key Entry Method	Select Hex or ASCII to use for encryption key.
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1X function first.

You may automatically generate encryption keys or manually enter the keys.

To generate the key automatically with passphrase, check the Passphrase box, enter a string of characters. Select the default key from the drop-down menu. Click **SAVE SETTINGS**.

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

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

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

WDS

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

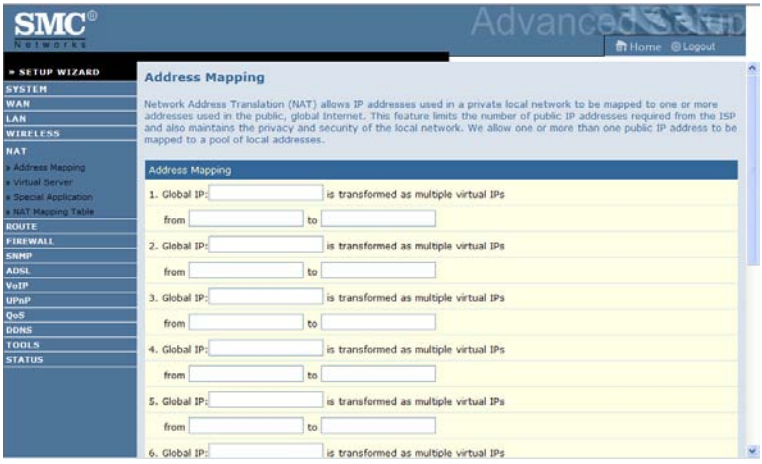
- Enable or disable WDS features: if you want to use the WDS function, select **enable**.
- AP MAC Address Table (up to 4 APs): choose up to 4 stations.

NAT

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

Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP into the "from" field.



Virtual Server

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

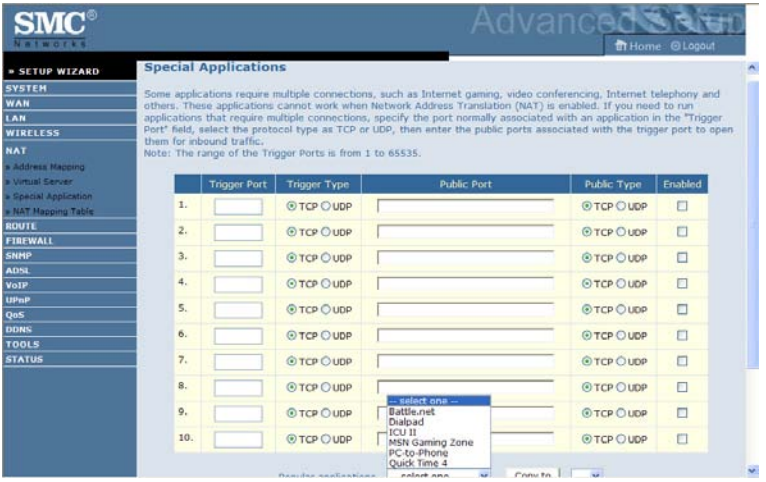
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they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

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

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

Special Application

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



NAT Mapping Table

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

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

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

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

ROUTE

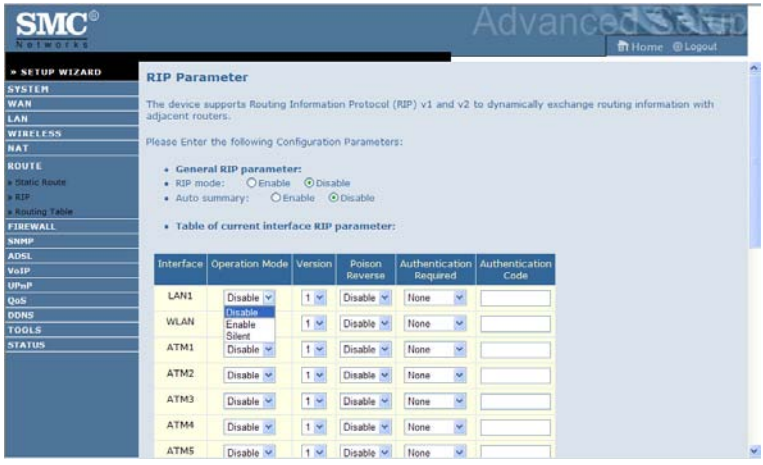
These screens define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

Static Route

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

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

RIP



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

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

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

Routing Table

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

FIREWALL

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

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

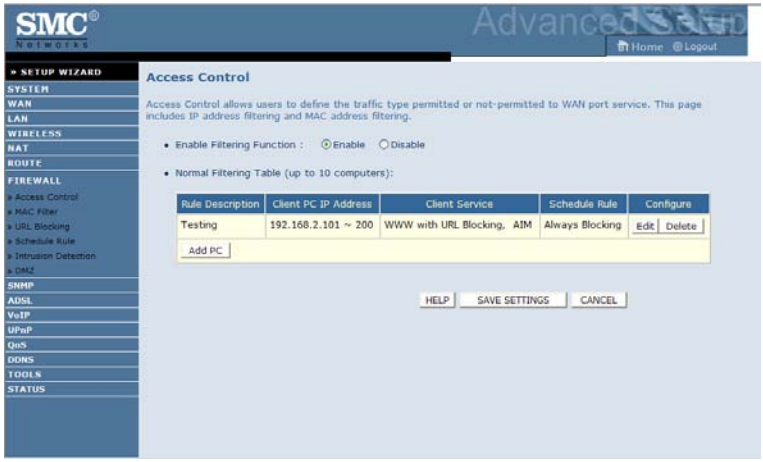
The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.
(For details see page 4-61.)

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.

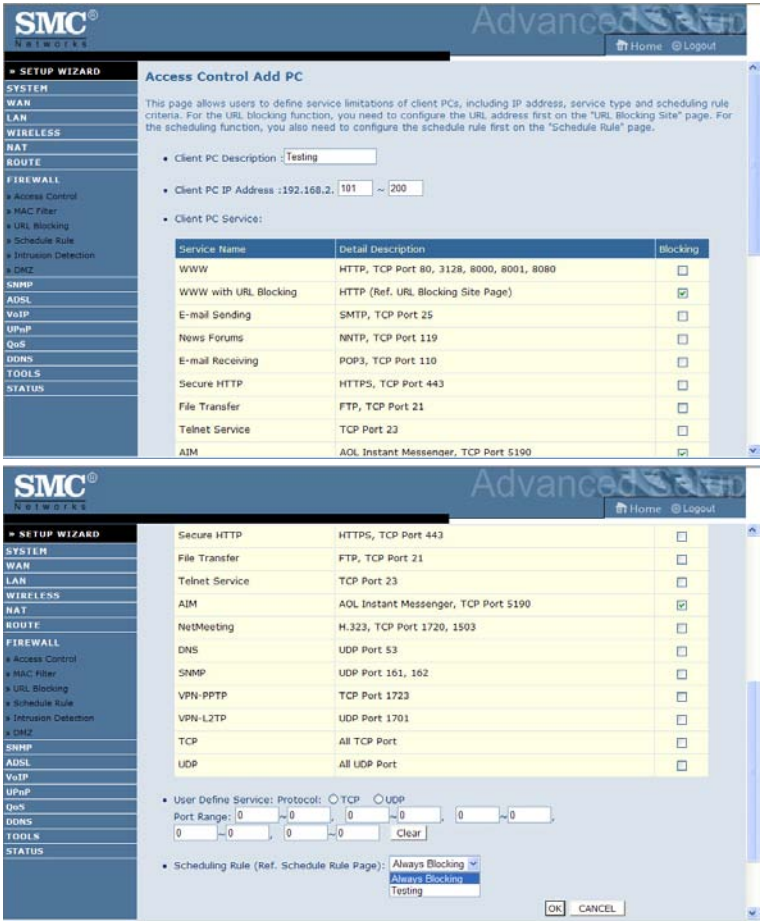


The following items are on the Access Control screen:

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.



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.

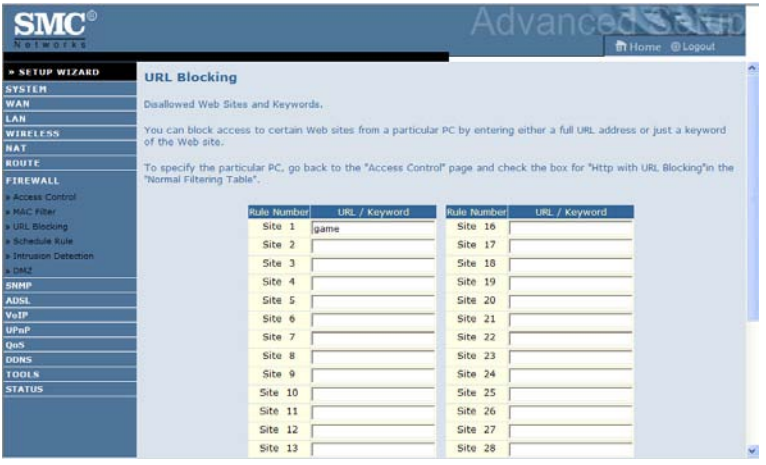
You can enter up to 32 MAC addresses in this table.

1. MAC Address Control: select enable or disable.

2. MAC Filtering Table: enter the MAC address in the space provided.

URL Blocking

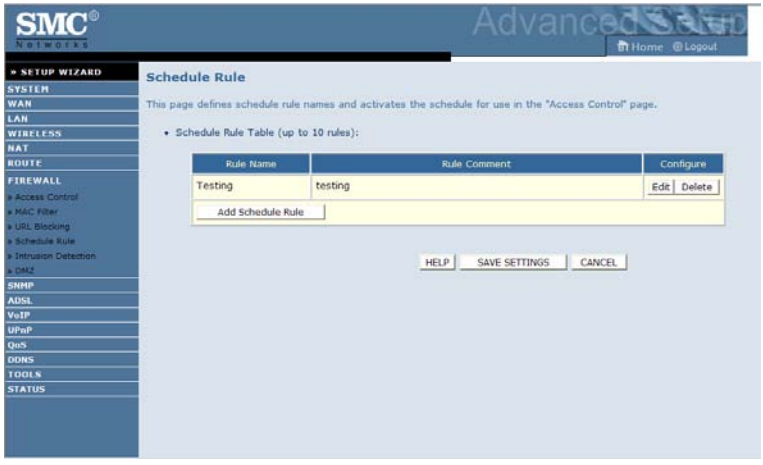
The Barricade allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.



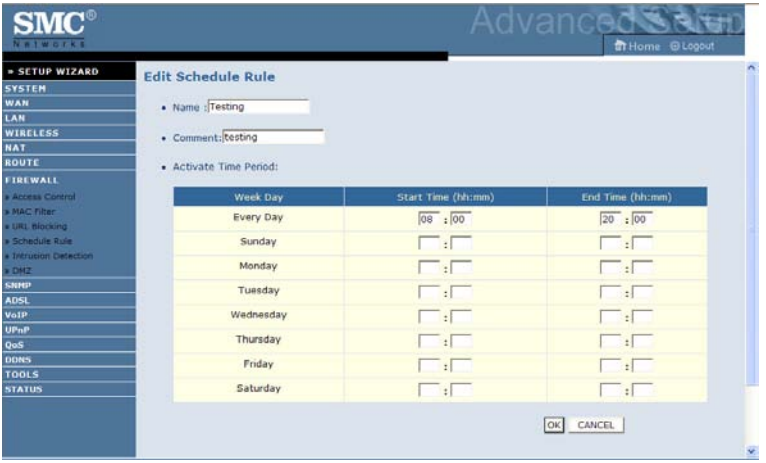
You can define up to 30 sites here.

Schedule Rule

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



Follow these steps to add a schedule rule:



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

2. Define the appropriate settings for a schedule rule.

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

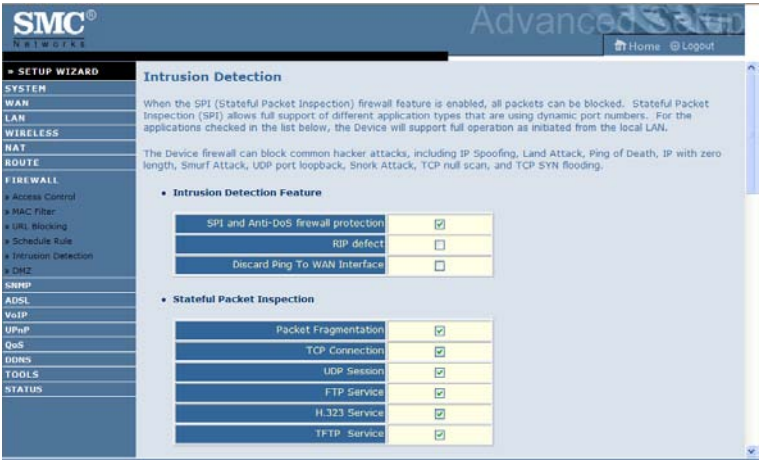
Intrusion Detection

- **Intrusion Detection Feature**

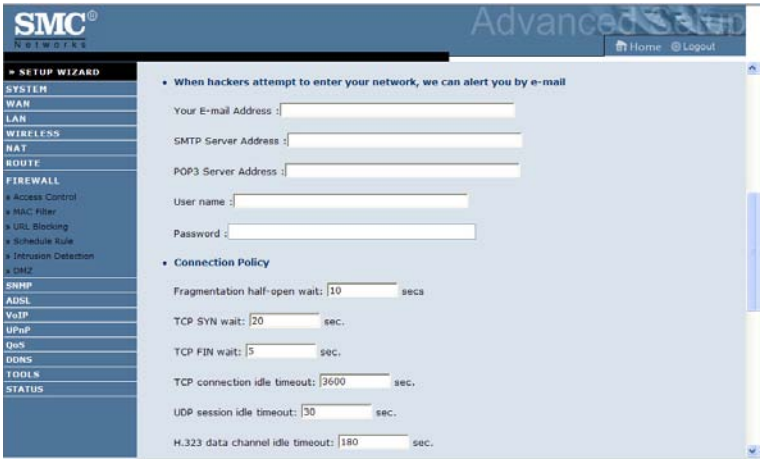
Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) — The Intrusion Detection Feature of the Barricade Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the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

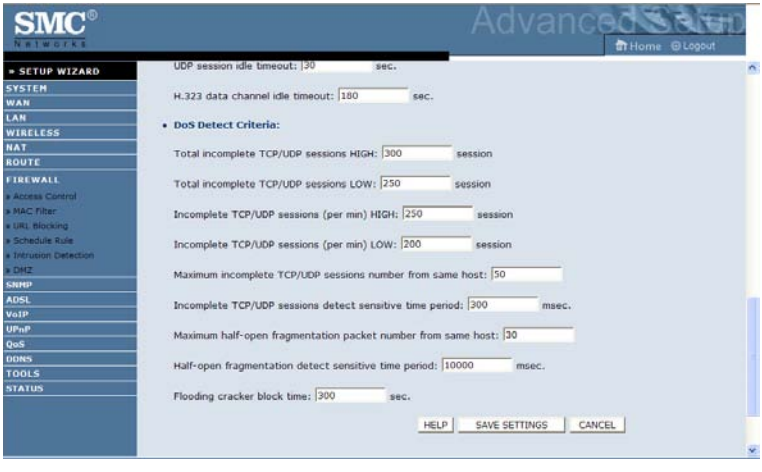
RIP Defect (Default: Enabled) — If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

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



Scroll down to view more information.


SMC
Networks
Advanced Setup
Home
Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
ADSL
VoIP
UPnP
QoS
DDNS
TOOLS
STATUS
When hackers attempt to enter your network, we can alert you by e-mail
Your E-mail Address :
SMTP Server Address :
POP3 Server Address :
User name :
Password :
Connection Policy
Fragmentation half-open wait: 10 secs
TCP SYN wait: 20 sec.
TCP FIN wait: 5 sec.
TCP connection idle timeout: 3600 sec.
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.


SMC
Networks
Advanced Setup
Home
Logout
» SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
» Access Control
» MAC Filter
» URL Blocking
» Schedule Rule
» Intrusion Detection
» DMZ
SNMP
ADSL
VoIP
UPnP
QoS
DDNS
TOOLS
STATUS
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.
DoS Detect Criteria:
Total incomplete TCP/UDP sessions HIGH: 300 session
Total incomplete TCP/UDP sessions LOW: 250 session
Incomplete TCP/UDP sessions (per min) HIGH: 250 session
Incomplete TCP/UDP sessions (per min) LOW: 200 session
Maximum incomplete TCP/UDP sessions number from same host: 50
Incomplete TCP/UDP sessions detect sensitive time period: 300 msec.
Maximum half-open fragmentation packet number from same host: 30
Half-open fragmentation detect sensitive time period: 10000 msec.
Flooding cracker block time: 300 sec.
HELP
SAVE SETTINGS
CANCEL

- **Stateful Packet Inspection**

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

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

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

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

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

- **Connection Policy**

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

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

- **DoS Criteria and Port Scan Criteria**

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

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

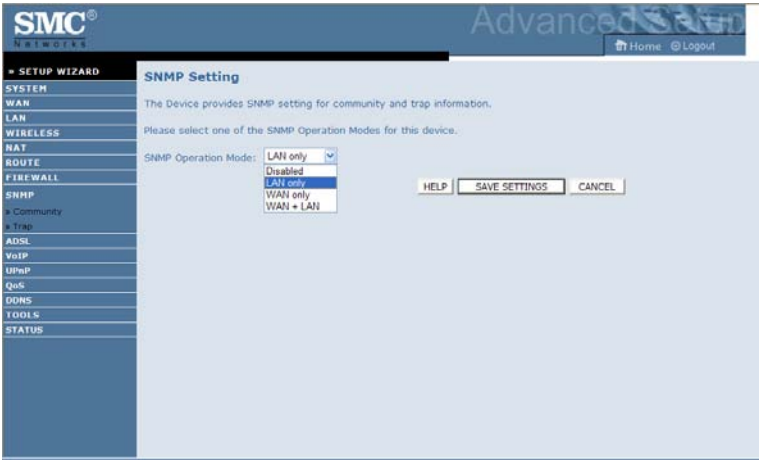
Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

DMZ

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

SNMP

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



Community

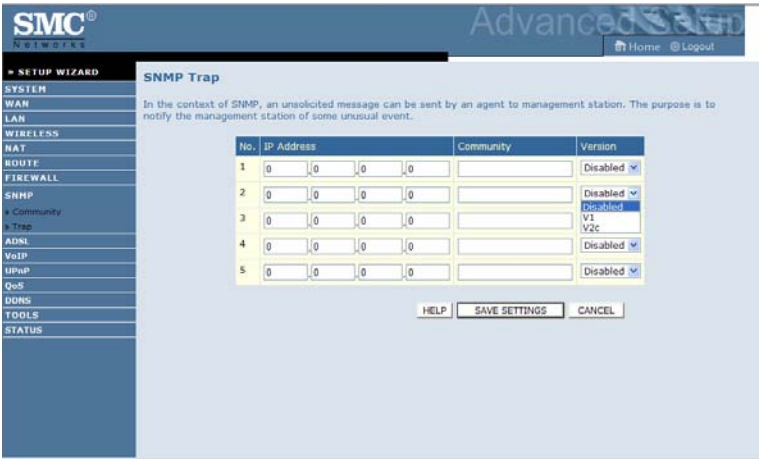
A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication.

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

Note: Up to five community names may be entered.

Trap

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



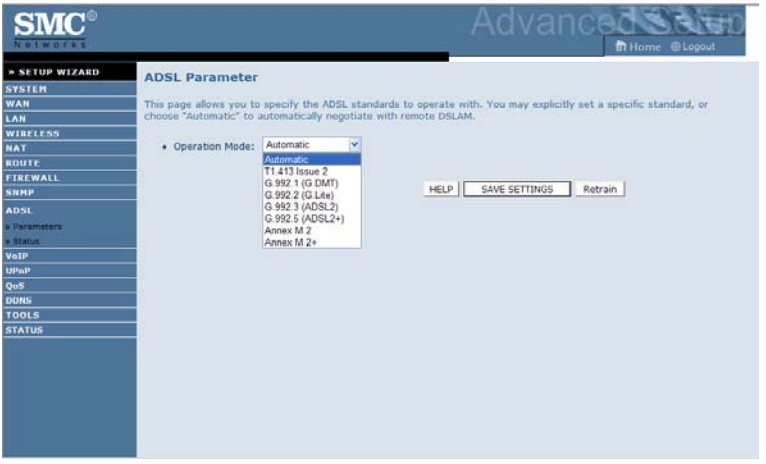
Parameter	Description
IP Address	Traps are sent to this address when errors or specific events occur on the network.
Community	A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information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

ADSL

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

ADSL Parameters

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



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

ADSL Status

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

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.
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.

VoIP

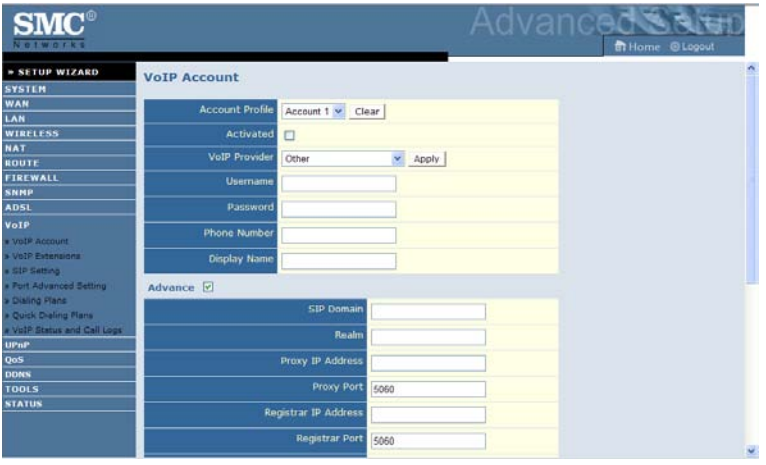
Voice over Internet Protocol (VoIP) is the routing of voice conversations over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of traditional dedicated, circuit-switched voice transmission lines.

VoIP Account

Configure your VoIP account settings on this screen. Before you begin you will need to obtain the following settings from your service provider:

- Username
- Password
- Phone Number
- SIP Domain
- Realm
- SIP Proxy Server address and port
- SIP Registrar Server address and port
- Prefer Codec

If you are missing any settings contact your VoIP service provider.



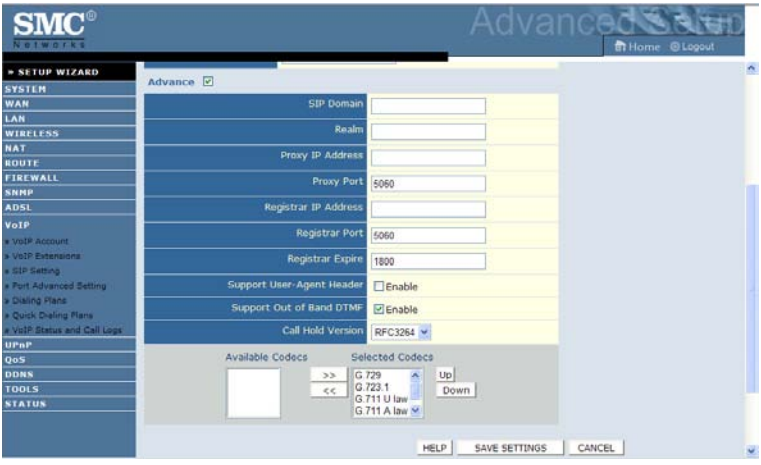
- Select the account form the **Account Profile** drop-down menu. To set-up a second VoIP account, select **Account 2**. Up to 4 accounts can be configured.

- Check the **Activated** check box to enable the account. If the box is unchecked the account is disabled.

- Select your VoIP provider form the **VoIP Provider** drop-down menu. This automatically configures the **SIP Domain**, **Realm**, **Proxy Address**, **Proxy Port**, **Registrar Address** and **Registrar Port** settings. If your VoIP provider is not listed select **Other**.

- Input the **Username**, **Password** and **Phone Number**. For the **Display Name** input your phone number. This is the number that will be displayed when you make a call. To hide your phone number, enter "Anonymous".

- If the **Advance** check box is not already selected, check this box to display advanced configuration options.



- Input the **SIP Domain**, **Realm**, **Proxy Address**, **Proxy Port**, **Registrar Address** and **Registrar Port**. If your VoIP provider was listed and selected, these settings should already be configured.

- Use the **Up** and **Down** buttons to change Codec priority. The preferred Codec goes at the top. Use the left and right arrow buttons to remove or add Codec's from the list of selected Codec's.

Parameter	Description
SIP Domain	Enter the SIP domain provided by your VoIP provider.
Realm	Enter the Realm provided by your VoIP provider.
Proxy IP Address	Enter the IP address/domain name of the SIP Proxy Server.
Proxy Port	Enter the port number for connecting to the SIP Proxy Server.
Registrar IP Address	Enter the IP address/domain name of the Registrar Server.
Registrar Port	Enter the port number for connecting to the Registrar Server.
Registrar Expire	The time to re-register with the registrar server.

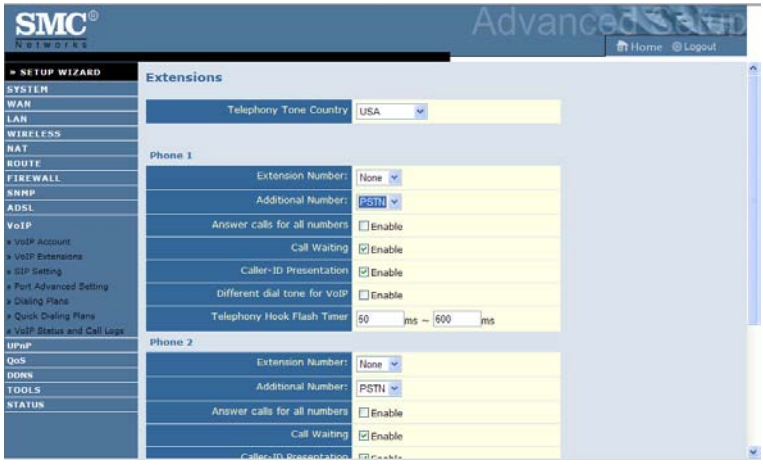
Parameter	Description
Support User-Agent Header	Enable or disables user-agent header support. Enabling this feature includes user agent information in the packet, e.g., the caller's ID may be displayed.
Support Out of Band DTMF	Check this box to enable support for Out of Band Dual Tone Multi-Frequency (DTMF). DTMF assigns a specific frequency (consisting of two separate tones) to each key so that it can be easily identified by a microprocessor.
Call Hold Version	Select the Call Hold version supported by your VoIP provider. Contact your provider to check if Call Hold is supported and what version to use.

Codec's are used to convert an analogue voice signal to digitally encoded version. Codec's vary in the sound quality, the bandwidth required, the computational requirements, etc. You can specify which audio coding process you would like to use. This Barricade supports the following codec's:

- G.729
- G.723.1
- G.711 U law
- G.711 A law

VoIP Extensions

You can configure the Line and Phone port settings on this screen.

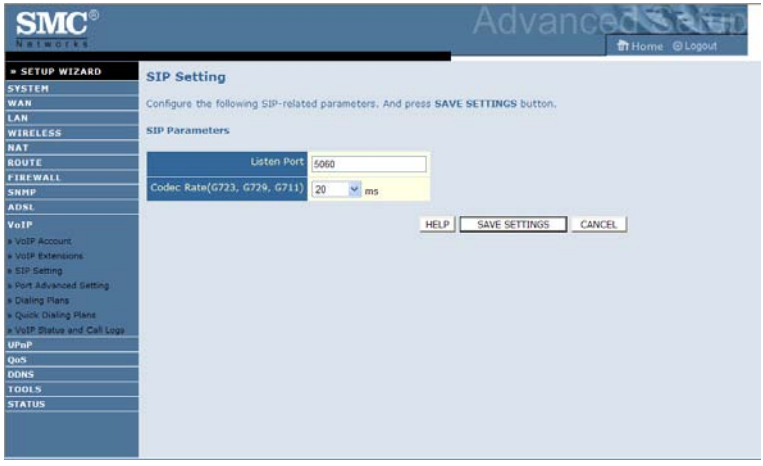


Parameter	Description
Telephony Tone Country Setting	Configures telephony tone set for the selected country.
Extension Number	Select Extension Number to assign to the phone. This should be your VoIP phone number. The extension number selected will be the default number used for making outgoing calls. You will also be able to receive phone calls for this number.
Additional Number:	Select an additional number to assign to the phone. This could be your PSTN number (Select PSTN) or a secondary VoIP account. Assigning an additional number allows you to receive phone calls for this number. By default outgoing calls are via the extension number. However in the event calling is not possible via the extension number, the call will be routed via this number.

Parameter	Description
For the following 4 items, check the box to enable the function:	
• Answer calls for all numbers	Check this box to answer all incoming calls.
• Call Waiting	Call Waiting plays audible tone to notify the user that a second call is in waiting. The user can place the existing call on hold and answer the incoming call using hook flash. Note: Call Hold and Call Waiting must be supported by the VoIP provider to use this feature.
• Caller-ID Presentation	A function to display the caller's number.
• Different dial tone for VoIP	Enabling this function gives a different dial tone when making VoIP calls. This feature allows you to differentiate if the outgoing call is over PSTN or VoIP.
Telephony Hook Flash Timer	This option allows you to define the length of time in milliseconds (ms) before the hook flash timer indicates a time-out. A hook flash is when you ON-hook then OFF-hook the phone. Hook flash is used to switch between two calls.

SIP Setting

The following SIP related parameters are configurable.



Parameter	Description
SIP Parameters	
SIP Listen Port	This option allows you to change the default SIP Listen Port. The default setting is 5060. It is recommended to leave this value unchanged.
Codec Rate(G723, G729, G711)	You can select the desired Codec rate. It is recommended to leave this value unchanged.

Port Advanced Setting

There are 11 advanced functions that can be configured in this screen.

- **Volume Gain Control:** Two modes are available. The fixed gain control means the device is supported to supply a constant level of amplification.
  The adaptive mode means a specified power level is produced at the output during periods of active speech.

- **Jitter Buffer Mode**: Three jitter modes are available. The fixed mode, which is the default mode, is a simple first in first out mode, with a fixed jitter buffer delay.
  The adaptive mode optimizes the size of the jitter buffer delay in response to network conditions.
  The sequential mode is also a fixed jitter buffer delay mode, but in this mode the jitter buffer function looks at the packet number for dropped or out of sequence packet problems.

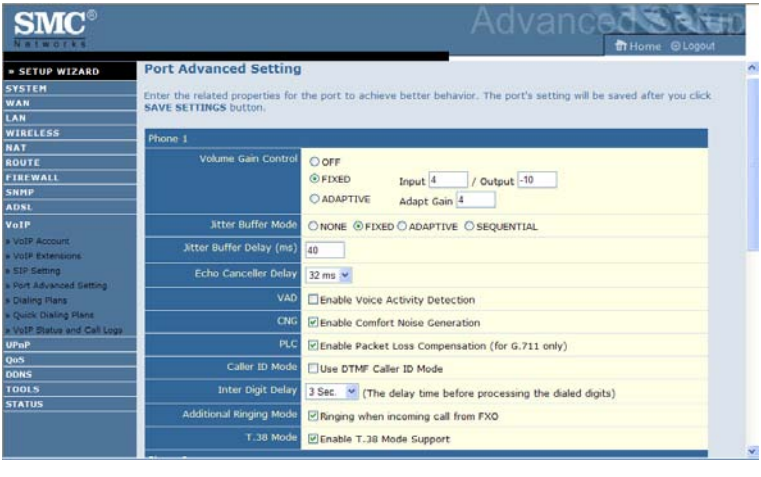
- **Jitter Buffer Delay:** This parameter represents the delay in milliseconds that the jitter buffer waits before it transmits the data samples that are collected from the host processor to the CODEC**.**

- **Echo Canceller Delay:** This is the function that filters out echoes occurred during periods of active speech.

- **VAD (Voice Activity Detection):** If this box is checked, only a certain level of voice volume will be send out as voice packets. This function is designed to save the bandwidth.

- **CNG (Comfort Noise Generation):** Check this box to enable the Comfort Noise Generation function. When no one is talking on a call this feature will generate comfort noise in the background so you know the call is active.

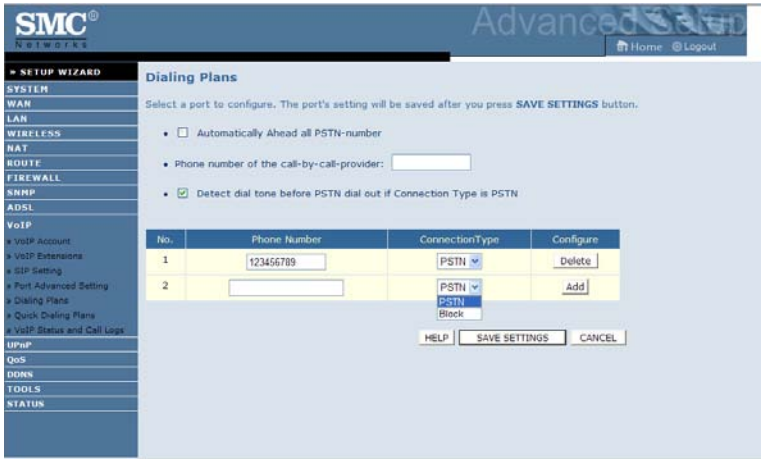
- **PLC (Packet Loss Compensation):** During the transmission of a series of packets, if one of them is lost, then the device will use the mathematical algorithm to calculate a value to make up the lost packet. This function is designed to make the voice conversation more smooth.
- **Caller ID Mode:** Check this box to use Dual Tone Multi-Frequency (DTMF) to send out the caller ID.
- **Inter Digit Delay**: This is the delay time before processing each dialed digit.
- **Additional Ringing Mode**: The ringing tone will sound when incoming calls from FXO.
- **T.38 Mode**: This is the fax over UDP feature, which enables fax data transmission (using the T.38 fax protocol) over UDP.



Parameter	Description
Volume Gain Control Jitter Buffer Mode Jitter Buffer Delay Echo Canceller Delay	It is recommended leaving these four settings at the default value. Changing the settings may affect the performance of VoIP and the voice quality. If you should need to change these settings, consult an experienced network administrator.
VAD	Check this box to enable the Voice Activity Detection function.
CNG	Check the box to enable the Comfort Noise Generation function.
PLC	This function is for G.711 only. Check the box to enable the Packet Loss Compensation function.
Caller ID Mode	By default the Barricade uses FSK Caller ID mode. To enable DTMF Caller ID mode check this box.
Inter Digit Delay	This is the delay time before processing each dialed digit. Increasing the value allows more time between dialling digits.
Additional Ringing Mode	Check the box to enable this function.
T.38 Mode	Check this box to enable T.38 Fax support.

Dialing plans

Dialing plans allow you to define the connection type used when a specified number is dialed. For example you may want numbers beginning "0800" to dial out over PSTN. Alternatively you may want numbers beginning "012" to dial out over the Internet (VoIP). Also you may want to block certain numbers from being dialed.



Parameter	Description
Automatically Ahead all PSTN-number	Check this box to automatically add the number which you have entered on the "Phone number of the call-by-call provider" space ahead of the numbers that you dial.
Phone number of the call-by-call-provider	This function is used in conjunction with the "Automatically ahead all PSTN-number". This is the number that you want the Barricade to add automatically in front of the number that you actually dial.
Detect dial tone before PSTN dial out if connection type is PSTN	Check this box to detect a dial tone before making a PSTN call. If no dial tone is detected the call will fail. When this option is disabled the number is dialled without detecting dial tone.

To set-up a dialing plan, take the following steps:

1. In the Phone number column enter a specific phone number, or the starting digits of a phone number that you want to create a dialing plan for.
   Example: If you enter "012" all phone numbers beginning "012" will dial out using the connection type defined.

2. Select the required connection type from the drop-down list. The connection type defines how the number is dialed, e.g. via PSTN or Internet, or if the call is Blocked.

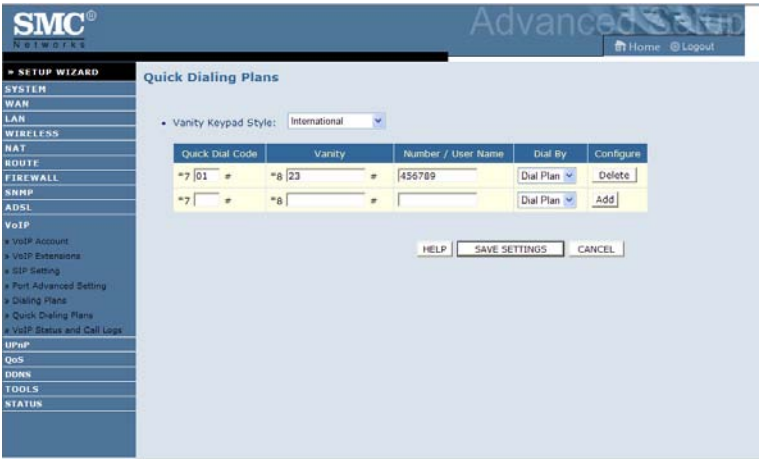
3. Click **Add** to add the dialing plan.

4. When you have finished creating your dialing plans, click **Save settings**.

Notes: By default all numbers dialled will use VoIP connection.

Quick Dialing Plans

This function allows you to configure up to 20 quick dialing plans. This is done by assigning a quick dial code for a specified phone number.



- Quick Dial Code: Enter quick dial code in the range of 01 to 20. To call the phone number associated with the quick dial code you would need to dial ***7[Quick Dial Code]#** .

- Vanity: Vanity converts the English alphabet to numbers. Take a look at your phone, you can see that characters a, b, and c, are represented by 2. Character d, e, and f, are represented by 3. Therefore, a person named "Frank" would translate to the numbers "37265" on your phone keypad. This provides an alternative to remembering the quick dial code and associated phone number by allowing you to enter a name which associated with the phone number.

- Number/User Name: Enter the phone number or user name you wish to associate with the quick dial code.

The following example shows how to set up a quick dialing plan for Frank who has the phone number 6194621719:

1. Select the vanity keypad style from the pull-down menu.

2. Enter the number "01" for the Quick Dial Code.

3. Enter the name "Frank" in the Vanity column.

4. Enter "6194621719" for the phone number/user name.

5. Click **Add**, and then **Save Settings**.

This Quick Dial Plan will then allow you to call Frank by either:

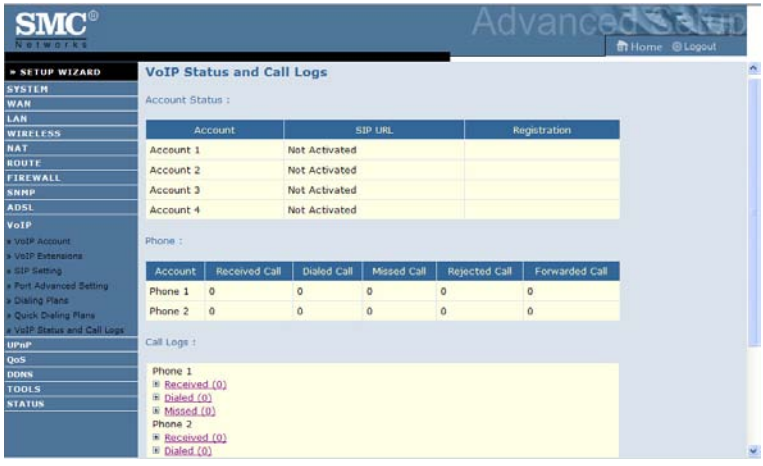
Dialing the Quick Dial code: *701#

or

Dialing with Vanity code: *837265#.

VoIP Status and Call logs

This page displays the VoIP registration status for accounts 1 - 4 and the call logs.



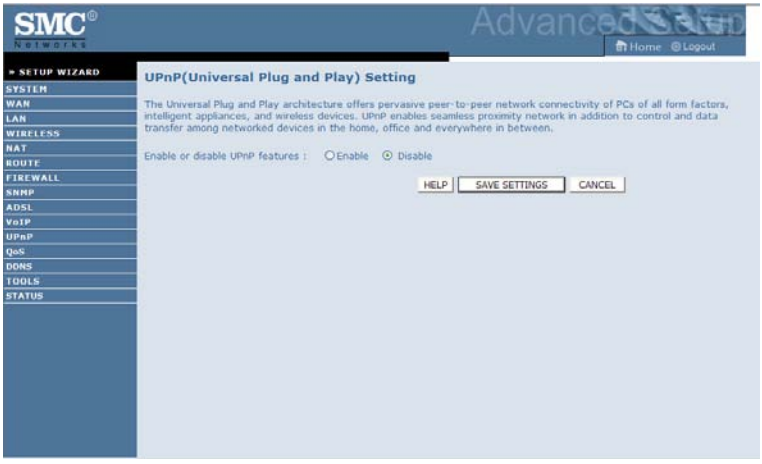
Parameter	Description
Account	SIP accounts 1 to 4.
SIP URL	Displays SIP URL for the corresponding account.
Registration	Displays SIP registration status for the corresponding account. The registration status will display "Success" for successful registration or "Fail" for failure.
Received Call	Number of received calls.
Dialed Call	Number of calls made.
Missed Call	Number of calls missed.
Rejected Call	Number of rejected calls.
Forwared Call	Number of forwared calls.

Click the **Refresh** button to update the status and log.

UPnP

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

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



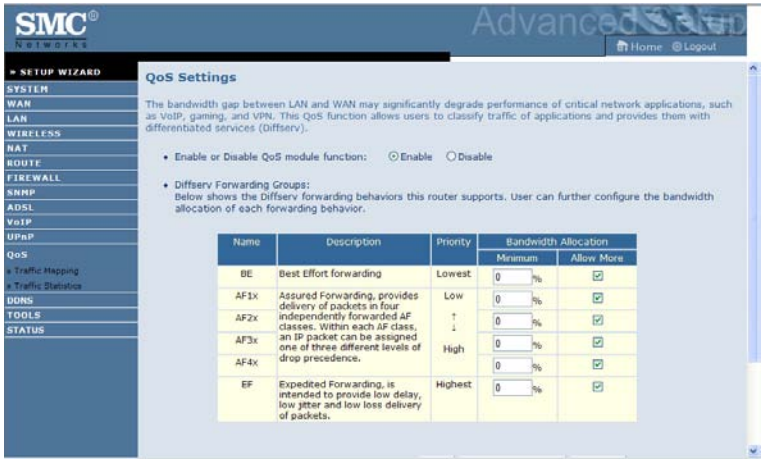
UPnP allows the device to automatically:

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

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

QoS

The QoS (Quality of Service) function allows you to differentiate VoIP traffic and provide it with high-priority forwarding service. In addition, you can specify the outgoing VC of VoIP packets to further guarantee the voice quality.



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.

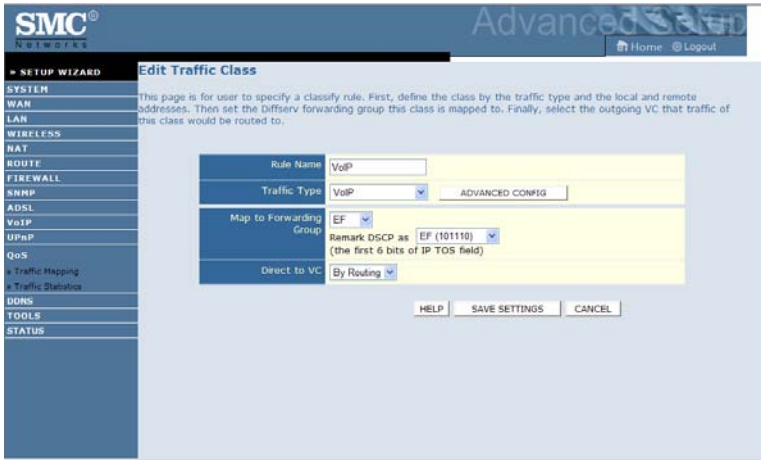
- Assured forwarding, defined in RFC 2597
- Expedited forwarding, defined in RFC 2598

Traffic Mapping

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

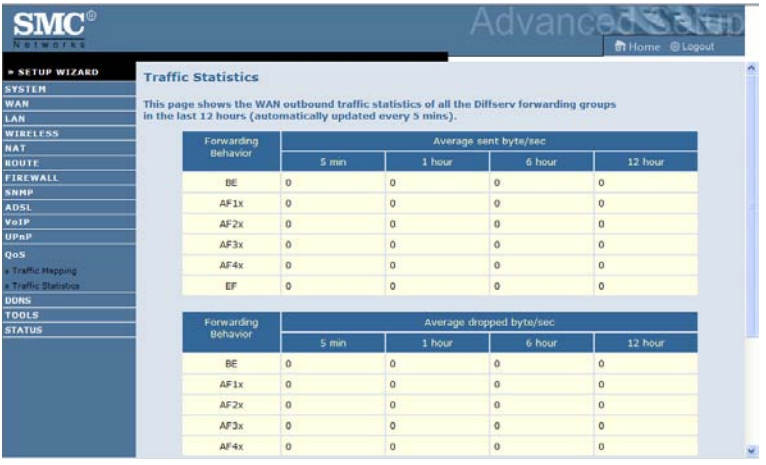
To create a new traffic class:

1. Click **ADD TRAFFIC CLASS** on the Edit Traffic Class screen.
2. Define the appropriate settings for traffic class.
3. Click **SAVE SETTINGS** to save your settings.



Traffic Statistics

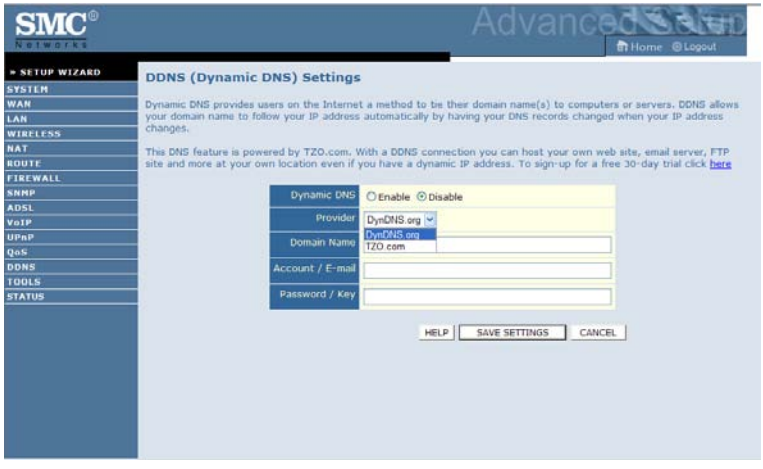
This screen shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours.



DDNS

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

This DNS feature is powered by DynDNS.org or TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

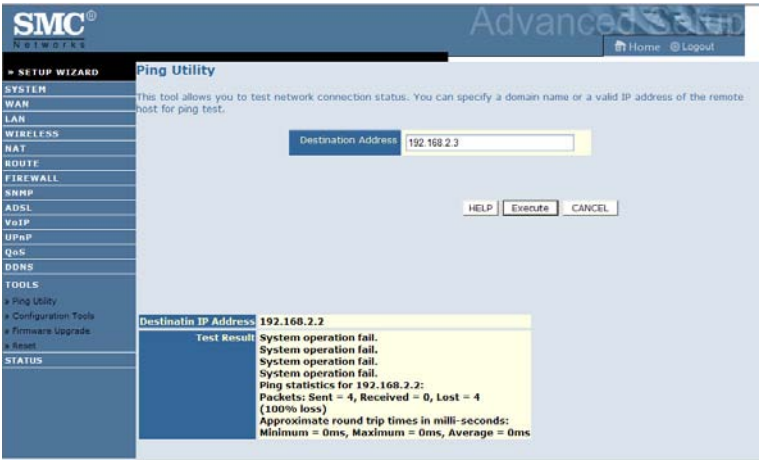


TOOLS

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

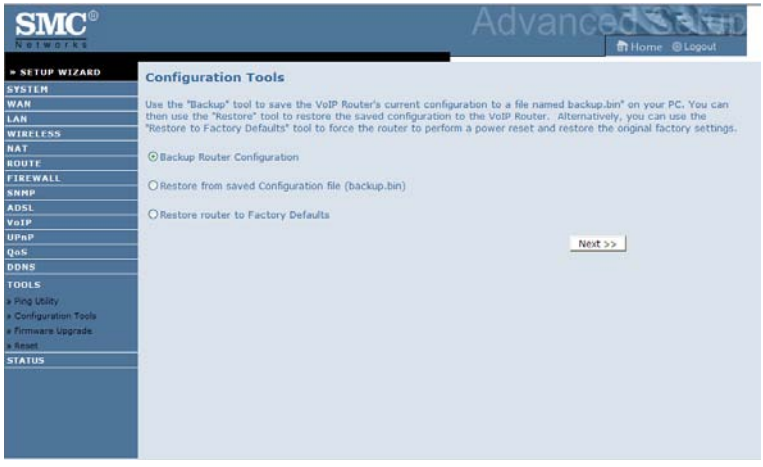
Ping Utility

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.



Configuration Tools

Choose a function and click **Next**.



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

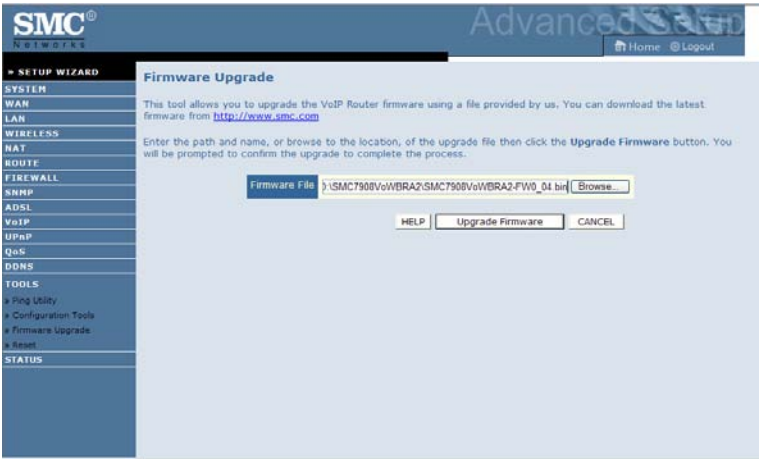
Firmware Upgrade

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

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

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

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



Reset

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

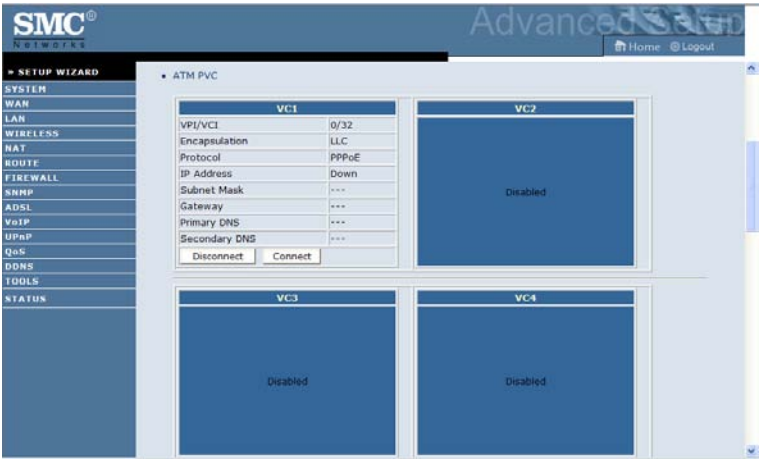
If you perform a reset from this screen, the configurations will not be changed back to the factory default settings.

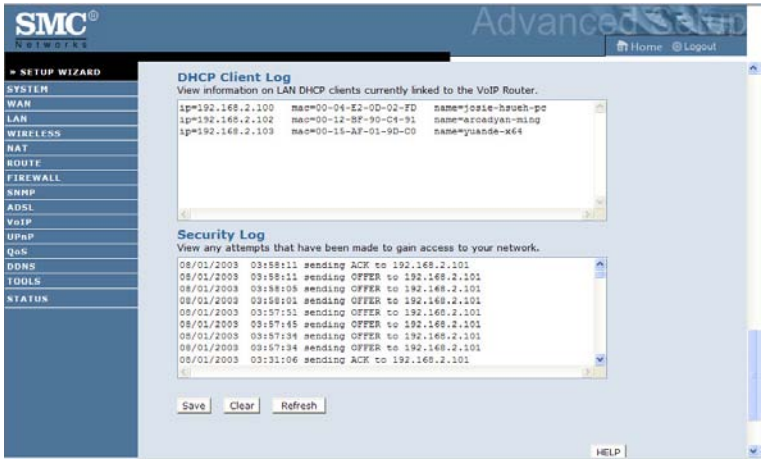
Note: If you use the Reset button on the back panel, the Barricade performs a power reset. If the button is pressed for over 10 seconds, all the LEDs will illuminate and the factory default settings will be restored.

STATUS

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

Scroll down to view more information on the Status screen.





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.
Disconnect	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.

Troubleshooting Chart	
Symptom	**Action**
Wireless Problems	
A wireless PC cannot associate with the Barricade.	• Make sure the wireless PC has the same SSID settings as the Barricade. See "Channel and SSID" on page 4-37 • You need to have the same security settings on the clients and the Barricade. See "Access Control" on page 4-38.
The wireless network is often interrupted.	• Move your wireless PC closer to the Barricade to find a better signal. If the signal is still weak, change the angle of the antenna. • There may be interference, possibly caused by a microwave ovens or wireless phones. Change the location of the interference sources or of the Barricade. • Change the wireless channel on the Barricade. See "Channel and SSID" on page 4-37. • Check that the antenna, connectors, and cabling are firmly connected.
The Barricade cannot be detected by a wireless client.	• The distance between the Barricade and wireless PC is too great. • Make sure the wireless PC has the same SSID and security settings as the Barricade. See "Channel and SSID" on page 4-37 and "Access Control" on page 4-38.

APPENDIX B
CABLES

Ethernet Cable

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

Specifications

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

Wiring Conventions

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

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

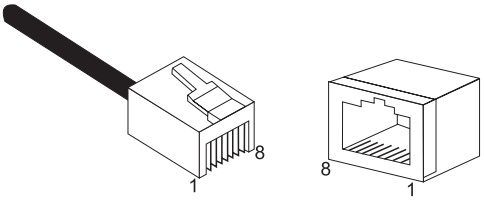


Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Connection

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

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

Pin Assignments

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

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

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

Straight-Through Wiring

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

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

Crossover Wiring

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

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

ADSL Cable

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-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.

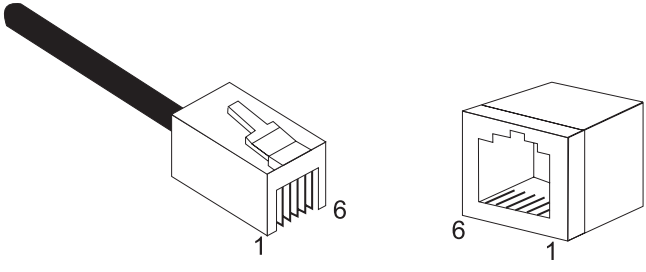
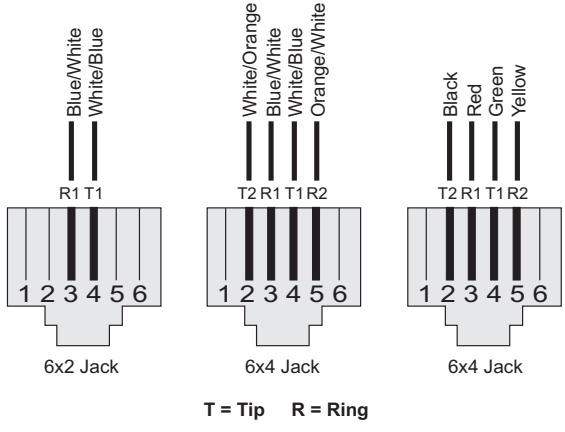


Figure B-2. RJ-11 Connector Pin Numbers



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 RJ-11 port
Two Phone ports
One Line port

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

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

VoIP Features
SIP
Codec - G.711, G.723, G.729a, G.168

Modulation Type
OFDM, CCK

Radio Features

Wireless RF module Frequency Band
802.11g Radio: 2.4GHz
802.11b Radio: 2.4GHz
USA - FCC
2412~2462MHz (Ch1~Ch11)
Canada - IC
2412~2462MHz (Ch1~Ch11)
Europe - ETSI
2412~2472MHz (Ch1~Ch13)
Spain
2457~2462MHz (Ch10~Ch11)
France
2457~2472MHz (Ch10~Ch13)
Japan - STD-T66/STD-33
2412~2484MHz (Ch1~Ch14)

Operating Channels IEEE 802.11b compliant:

11 channels (US, Canada)
13 channels (ETSI)
2 Channels (Spain)
4 Channels (France)
14 channels (Japan)

Operating Channels IEEE 802.11g compliant:

13 channels (US, Canada, Europe, Japan)

RF Output Power Modulation Rate-Output Power (dBm)

802.11b - 1Mbps 16
802.11b - 2Mbps 16
802.11b - 5.5Mbps 16
802.11b - 11Mbps 16

Modulation Rate-Output Power (dBm)

802.11g - 6Mbps 15
802.11g - 9Mbps 15
802.11g - 12Mbps 15
802.11g - 18Mbps 15
802.11g- 24Mbps 15
802.11g - 36Mbps 15
802.11g- 48Mbps 15
802.11g - 54Mbps 15

Sensitivity Modulation Rate-Receiver 2.412 ~ 2.484 GHz Sensitivity (dBm)

802.11b - 1Mbps -90
802.11b - 2Mbps -88
802.11b - 5.5Mbps -85
802.11b- 11Mbps -84

Modulation Rate-Receiver Sensitivity Typical (dBm)
802.11g - 6Mbps -88
802.11g - 9Mbps -87
802.11g - 12Mbps -84
802.11g - 18Mbps -82
802.11g - 24Mbps -79
802.11g - 36Mbps -75
802.11g - 48Mbps -68
802.11g - 54Mbps -68

Temperature: IEC 68-2-14
0 to 50 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: 233.5 x 155 x 38.5 (mm)

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

Safety
CSA/NRTL (UL1950, CSA 22.2.950) GS (EN60950), CB (IEC60950)

SMC Networks

TECHNICAL SUPPORT
From U.S.A. and Canada (24 hours a day, 7 days a week)
Phn: 800-SMC-4-YOU / 949-679-8000
Fax: 949-502-3400

ENGLISH
Technical Support information available at www.smc.com

FRENCH
Informations Support Technique sur www.smc.com

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

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

DUTCH
Technische ondersteuningsinformatie beschikbaar op www.smc.com

PORTUGUES
Informações sobre Suporte Técnico em www.smc.com

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

INTERNET
E-mail address: techsupport@smc.com

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

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

SMC7908VoWBRA2