



# Cable/DSL Broadband Router

Built-in 4-Port 10/100Mbps Switch

User Guide

**SMC7004VBR V.2**



# **Cable/DSL Broadband Router Built-in 4-Port 10/100Mbps Switch User Guide**

---

From SMC's Barricade™ line of Broadband Routers

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>1</b>
Features and Benefits .....	2
Package Contents .....	3
Minimum Requirements .....	4
<b>Getting to Know the Barricade™</b> .....	<b>5</b>
LED Indicators .....	6
<b>Getting Connected</b> .....	<b>7</b>
Basic Installation Procedure .....	7
<b>Configuring your Computer</b> .....	<b>9</b>
Configuring Windows 95/98/Me .....	9
Configuring Windows 2000 .....	11
Configuring Windows XP .....	13
Configuring a Macintosh Computer .....	14
<b>Configuring the Barricade™</b> .....	<b>15</b>
Browser Configuration .....	15
Disable Proxy Connection .....	16
Accessing the Barricade™ Management .....	17
<b>Navigating the Web-based Administration</b> .....	<b>19</b>
Making Configuration Changes .....	19
Setup Wizard .....	21
Step One: Time Zone .....	21
Step Two: Broadband Type .....	22
Step Three: Finish Configuration .....	23
Advanced Setup .....	23
System .....	24
WAN .....	27
LAN .....	33
NAT .....	34
Firewall .....	36

*Table of Contents*

DDNS (Dynamic DNS) ..... 41  
UPnP ..... 42  
Tools ..... 43  
Status ..... 44

**Troubleshooting .....47**

**Technical Specifications .....53**

**Compliances ..... i**

**Legal Information and Contacts .....v**

# INTRODUCTION

Congratulations on your purchase of a Barricade™ Cable/DSL Broadband Router (SMC7004VBR). SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet.

## Important Information!

**This information is addressed to the DSL-Users without a flat rate contract\*\*.**

With your DSL-router you have received a device of high quality, which allows you fast and easy access to the Internet.

The factory default settings of this router have been done in a way to provide you with uninterrupted access and use of the Internet. With this background for cost reasons we recommend that you enter into a "flat rate" – contract with your DSL-line provider.

### **Why should you do that?**

Please consider that a router, an entirely independent working device, does not switch off automatically when shutting off your PC!

You may trigger such an automatic shut-off by setting a so called "idle-time" (for details consult your manual at PPPoE or PPTP WAN access configuration). Depending at the set time (1 to 5 min) the router cuts the DSL-link when idle, indeed. But this still does not provide for 100% security.

## *Introduction*

This disconnect only happens if there are no more open requests received from either the LAN or the WAN side (here this can be requests from the internet, i.e. initiated through the use of so called file sharing programs like eMule, eDonkey, etc.) that keep the router active.

In order to counter such incalculable activity and protect yourself from higher than expected on-line costs we therefore recommend again a flat-rate contract for your DSL-connection.

The only safe alternative: Pull the plug!

That is to disconnect your router from the mains.

Please feel free to contact our SMC-hotline if you have further questions.

\*\* Flat-rate is an offer of your DSL-line provider, which gives you timely unlimited access to the Internet at a defined (flat-) rate.

## **Features and Benefits**

- Internet connection to DSL or cable modem via a 10/100 Mbps WAN port.
- Local network connection via 10/100 Mbps Ethernet switch ports.
- DHCP for dynamic IP configuration, and DNS for domain name mapping.
- Firewall with Stateful Packet Inspection, client privileges, hacker prevention, DoS, and NAT.
- NAT also enables multi-user access with a single-user account, and virtual server functionality (providing protected access to Internet services such as web, mail, FTP, and Telnet).

- Virtual Private Network support using PPTP, L2TP, or IPsec pass-through.
- User-definable application sensing tunnel supports applications requiring multiple connections.
- Parental controls allows the user to block access to certain web sites.
- Email alerts when the users network is being compromised.
- Easy setup through a web browser on any operating system that supports TCP/IP.
- Compatible with all popular Internet applications.

## **Package Contents**

Before installing the Barricade™ Cable/DSL Broadband Router, verify that you have the items listed under Package Contents. Also be sure that you have the necessary cabling. If any of the items are missing or damaged, contact your local SMC distributor.

- Barricade™ Broadband Router.
- Power adapter.
- One CAT-5 Ethernet cable.
- Four rubber feet.
- One CD-ROM.

If possible, retain the carton and original packing materials in case there is a need to return the product.

## **Minimum Requirements**

- Cable or DSL Modem with Ethernet connection and Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem or cable modem.
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or USB-to-Ethernet converter.
- Network adapter with Ethernet (UTP CAT 5) cabling and TCP/IP protocol installed per PC.
- Internet Explorer 4.0 (or Higher) or Netscape Navigator 4.7 (or Higher) for Web-based configuration of the Barricade™.



# GETTING TO KNOW THE BARRICADE™

The SMC7004VBR Barricade™ Cable/DSL Broadband Router is the perfect solution for the home/office environment. This fullfeatured router offers:

- 4 – 10/100 Mbps Auto-Sensing LAN ports with Auto-MDI MDIX feature.
- 1 – 10/100 Mbps WAN port with Auto-MDI MDIX feature.
- Comprehensive LEDs for network status and troubleshooting.
- [Reset] Button.



## LED Indicators

The Barricade™ includes LED indicators on the front panel that simplify installation and network troubleshooting.

LED	ON	OFF	FLASHING
<b>PWR</b>	Receiving power	Not receiving power	N/A
<b>WAN</b>	Good WAN connection detected	No WAN connection detected	Transmitting or receiving traffic
<b>LINK/ACT</b>	Good LAN connection detected	No LAN connection detected	Transmitting or receiving traffic
<b>10/100 Mbps</b>	LAN port operating at 100 Mbps	LAN port operating at 10 Mbps	N/A

### Resetting the Barricade™

The [Reset] button is located on the rear panel of the Barricade™ Broadband Router. Use a paper clip or a pencil tip to push the Reset button.

#### Reset

If the Router is having problems connecting to the Internet, simply unplug the router for 3 seconds then plug back in.

#### Restore Factory Defaults

If resetting the router does not resolve your issue, then you can follow these steps:

1. Leave power plugged into the router.
2. Locate the [Reset] button on the back panel, press and hold until WAN LED flashes off.
3. Release [Reset] button.

# GETTING CONNECTED

The SMC7004VBR Barricade™ Cable/DSL Broadband router is connected between the Cable/DSL Broadband Modem and your computers. If you have more than one computer to connect, simply plug the other computers into the LAN ports on the back of the router.



## Basic Installation Procedure

### 1. Connect the LAN

Run an Ethernet cable from one of the LAN ports on the back of the Barricade™ to your computer's network adapter.

### 2. Connect the WAN

Connect an Ethernet cable from your cable or DSL modem to the Barricade™'s WAN port on the back on the router.

### 3. Power on

Connect the power cable to the Barricade™.

Once you have completed connecting all of the hardware, simply insert the Barricade™ CD-ROM and the EZ 3-Click Installation Wizard will automatically connect you to the Internet.

For configuration of the PCs, see *Configuring your Computer*.

For advanced configuration of the Barricade™ Broadband Router, see *Configuring the Barricade™*.

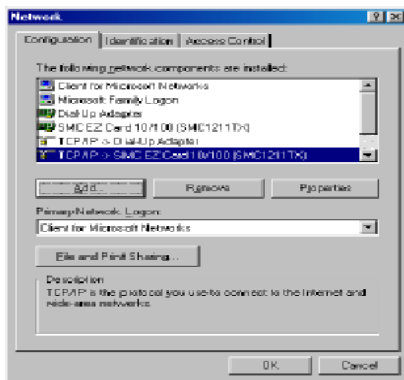
# CONFIGURING YOUR COMPUTER

The information outlined in this chapter will guide you through the configuration for the following Operating Systems:

- Windows 95/98
- Windows Me
- Windows 2000
- Windows XP
- Apple Macintosh

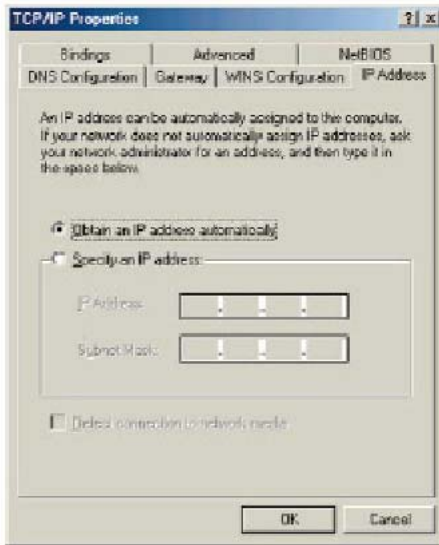
## Configuring Windows 95/98/Me

1. Access your network settings by clicking [Start], choose [Settings], and then select [Control Panel].
2. In the Control Panel, locate and double-click the [Network] icon.



## Configuring your Computer

3. Highlight the TCP/IP line that has been assigned to your network card on the [Configuration] tab of the [Network] properties window.
4. Next, click the [Properties] button to view that adapter's TCP/IP settings.



5. From the [TCP/IP Properties] dialog box, click the [Obtain an IP address automatically] option.
6. Next click on the [Gateway] tab and verify the [Gateway] field is blank. If there are IP addresses listed in the [Gateway] section, highlight each one and click [Remove] until the section is empty.

7. Click the [OK] button to close the [TCP/IP Properties] dialog box.
8. On the [Network Properties] window, click the [OK] button to save these new changes.

**Note:** Windows may ask you for the original Windows installation disk or additional files. Check for the files at `c:\windows\options\cabs`, or insert your Windows CD-ROM into your CD-ROM drive and check the correct file location, for example, `D:\win98`, `D:\win9x`. (assume "D" is your CD-ROM drive).

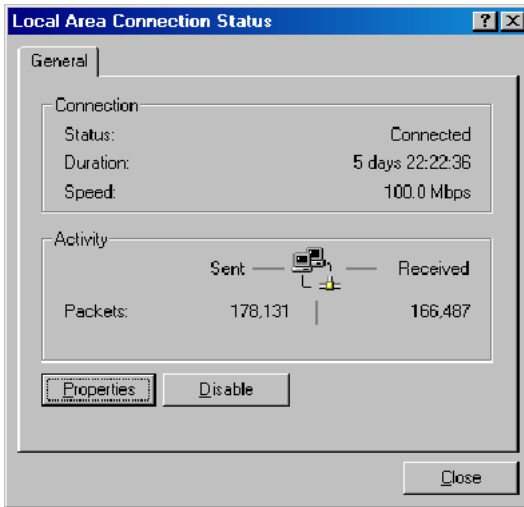
9. Windows may prompt you to restart the PC. If so, click the [Yes] button. If Windows does not prompt you to restart your computer, do so anyways to ensure your settings.

## **Configuring Windows 2000**

1. Access your network settings by clicking [Start], choose [Settings], and then select [Control Panel].
2. In the Control Panel, locate and double-click the [Network and Dial-up Connections] icon.

## Configuring your Computer

3. Locate and double-click the [Local Area Connection] icon for the Ethernet adapter that is connected to the Barricade™. When the [Status] dialog box window opens, click the [Properties] button.

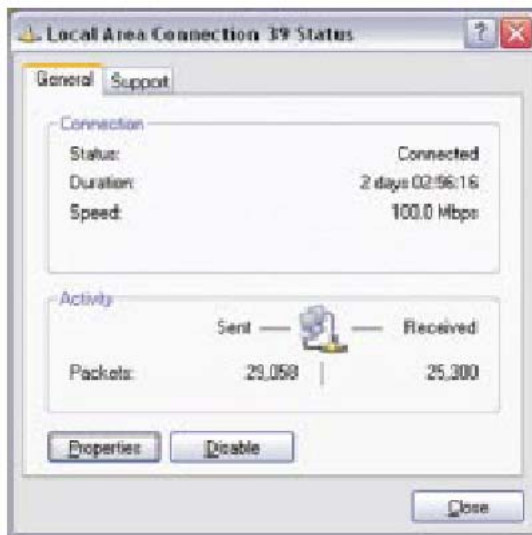


4. On the [Local Area Connection] Properties box, verify the box next to [Internet Protocol (TCP/IP)] is checked. Then highlight the Internet Protocol (TCP/IP), and click the [Properties] button.
5. Select [Obtain an IP address automatically] to configure your computer for DHCP. Click the [OK] button to save this change and close the [Properties] window.
6. Click the [OK] button again to save these new changes.
7. Reboot your PC.

## Configuring Windows XP

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000 outlined above.

1. Access your network settings by clicking [Start], choose [Control Panel], select [Network and Internet Connections] and then click on the [Network Connections] icon.
2. Locate and double-click the [Local Area Connection] icon for the Ethernet adapter that is connected to the Barricade™ Router. Next, click the [Properties] button.



3. On the [Local Area Connection] Properties box, verify the box next to [Internet Protocol (TCP/IP)] is checked. Then highlight the Internet Protocol (TCP/IP), and click the [Properties] button.



## *Configuring your Computer*

4. Select [Obtain an IP address automatically] to configure your computer for DHCP. Click the [OK] button to save this change and close the [Properties] window.
5. Click the [OK] button again to save these new changes.
6. Reboot your PC.

## **Configuring a Macintosh Computer**

You may find that the instructions here do not exactly match your screen. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 8.5.

1. Pull down the [Apple] Menu. Click [Control Panel] and select [TCP/IP].
2. In the [TCP/IP] dialog box, make sure that [Ethernet] is selected in the [Connect Via:] field.

If [Using DHCP Server] is already selected in the [Configure] field, your computer is already configured for DHCP. Close the [TCP/IP] dialog box, and skip to Step 2 Disable HTTP Proxy (bottom of this page).

3. All the information that you need to record is on the [TCP/IP] dialog box. Use the space below to record the information.
4. Select [Using DHCP Server] in the [Configure] field and close the window.
5. Another box will appear asking whether you want to save your TCP/IP settings. Click [Save].

# CONFIGURING THE BARRICADE™

After you have configured TCP/IP on a client computer, use a web browser to configure the Barricade™ Broadband Router. The Barricade™ can be configured by any Java-supported browser including Internet Explorer 4.0 or above, or Netscape Navigator 4.7 or above. Using the web management interface, you may configure the Barricade™ and view statistics to monitor network activity.

**Note:** Before you attempt to configure your router, if you have access to the Internet please visit [www.smc.com](http://www.smc.com) or [www.smc-europe.com](http://www.smc-europe.com) and download the latest firmware update.

Before you attempt to log into the Barricade™'s Web-based Administration, please verify the following:

1. Your browser is configured properly (see below).
2. Disable any firewall or security software that may be running.
3. Confirm that you have a good "link" LED where your computer is plugged into the Barricade™. If you don't have a "link" light, try another cable until you get a good link.

## Browser Configuration

Confirm your browser is configured for a direct connection to the Internet using the Ethernet cable that is installed in the computer. This is configured through the options/preference section of your browser.

## **Disable Proxy Connection**

You will also need to verify that the HTTP Proxy feature of your web browser is disabled. If it is disabled, your web browser will be able to view the Barricade™ configuration pages. The following steps are for Internet Explorer and for Netscape. Determine which browser you use and follow the appropriate steps.

### **Internet Explorer (5 or above)**

1. Open Internet Explorer. Click [Tools], and then select [Internet Options].
2. In the [Internet Options] window, click the [Connections] tab.
3. Click the [LAN Settings] button.
4. Clear all the check boxes and click [OK] to save these LAN settings changes.
5. Click [OK] again to close the [Internet Options] window.

### **Netscape (4 or above)**

1. Open Netscape. Click [Edit], and then select [Preferences].
2. In the [Preferences] window, under [Category], double-click [Advanced], then select the [Proxies] option.
3. Check [Direct connection to the Internet].
4. Click the [OK] button to save the changes.

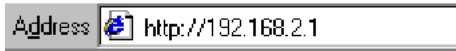
## Accessing the Barricade™ Management

To access the Barricade™'s web-based management screens, follow the steps below:

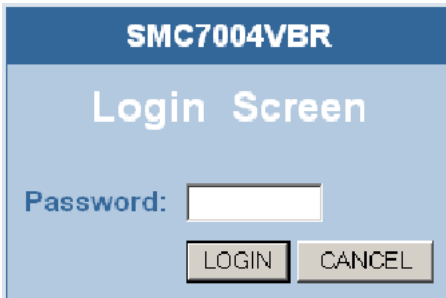
1. Launch your web-browser.

**Note:** Your computer does not have to be ONLINE to configure the Barricade™ Router.

2. In the Address Bar, type: <http://192.168.2.1>



3. When the Barricade™'s Login screen appears, enter the default password, and click the [Login] button to access the router.



**Note:** The Barricade™ default password is smcadmin.  
The password is case sensitive.

Once you have logged into the Barricade™ web-based admin screens, you have 2 options which are outlined in Navigating the Web-based Administration.

# NAVIGATING THE WEB-BASED ADMINISTRATION

The Barricade™'s management interface features a Setup Wizard and an Advanced Setup section. Use the Setup Wizard if you want to quickly setup the Barricade™ for use with a cable modem or DSL modem. Advanced setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, intrusion detection, virtual server setup, virtual DMZ hosts, as well as other advanced functions.

## **Making Configuration Changes**

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click the [Apply] or [Next] button at the bottom of the page to enable the new setting.

## Navigating the Web-based Administration

**Note:** To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 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].



The screenshot displays the SMC Networks web-based administration interface. At the top left, the SMC Networks logo is visible. The main content area is divided into several sections:

- Setup Wizard:** A section with a small image of a child at a computer. The text reads: "The Barricade setup will allow you to configure your Barricade for use with an external Cable or DSL modem. Click on the navigation menu on the left to change individual settings."
- Advanced Setup:** A section with a small image of a person in a dark room. The text reads: "The Barricade supports advanced functions like Intrusion Detection, IP and MAC address filtering, parental control, virtual servers, and special applications. We recommend you keep the default settings."
- Overview:** A section with the text: "Thank you for purchasing the SMC EZ Connect Barricade Broadband Router. The Barricade is a secure device ideal for home networking and small business users alike. Its easy setup will allow you to enjoy risk-free Internet access within minutes."

# Setup Wizard

Below is an outline of each option available from the [Setup Wizard] section. This wizard takes 3 steps to complete an ISP configuration.

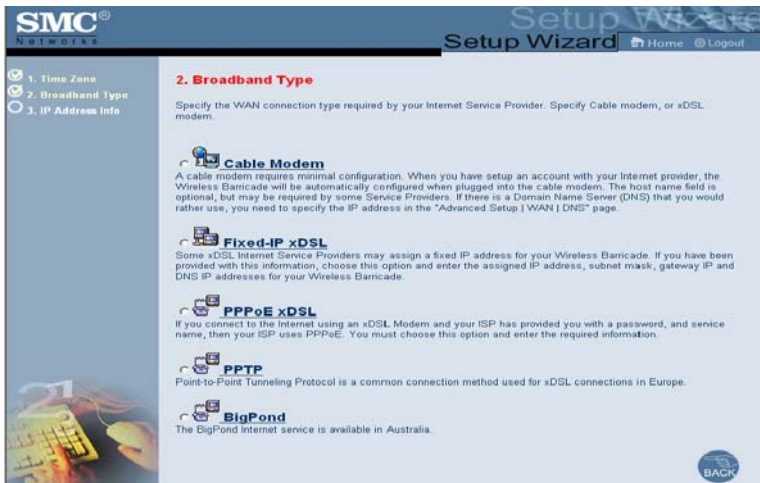
## Step One: Time Zone

The first step is to configure the Time Zone you are located in. This setting is used for accurate timing of client filtering and log events.



### Step Two: Broadband Type

Select the type of broadband connection you have.



- **[Cable Modem]**

Your ISP may have given you a host name. If so, enter it into this field.

- **[Fixed-IP xDSL]**

Some xDSL Internet Service Providers may assign a fixed (static) IP address for your gateway. If you have been provided with this information, choose this option and enter the assigned IP address, subnet mask, gateway IP, and DNS IP addresses for the Barricade™.



- **[PPPoE]**

Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Leave the Maximum Transmission Unit (MTU) on the default value (1492) unless you have a particular reason to change it. Enter a maximum idle time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will be dropped. Enable the [Auto-reconnect] option to automatically re-establish the connection as soon as you attempt to access the Internet again.

- **[PPTP]**

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.

- **[BigPond®]**

The BigPond® Internet service is used in Australia.

### Step Three: Finish Configuration

Once you have configured your type of ISP connection, simply click the [Finish] button and the Barricade™ will automatically configure your Internet connection.

## Advanced Setup

Below is an outline of the [Advanced Setup] section. This section is used to manually configure your ISP connection and also define the advanced system parameters, manage and control the Barricade™ and its ports, or monitor network conditions.

# Navigating the Web-based Administration

## System

This section is used to configure the local time zone, password for administrator access, and the IP address of a PC that will be allowed to manage the Barricade™ remotely.

- **[Time Zone]**

Use this option to configure the time zone for the Barricade™. This information is used for log entries and client access control.

There are 3 options to configure the Router's internal clock:

- Using preset or custom NTP servers.
- Using your computer system's clock.
- Manually configure the Time and Date.

The screenshot shows the 'Time Zone' configuration page in the SMC Networks Advanced Setup interface. The page has a blue header with the SMC Networks logo and navigation links for Home and Logout. A left sidebar contains a menu with options like System, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Time Zone' and includes instructions on how to configure the system time. Three radio buttons are used to select a configuration method: 'Set Date and Time by online Time Servers (NTP)', 'Set Date and Time using PC's Date and Time', and 'Set Date and Time manually'. The first option is selected, showing a dropdown for 'Time Zone' set to '(GMT-08:00)Pacific Time (US & Canada): Tijuana', a 'Pre-set Servers' dropdown set to 'time.nist.gov', and a 'Custom Server' input field with a 'Sync Now!' button. The second option is also visible, showing a 'Computer Time/Date' field set to 'Thursday, June 19, 2003 11:18:06 PM'. The third option shows fields for 'Date' (Year: 2003, Month: Jun, Day: 19) and 'Time' (Hour: 22, Minute: 35, Second: 44). At the bottom right, there are buttons for HELP, APPLY, and CANCEL.

- **[Password Settings]**

Use this menu to restrict access based on a password. By default, the password is smcadmin.

**Note:** Passwords can contain up to 9 alphanumeric characters and are case sensitive.

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System (expanded), Time Zone, Password Settings, Remote Management, WAN, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Password Settings" and includes the following text: "Set a password to secure access to the Barricade Web Management. You can also configure the amount of time that you will stay logged into the router using the idle time settings." Below this text are two sections: "Password Options" and "Idle Time Out Settings".

Password Options	
Current Password :	<input type="password"/>
New Password :	<input type="password"/>
Confirm New Password :	<input type="password"/>

Idle Time Out Settings	
Idle Time Out :	<input type="text" value="0"/> Mins (Idle Time =0 : NO Time Out)

At the bottom right of the interface are three circular buttons: HELP, APPLY, and CANCEL.

- **[Remote Management]**

This feature allows a remote PC to configure, manage, and monitor the Barricade™ using a standard web browser.

1. Check [Enable].
2. Set the [Allow Access to] policy to one of the 2 options:

**[Any IP Address]**

You can remotely manage the Barricade™ from any IP address on the WAN side.

# Navigating the Web-based Administration

## [Single IP]

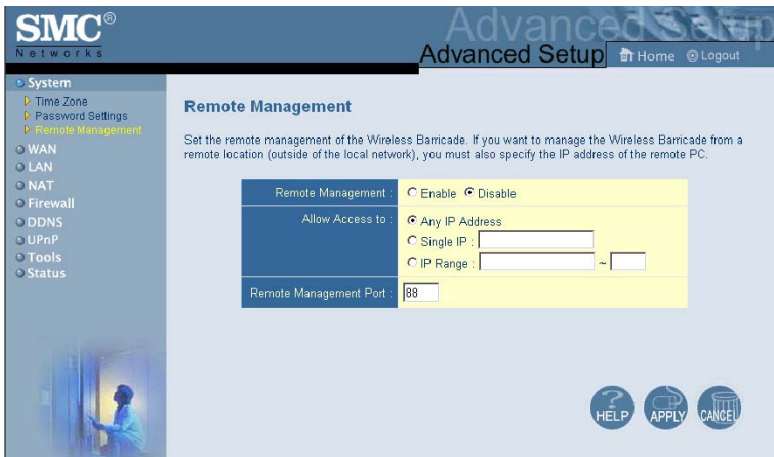
You can only remotely managed the Barricade™ from this IP address on the WAN side.

## [IP Range]

You can remotely manage the Barricade™ from any IP address in this range.

3. Set the Remote Management Port to the port through which you want to remotely access the Barricade™.

**Note:** Do not set this for a port that is already in use. For example, if you are running a web server on port 80, you can't set the remote admin port to 80.



## WAN

Specify the WAN connection type provided by your Internet Service Provider, then click [More Configuration] to enter detailed configuration parameters for the selected connection type.

- **[Dynamic IP]**

The Host Name is optional, but it may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Barricade™. Use this address when registering for Internet service, and do not change it unless required by your ISP. If your ISP used the MAC address of an Ethernet card as an identifier when first setting up your broadband account, connect only the PC with the registered MAC address to the Barricade™ and click the [Clone MAC Address] button. This will replace the current Barricade™ MAC address with the already registered Ethernet card MAC address.

If you are unsure of which PC did the broadband technician originally set up, call your ISP and request they register a new MAC address for your account. Register using the Barricade™'s MAC address.

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with options: System, WAN (selected), Dynamic IP (expanded), PPPoE, PPTP, Static IP, BigPond, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Dynamic IP" and contains the following text:

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

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

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

The configuration form includes:

- Host Name:
- MAC Address:
- Clone MAC Address:

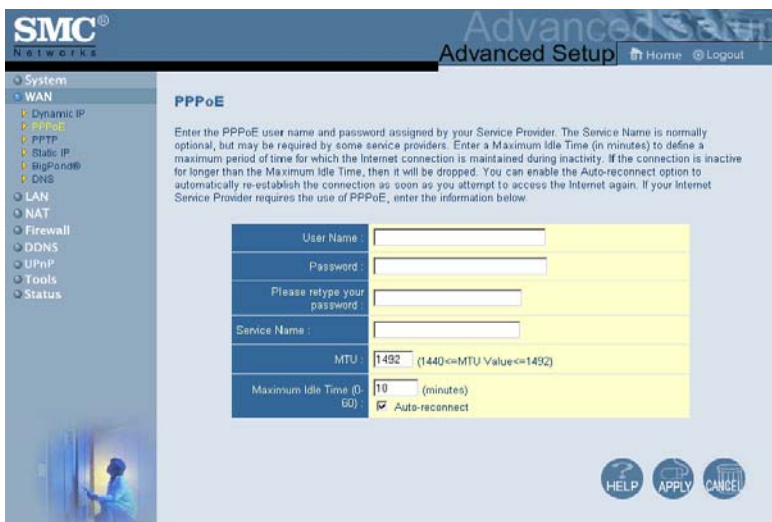
At the bottom right, there are three circular buttons: HELP, APPLY, and CANCEL. The top right of the interface shows "Advanced Setup" and navigation links for Home and Logout.

## Navigating the Web-based Administration

- **[PPPoE]**

Enter the PPPoE user name and password assigned by your Service Provider. The [Service Name] field is normally optional, but may be required by some service providers. The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1492) unless you have a particular reason to change it.

In [Maximum Idle Time (in minutes)] enter a value to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. Enable the [Auto-reconnect] option to automatically re-establish the connection when an application attempts to access the Internet again.



The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with options: System, WAN, Dynamic IP, PPPoE, PPTP, Static IP, BigPond®, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "PPPoE" and contains the following text: "Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet Service Provider requires the use of PPPoE, enter the information below."

User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Service Name :	<input type="text"/>
MTU :	1492 (1440<=MTU Value<=1492)
Maximum Idle Time (0-60) :	10 (minutes)
	<input checked="" type="checkbox"/> Auto-reconnect

At the bottom right of the form are three buttons: HELP, APPLY, and CANCEL.

- **[PPTP]**

Point-to-Point Tunneling Protocol (PPTP) allows the secure remote access over the Internet by simply dialing in a local point provided by an ISP. Using the above screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

**SMC<sup>®</sup>**  
NETWORKS

Advanced Setup | Home | Logout

**PPTP**

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

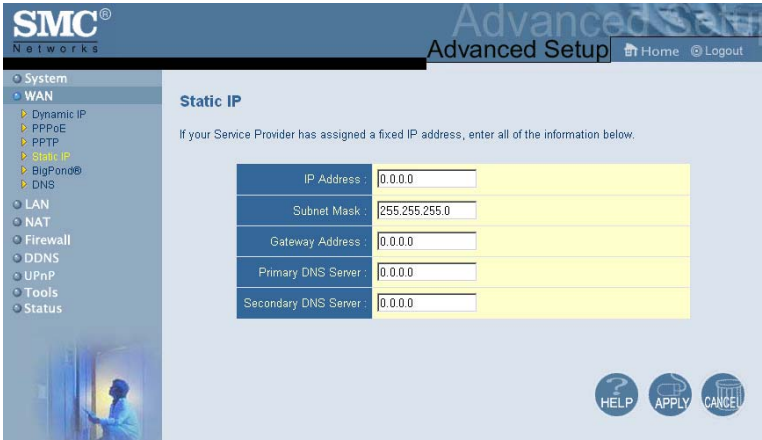
PPTP Account:	<input type="text"/>
PPTP Password:	<input type="password"/>
Please retype your password:	<input type="password"/>
Service IP Address:	<input type="text" value="0.0.0.0"/>
My IP Address:	<input type="text" value="0.0.0.0"/>
My Subnet Mask:	<input type="text" value="255.255.255.0"/>
Connection ID:	<input type="text"/>
MTU:	<input type="text" value="1492"/> (1400-1450)
Maximum Idle Time (0-80):	<input type="text" value="10"/> (minutes)
	<input checked="" type="checkbox"/> Auto-reconnect

HELP APPLY CANCEL

## Navigating the Web-based Administration

- **[Static IP Address]**

If your Internet Service Provider has assigned a fixed IP address to you, enter the assigned address and subnet mask for the Barricade™, and then enter the gateway address of your ISP. You may need a fixed address if you want to provide Internet services, such as a web server, or FTP server.



The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP (highlighted), BigPond®, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Static IP" and includes the instruction: "If your Service Provider has assigned a fixed IP address, enter all of the information below." Below this instruction is a table with five rows, each containing a label and a text input field with a yellow background. The rows are: IP Address (0.0.0.0), Subnet Mask (255.255.255.0), Gateway Address (0.0.0.0), Primary DNS Server (0.0.0.0), and Secondary DNS Server (0.0.0.0). At the bottom right of the main area are three circular buttons: HELP (with a question mark), APPLY (with a checkmark), and CANCEL (with a red X).

IP Address :	<input type="text" value="0.0.0.0"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>
Gateway Address :	<input type="text" value="0.0.0.0"/>
Primary DNS Server :	<input type="text" value="0.0.0.0"/>
Secondary DNS Server :	<input type="text" value="0.0.0.0"/>



- **[BigPond®]**

Use this section to configure the built-in client.

The screenshot shows the SMC Networks Advanced Setup interface. The top navigation bar includes the SMC Networks logo, the title "Advanced Setup", and links for "Home" and "Logout". A left-hand menu lists various system settings: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP, BigPond®, DNS, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "BigPond" and contains the following text: "In this section you can configure the built-in client for the BigPond Internet service available in Australia." Below this text is a configuration form with four rows of input fields:

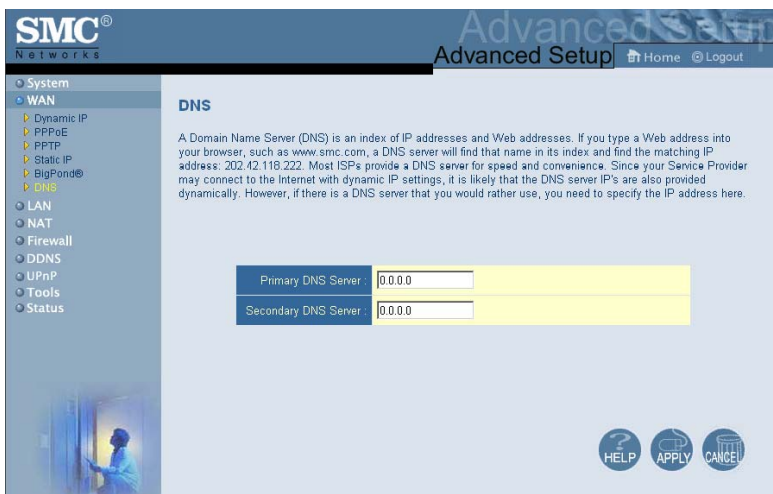
User Name :	<input type="text"/>
Password :	<input type="password"/>
Please retype your password :	<input type="password"/>
Authentication Service Name :	<input type="text"/> (optional)

At the bottom right of the main content area, there are three circular buttons: "HELP" (with a question mark icon), "APPLY" (with a checkmark icon), and "CANCEL" (with an 'X' icon).

## Navigating the Web-based Administration

- **[DNS]**

Domain Name Servers map numerical IP addresses to the equivalent domain name (e.g. [www.smc.com](http://www.smc.com) or [www.smc-europe.com](http://www.smc-europe.com)). Your ISP should provide the IP address of one or more domain name servers. Enter those addresses on this screen.



The screenshot shows the SMC Networks Advanced Setup web interface. The top navigation bar includes the SMC logo, the text "Advanced Setup", and links for "Home" and "Logout". A left-hand sidebar menu lists various system settings: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP, BigPond®, DNS (highlighted), LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "DNS" and contains a descriptive paragraph: "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: 202.42.118.222. 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." Below the text are two input fields: "Primary DNS Server" and "Secondary DNS Server", both containing the value "0.0.0.0". At the bottom right of the page are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

## LAN

From this section, you can configure the TCP/IP configuration for the Barricade™ LAN interface and DHCP clients.

- **LAN IP**

Use the [LAN] menu to configure the LAN IP address for the Barricade™ and to enable the DHCP server for dynamic client addresses allocation. Set a period for the lease time if required. For home networks, this may be set to "Forever", which means there is no time limit on the IP address lease.

- **IP Address Pool**

A dynamic IP start address may be specified by the user, e.g. 192.168.2.100 (default value). In this example, the IP addresses run from 192.168.2.100 to 192.168.2.199 which will be part of the dynamic IP address pool. IP addresses from 192.168.2.2 to 192.168.2.99, and 192.168.2.200 to 192.168.2.254 will be available as static IP addresses.

**Note:** Do not include the address of the Barricade™ in the DHCP client address pool.

The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with options: System, WAN, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "LAN Settings" and includes a descriptive paragraph: "You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Wireless Barricade must have an IP address for the local network." Below this are two configuration sections:

LAN IP Settings	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

DHCP Server Settings	
Lease Time	One Week
Start IP Address pool	192.168.2.100
End IP Address pool	192.168.2.199

At the bottom right of the interface are three buttons: HELP, APPLY, and CANCEL.

## Navigating the Web-based Administration

### NAT

From this section, you can configure the [Virtual Server] and [Special Application] features that provide control over the port openings in the router's firewall. This section can be used to support several Internet based applications such as VPN connections.

- **[Virtual Server]**

You can configure the Barricade™ as a virtual server. Remote users accessing services such as the Web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. To provide the most flexibility, the Barricade™ can support either a single port (80) or a range of ports (80-100). The traffic type can also be defined as TCP, UDP, or both (UDP and TCP).

Some of the more common ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

**Virtual Server**

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

Virtual Server services:

ID	IP Address	Ports	Data Type	Enable
1	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
2	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
3	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
4	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
5	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
6	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
7	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
8	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
9	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
10	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
11	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
12	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
13	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
14	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
15	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
16	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
17	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
18	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
19	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>
20	192.168.2.x	<input type="text"/>	TCP	<input type="checkbox"/>

- **[Special Applications]**

Some applications, such as Internet gaming, videoconferencing, Internet telephony require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use the following screen to specify the additional public ports to be opened for each application.

Specify the port or port range normally associated with an application in the [Trigger Port/s] field, select the protocol type as TCP or UDP, and then enter the public ports and data type associated with the trigger port to open them for inbound traffic.

The maximum range that you can use for all NAT ports is 0 to 65535.

**Special Applications**

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

Popular applications:

ID	Trigger Port/s	Trigger Type	Incoming Port/s	Data Type	Enable
1	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
2	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
3	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
4	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
5	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
6	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
7	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
8	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
9	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>
10	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="checkbox"/>

### **Firewall**

The firewall does not significantly affect system performance, so we advise enabling it to protect your network users. To enable the Stateful Packet Inspection (SPI) firewall, click on [Advanced] under the [Firewall] section and select [Enable] and click the [Apply] button.

The Barricade™ SPI firewall can provide the access control of connected client PCs, block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP Port Loopback, Snork Attack, TCP Null Scan, and TCP SYN Flooding.

- **[Parental Control:]**

Using this option allows you to specify different privileges for the client PCs. This is an excellent tool to control a child's access to specific content and/or general internet access for a specific time and/or date.

**To setup a Parental Control Rule:** Click on [Click here to configure a new Parental Control Rule] link. This will take you to the [Rule Setup] section.

Parental Control :  Enable  Disable

Create Rule : [Click here to configure a new Parental Control Rule](#)

Rule Description :

DHCP menu option :  Computer Name :  DHCP client list   
 Single IP : 192.168.2.  
 IP Range : 192.168.2. -

Schedule for Rule :  Rule is **Active** all the time  
 Set Time and Date Rule is **Active**

### Pre-Defined Blocking Options

Block	Block Information	Enable
..Any Internet Access	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<input type="checkbox"/>
..Specific Web Sites	<a href="#">Set Web Sites and Keywords you want to block</a>	<input type="checkbox"/>
..Secure Web Sites	HTTPS, TCP Port 443	<input type="checkbox"/>
..E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
..E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
..Newsgroup Access	NNTP, TCP Port 119	<input type="checkbox"/>
..FTP Access	FTP, TCP Port 20,21	<input type="checkbox"/>

### Custom Blocking Options

Block	Port Types	Enable
Ports: <input type="text"/> - <input type="text"/>	<input type="text"/> TCP <input type="button" value="v"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text"/> TCP <input type="button" value="v"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text"/> TCP <input type="button" value="v"/> Traffic	<input type="checkbox"/>
Ports: <input type="text"/> - <input type="text"/>	<input type="text"/> TCP <input type="button" value="v"/> Traffic	<input type="checkbox"/>

- **[Rule Description:]**

Set a rule description so you know what this rule applies to.  
 Ex. Jon's Internet Access.

- **[DHCP menu option:]**

Apply this rule to a specific IP Address or range of IP's on your network. You can use the DHCP client list to quickly add IP addresses that were provided via DHCP connections.

## Navigating the Web-based Administration

- **[Schedule for Rule:]**

Set the time and date this rule is active. You can have this rule be active all the time or configure it to only be active on set days and times.

You can pick the dates you want this rule to be active by checking the box next to the date.

For time, set the start time you want the Rule to active, and then set how long you want the rule to run.

Schedule for Rule :	<input type="radio"/> Rule is <b>Active</b> all the time <input checked="" type="radio"/> Set Time and Date Rule is <b>Active</b>
Rule is Active on :	<input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday
Rule Starts at :	<input type="text"/> : <input type="text"/> AM <input type="text"/>
Rule is Active for :	<input type="text"/> hours <input type="text"/> minutes

- **[MAC Filtering Table]**

The MAC Filtering feature of the Barricade™ allows you to control access to your network based on the MAC (Media Access Control) Address of the client machine. This ID is unique to each network adapter.

You can configure that MAC address to be allowed to access your network, or to deny access to the network.



This tool will also allow you to MAP DHCP IP Addresses to certain MAC Addresses. This tool works well in conjunction with the Parental Control rules to provide maximum control.

**MAC Filtering Table**

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

MAC Address Control:  Enable  Disable

DHCP Client List:

[Previous page](#) [Next page](#)

ID	Computer Name	IP Address	MAC Address	Allow	Deny
1	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	<input type="text"/>	192.168.2. <input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- **Website Blocking**

The [Website Blocking] feature of the Barricade™ limits access to website domains (i.e. www.somesite.com) or by using keywords which will block any websites that have that keyword in the URL. This feature is an ideal way to protect your family members from questionable content on the Internet.

**Website Blocking**

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

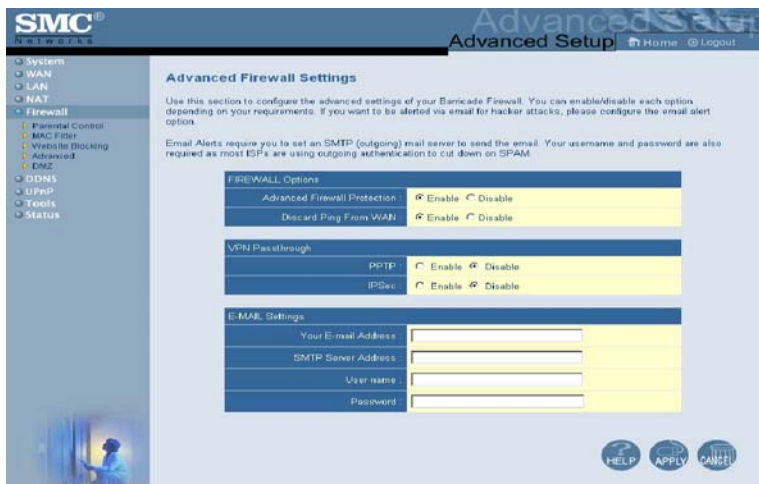
To specify the PC's that you want to block these websites to, go to the "Parental Control" page and check the box for "Block Specific Web Sites" in the "Pre-Defined Blocking Options" section.

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1	<input type="text"/>	Site 2	<input type="text"/>
Site 3	<input type="text"/>	Site 4	<input type="text"/>
Site 5	<input type="text"/>	Site 6	<input type="text"/>
Site 7	<input type="text"/>	Site 8	<input type="text"/>
Site 9	<input type="text"/>	Site 10	<input type="text"/>
Site 11	<input type="text"/>	Site 12	<input type="text"/>
Site 13	<input type="text"/>	Site 14	<input type="text"/>
Site 15	<input type="text"/>	Site 16	<input type="text"/>
Site 17	<input type="text"/>	Site 18	<input type="text"/>
Site 19	<input type="text"/>	Site 20	<input type="text"/>
Site 21	<input type="text"/>	Site 22	<input type="text"/>
Site 23	<input type="text"/>	Site 24	<input type="text"/>

## Navigating the Web-based Administration

- **[Advanced Firewall Settings]**

This section allows you to configure several advanced features for the Barricade™ Firewall.



The following features can be set on this page:

### **[Advanced Firewall Protection:]**

Enable/Disable SPI section of firewall.

### **[Discard Ping from WAN:]**

When this feature is enabled, any host on the WAN cannot ping this product. This helps avoid unnecessary attacks from the WAN side because your connection is invisible. It is recommended that you enable this option for security.

### **[VPN Pass-through:]**

Enable this option if you are using a PPTP, L2TP or IPSec VPN connection.

**[Email Settings:]**

Configure this option if you want the Barricade™ to email when hackers attempt to attack your network to a specific email address. You will need to configure your email address, username and password, as well as a SMTP server to send the mail through.

- **DMZ (Demilitarized Zone)**

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client PC up to unrestricted two-way Internet access. Enter the LAN IP address of a DMZ host and click [Enable].

**Note:** Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks. Only use this option as a last resort.

## **DDNS (Dynamic DNS)**

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

## Navigating the Web-based Administration

The section also has a [Server Configuration] section that automatically opens the port options checked in the [Virtual Server] section. Simply enter in the IP address of your server, such as a web server, and then click on the port option [HTTP Port 80] so users can access your server from the WAN connection (Internet).



The screenshot displays the 'Advanced Setup' page for SMC Barricade. The left sidebar contains a navigation menu with options: System, WAN, LAN, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'DDNS (Dynamic DNS) Settings'. Below the title, there is a descriptive paragraph: 'Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.' The configuration section includes a 'Dynamic DNS' toggle set to 'Enable'. Under 'Service Configuration', there is a dropdown menu for 'DDNS Service' (set to 'DynDNS.org(Dynamic)'), and input fields for 'Domain Name', 'Username / E-mail', and 'Password / Key'. The 'Server Configuration' section shows a 'Server IP' field with '192.168.2' and a 'Server Type' section with checkboxes for 'Web Server: (HTTP) Port 80', 'Port 8000', 'FTP Server: Port 20', 'Port 21', and 'Email Server:(POP3) Port 110 (SMTP) Port 25'. At the bottom right, there are 'HELP', 'APPLY', and 'CANCEL' buttons.

## UPnP

The Barricade™ supports UPnP (Universal Plug and Play), a networking architecture that provides compatibility amongst networking equipment. This feature allows an UPnP based operating system, like Windows XP to automatically communicate with the Barricade™ and open the required services when needed.

## Tools

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

- **[Configuration Tools]**

**[Backup Router Settings]**

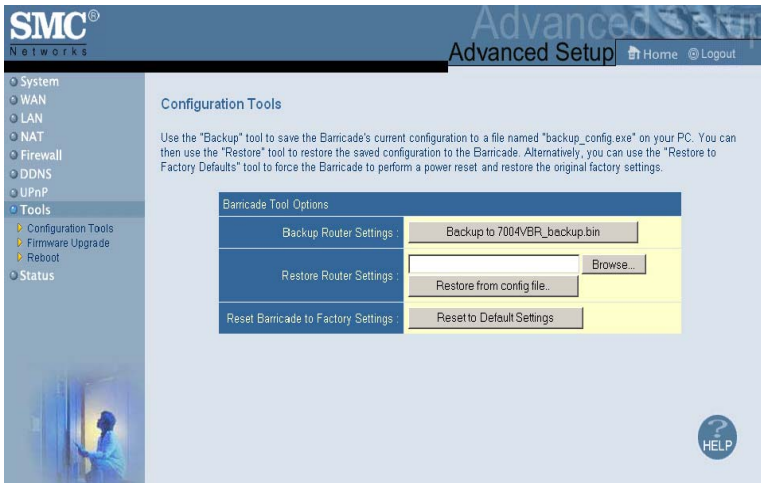
Backup saves the Barricade™'s configuration to a file.

**[Restore Router Settings]**

To restore settings from a saved backup configuration file.

**[Reset Barricade to Factory Settings]**

Restores the Barricade™ settings back to the factory default settings.



## *Navigating the Web-based Administration*

- **Firmware Upgrade**

This tool permits easy downloading of the latest Firmware. Download the upgrade file from the SMC website ([www.smc.com](http://www.smc.com) or [www.smc-europe.com](http://www.smc-europe.com)) and save it to your hard drive. Browse for the file and then click [Apply]. Check the [Status page Information] section to confirm that the upgrade process was successful.

- **Reboot**

Click [Apply] to reboot the Barricade™. The reset will be complete when the power LED stops blinking.

**Note:** Some options, when enabled, will require you to reboot the router. You can use this option to perform that function.

## **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 following items are included on this screen:

- **[INTERNET]**

Displays WAN connection type and status.

- **[GATEWAY]**

Displays system IP settings, as well as DHCP and Firewall status.

- **[INFORMATION]**

Displays the number of attached clients, the firmware versions, and the physical MAC address for each media interface, as well as the hardware version and serial number.

- **[Security Log]**

Displays illegal attempts to access your network.

- Click on the [Save] button to save a security log file.
- Click on the [Clear] button to delete the access log.
- Click on the [Refresh] button to refresh the screen.

- **[DHCP Client Log]**

Displays information on all DHCP clients on your network.

For additional information on the 7004VBR, please visit [www.smc.com](http://www.smc.com) or [www.smc-europe.com](http://www.smc-europe.com).

# TROUBLESHOOTING

The information outlined in this section describes some useful steps for getting your computer and Barricade™ router online.

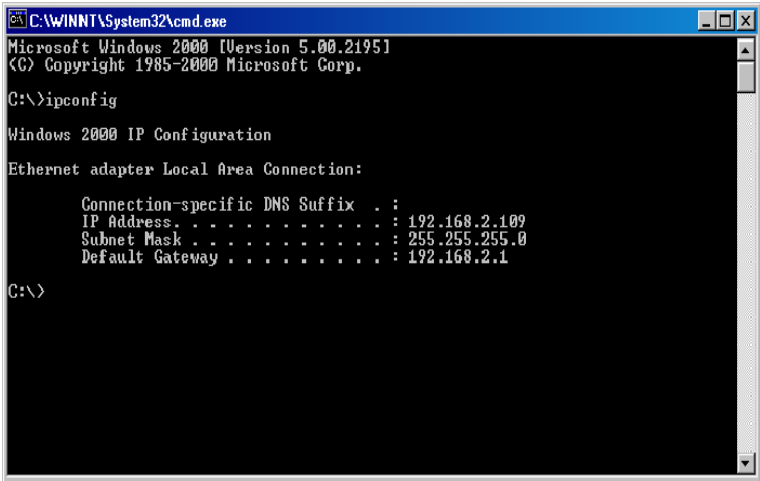
## Verify you are connected to the Barricade™ Router

If you are unable to access the Barricade™'s web-based administration pages, then you may not be properly connected or configured. The screen shots in this section were taken on a Windows 2000 machine, but the same steps will apply to Windows 95/98/Me/XP.

To determine your TCP/IP configuration status, please follow the steps below:

1. Click [Start] then choose [Run].
2. Type cmd or command to open a DOS prompt.
3. In the DOS window, type ipconfig and verify the information that is displayed.
4. If your computer is setup for DHCP, then your TCP/IP configuration should be similar to the information displayed:
  - [IP Address]: 192.168.2.X  
(x is number between 100 and 199)
  - [Subnet]: 255.255.255.0
  - [Gateway]: 192.168.2.1





If you have an IP address that starts with 169.254.XXX.XXX then see section “I am getting an IP Address that starts with 169.254.XXX.XXX”.

If you have another IP address configured, see section “I have another IP Address displayed”.

## **I am getting an IP Address that starts with 169.254.XXX.XXX**

If you are getting this IP Address, then you need to check that you are properly connected to the Barricade™ Router.

Confirm that you have a good link light on the Barricade™'s port to which this computer is connected. If not, please try another cable.

If you have a good link light, please open up a DOS window as described in section “Verify you are connected to the Barricade™ Router” and type ipconfig/renew.

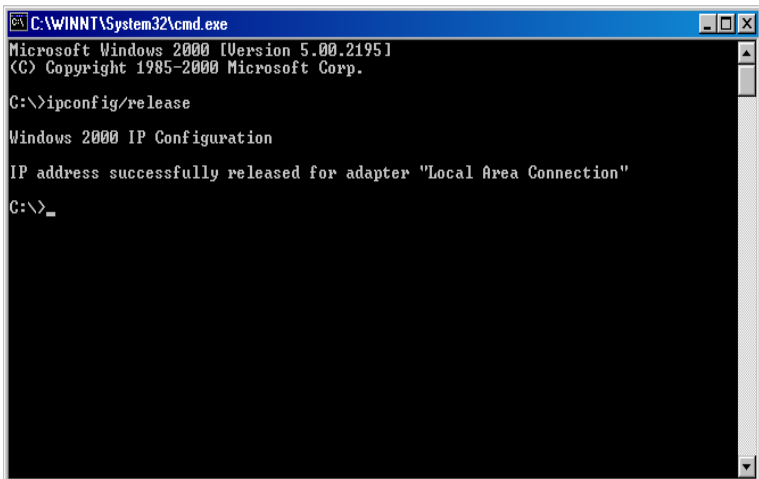
If you are still unable to get an IP Address from the Barricade™, reinstall your network adapter. Please refer to your adapter manual for instructions.

## I have another IP Address displayed

If you have another IP address listed, then the PC may not be configured for a DHCP connection. Please refer to Configuring your Computer for information.

Once you have confirmed your computer is configured for DHCP, then please follow the steps below.

1. Open a DOS window as described above.
2. Type ipconfig/release.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig/release

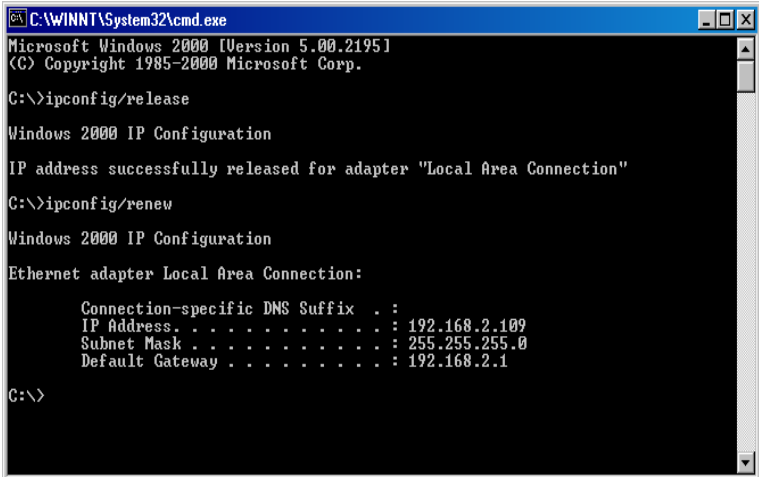
Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>_
```

## Troubleshooting

3. Then type `ipconfig/renew`.



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 192.168.2.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\>
```

Once you are able to get a valid IP address from the Barricade™ Router, then you can now access the web-based Administration pages.

If you still are not getting an IP address from the Barricade™, please reset the router as outlined in Getting to Know the Barricade™ and follow the steps outlined in Troubleshooting section again.

If you still cannot access the router once you have reset it, please contact SMC Technical Support.

## **I have a Dynamic IP connection and I can't get online**

Most cable companies use a Dynamic IP configuration to provide Internet access. If you have this type of connection, and are unable to get connected, please follow the steps outlined below:

1. Unplug the power from your Cable or DSL modem for 2 mins.
2. Confirm that your Barricade™ router is configured for a Dynamic IP configuration.
3. Plug the power back into your Modem.
4. Wait for your Modem to connect to the network, and then click on the status page of the router to confirm that you are online.

The reason this process works is because certain broadband connections require a MAC address to gain network access. This MAC address can be changed by following the above process to re-set the approved MAC address to the MAC address of the Barricade™ router.

# TECHNICAL SPECIFICATIONS

Below is an outline of the Technical Specifications for the Barricade™ 4-Port Cable/DSL Broadband Router.

## **Standards**

802.3, 802.3u

## **WAN Port**

1 - 10/100Mbps RJ45, with Auto MDI/MDIX

## **LAN Port**

4 - 10/100Mbps RJ45, with Auto MDI/MDIX

## **Supported WAN type**

Static IP

Dynamic IP

PPP over Ethernet

PPTP

Big Pond

## **NAT**

Maximum 253 Users

## **Protocol**

IP Protocol

TCP/IP v4

DHCP server

Proxy DNS server

## **Management and Configuration**

Web-based

## **Firewall**

NAT firewall and SPI firewall

## **VPN**

VPN pass-through including PPTP/L2TP/IPsec

## *Technical Specifications*

### **User Authentication**

Password protected browser-based UI PAP/CHAP/MSCHAP  
Authentication protocol supported

### **Upgrade method**

Web-based

### **LEDs**

Power

WAN

Link

Activity

### **Input Power**

DC 5V 2A

### **Operating Temperature**

0°~40°C

### **Humidity**

10%~90% non-condensing

### **Storage Temperature**

-200~700C

### **Humidity**

0~95% non-condensing

### **Compliance**

FCC

CE

UL

### **Dimensions**

13.2 x 8.7 x 3.3 cm

### **Weight**

200g

# COMPLIANCES

## **FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

## **Industry Canada – Class B**

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus" ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe B prescrites dans la norme sur le matériel brouilleur: « Appareils Numériques » NMB-003 édictée par le ministère des Communications.

## **EC Conformance Declaration – Class B**

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.

This product complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

# COMPLIANCES

## Emission:

EN 5022: 1998+A1:2000

EN 61000-3-2: 2000, EN 61000-3-3: 1995+A1:2000

## Immunity

EN 55024:1998+A1:2001,

EN 61000-4-2, 61000-4-3, 61000-4-4, 61000-4-5

EN 61000-4-6, 61000-4-11

## Safety Test:

EN 60950

## **Safety Compliance**

### **Wichtige Sicherheitshinweise (Germany)**

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschlußsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Beschädigungen hervorrufen.
7. Die Belüftungsöffnungen dienen der Luftzirkulation, die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
9. Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen, die sich am Gerät befinden, sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.



14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  - a. Netzkabel oder Netzstecker sind beschädigt.
  - b. Flüssigkeit ist in das Gerät eingedrungen.
  - c. Das Gerät war Feuchtigkeit ausgesetzt.
  - d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  - e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  - f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der EN60950 geprüft ist. Ausgangswerte der Stromversorgung sollten die Werte von AC 7,5-8V, 50-60Hz nicht über- oder unterschreiten sowie den minimalen Strom von 1A nicht unterschreiten. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weniger.

# LEGAL INFORMATION AND CONTACTS

## **SMC's Limited Warranty Statement**

SMC Networks Europe ("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 2 year 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 endeavour to repair or replace any product returned under warranty within 30 days of receipt of the product. 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.

The standard limited warranty can be upgraded to a 5 year 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 a period of 5 years from the date of purchase of the product from SMC or its authorized reseller.

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. 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 A 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**

## LEGAL INFORMATION AND CONTACTS

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

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

SOME COUNTRIES 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 COUNTRY TO COUNTRY. NOTHING IN THIS WARRANTY SHALL BE TAKEN TO AFFECT YOUR STATUTORY RIGHTS.

\* 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.

### **Full Installation Manual**

Full installation manuals are provided on the Installation CD-Rom. Manuals in other languages than those included on the CD-Rom are provided on [www.smc-europe.com](http://www.smc-europe.com) (section support).

### **Firmware and Drivers**

For latest driver, technical information and bug-fixes please visit [www.smc-europe.com](http://www.smc-europe.com) (section support).

### **Contact SMC**

Contact details for your relevant countries are available on [www.smc-europe.com](http://www.smc-europe.com) and [www.smc.com](http://www.smc.com).

### **Statement of Conditions**

In line with our continued efforts to improve internal design, operational function, and/or reliability, SMC reserves the right to make changes to the product(s) described in this document without notice. SMC does not assume any liability that may occur due to the use or application of the product(s) described herein. In order to obtain the most accurate knowledge of installation, bug-fixes and other product related information we advise to visit the relevant product support page at [www.smc-europe.com](http://www.smc-europe.com) before you start installing the equipment. All information is subject to change without notice.

### **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.

### **Copyright**

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC 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 SMC. SMC reserves the right to change specifications at any time without notice.

### **Trademarks**

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

