SMC Networks

SMC7004VBR Barricade™ Cable/DSL Broadband Router

USER GUIDE

Copyright

Trademarks

Compliances

FCC - Class B
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that the interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
• Reorient the receiving antenna
• Increase the separation between the equipment and receiver
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
• Consult the dealer or an experienced radio/TV technician for help

FCC Caution: To assure continued compliance, (for example - use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION STATEMENT:

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 5 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Note: In order to maintain compliance with the limits of a Class B digital device, SMC requires that you use a quality interface cable when connecting to this device. Changes or modifications not expressly approved by SMC could void the user's authority to operate this equipment. Attach unshielded twisted-pair cable (UTP) to the RJ-45 port and shielded USB cable to the USB port.

EC Conformance Declaration – Class B

SMC contact for these products in Europe is:

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

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

Important Safety Notices

- Unplug this product from the AC power before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a dry cloth for cleaning.
- Route the power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords at plugs, convenience receptacles, and the point where they exit from the product.
- Situate the product away from heat sources such as radiators, heat registers, stoves, and other products that produce heat.
- To prevent fire or shock hazard, do not expose this unit to rain or moisture. Do not allow water or any foreign objects to enter the interior. This may cause a fire or electric shock. In the event that water or other foreign objects get into the product, immediately unplug the AC adapter from the electrical outlet and contact Customer Service for inspection and/or repair/replacement options.
- Do not take apart the equipment. This may cause fire, electric shock or other injuries.
- Do not overload wall outlets and extension cords as this can result in a fire or electric shock.
- This product is for use with the AC adapter that comes with it. Use with any other AC power is strongly discouraged as it may cause fire, electric shock, or damage to the equipment.

TABLE OF CONTENTS

1 | System Requirements

- Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem, cable modem, Dial-Up modem, or ISDN modem
- A PC using a fixed IP address or dynamic IP address assigned via DHCP, as well as a Gateway server address and DNS server address from your service provider
- A computer equipped with a 10 Mbps, 100 Mbps, or 10/100 Mbps Fast Ethernet card, or a USB-to-Ethernet converter
- TCP/IP network protocol installed on each PC that needs to access the internet
- A Java-enabled web browser, such as Microsoft Internet Explorer 5.0 or above, or Netscape Communicator 4.0 or above installed on one PC at your site for configuring the router.

2 | Equipment Checklist

After unpacking the Barricade™ Cable/DSL Broadband Router, check the contents of the box to be sure you have received the following components:

- 1 Barricade™ Cable/DSL Broadband Router
- 1 EZ Installation Wizard and Documentation CD
- 1 Ethernet (CAT5-UTP/Straight-Through) Cable
- 1 Power Adapter
- 1 Quick Installation Guide

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.

Please register this product and upgrade the product warranty at SMC's Web site:
http://www.smc.com

3 | Functions and Features

Broadband Modem and NAT Router	Connects multiple computers to a broadband (cable or DSL) modem, and/or Ethernet router to access the Internet.
10/100 Mbps Ethernet Interface	Provides a 10/100 Base-TX interface to connect to a DSL or cable modem for broadband Internet access.
Auto-sensing Ethernet Switch	Equipped with a 4-port auto-sensing Ethernet switch.
WAN type supported	The router supports some WAN types, Static, Dynamic, PPPOE, PPTP, and Dynamic IP with Road Runner.
Firewall	All unwanted packets from outside sources are blocked to protect your intranet.
DHCP Server Supported	All networked computers can retrieve TCP/IP settings automatically from this device.
Web-based Configuration	Configurable by any networked computer's Web browser using Netscape or Internet Explorer.
Network Filter Supported	The Packet Filter lets you control access to a network by analyzing the incoming and outgoing packets; this lets you either pass or halt the packets based on the IP address or the source and destination.
Universal Plug and Play (UPnP) Supported	Enables devices such as PCs, routers and printers to be plugged into a network and ensure automatic recognition.
Virtual Server Supported	Lets you make your Website, FTP site, and other services on your LAN accessible to Internet users.
User Defined Application Sensing Tunnel	Lets you define the attributes to support special applications that require multiple connections like Internet gaming, video conferencing, Internet telephony, and so on. This device can sense the application type and opens a multi-port tunnel for it.
DMZ Host Supported	Enables a computer to be fully accessible to the Internet. This function is used when the special application sensing tunnel feature is insufficient to allow an application to function correctly.
SNMP Supported	SNMP (Simple Network Management Protocol) is a protocol that lets users remotely manage a computer network by polling and setting terminal values, and monitoring network events.
System Time Supported	Lets you synchronize system time with the network time server.
Virtual Computers Supported	The virtual computer lets you use the original NAT feature, which lets you setup the one-to-one mapping of multiple global and local IP addresses.
URL Blocking Supported	Lets you block hundreds of Website connections by simply entering a keyword.
Schedule Rule	Lets you set a time schedule for different services.
Routing Table Supported	Allows you to determine which physical interface address to use for outgoing IP data grams. If you have more than one router and subnet, enable the routing table to allow packets to find the proper routing path and the different subnets to communicate with each other.

4 | Panel Layout

The following figure shows the front panel layout, which is followed by a table describing in detail the status and function of each LED.

SMC7004VBR

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

5 | Hardware Installation

The router can be placed anywhere in your office or home. No special wiring or cooling requirements are necessary. However, you should comply with the following guidelines:

- Place your router on a flat, horizontal surface
- Be sure to place your router away from any heating devices
- Avoid dusty and/or humid areas

1) **Setup LAN Connection:** Connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of the router.
2) **Setup WAN Connection:** Insert one end of the Ethernet cable into the WAN port on the back panel of your router, and the other end to the cable/DSL modem. You may connect an analog modem (optional) to function as a backup connection.
3) **Power Up:** The router automatically enters the self-testing phase once the power cord is plugged into a wall outlet. When in self-testing phase, the M1 indicator LED illuminates for about five seconds to indicate proper connection. The M1 LED flashes twice as soon as the self-testing phase is completed. After the completion of the self-testing phase, the M1 LED should flash once per second to indicate that the router is functioning properly.

6 | Network Settings and Software Installation

Default Settings	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Administrator Password	smcadmin

You must first verify that the TCP/IP communication protocol is properly installed and the computer is configured to get its IP address via the DHCP Server that is built-into this router. If you have not previously installed TCP/IP protocols on your client PCs, refer to the following section.

6.1 Installing TCP/IP

Windows 95/98/Me

1. Click Start/Settings/Control Panel.
2. Double-click the Network icon and select the Configuration tab in the Network window.
3. Click the Add button.
4. Double-click Protocol.
5. Select Microsoft in the manufacturers list. Select TCP/IP in the Network Protocols list. Click the OK button to return to the Network window.
6. The TCP/IP protocol will be listed in the Network window
7. Click OK. The operating system may prompt you to restart your system. Click "Yes" and the computer will shut down and restart.

Windows 2000/XP

1. Click the Start button and choose Settings, then click the Network and Dial-up Connections icon.
2. Double-click the Local Area Connection icon, and click the Properties button on the General tab.
3. Click the install button.
4. Double-click Protocol.
5. Choose Internet Protocol (TCP/IP). Click the OK button to return to the Network window.
6. The TCP/IP protocol will be listed in the Network window. Click OK to complete the installation procedure.

6.2 | Setting up TCP/IP

Windows 95/98/Me

You may find that the instructions here do not exactly match your version of Windows. This is because these steps and screenshots were created in Windows 98. Windows 95 and Windows Millennium Edition are very similar, but not identical, to Windows 98.

1. From the Windows desktop, click Start/Settings/Control Panel.
2. In the Control Panel, locate and double-click the Network icon.
3. On the Network window Configuration tab, double-click the TCP/IP entry for your network card.
4. Click the IP Address tab.
5. Click the "Obtain an IP address" 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 window.
8. On the Network Properties Window, click the OK button to save these new settings. 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 CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x. (If D: is the letter of 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 to insure your settings.

Windows NT

1. From the Windows desktop click Start/Settings/Control Panel.
2. Double-click the Network icon.
3. Click on the Protocols tab.
4. Double-click TCP/IP Protocol.
5. Click on the IP Address tab.
6. In the Adapter drop-down list, be sure your Ethernet adapter is selected.
7. Click on "Obtain an IP address from a DHCP server."
8. Click OK to close the window.
9. Windows may copy files and will then prompt you to restart your system. Click Yes and your computer will shut down and restart.

Windows 2000/XP

1. Access your Network settings by clicking Start, then choose Settings and then select Control Panel.
2. In the Control Panel, locate and double-click the Network and Dial-up Connections icon.
3. Locate and double-click the Local Area Connection icon for the Ethernet adapter that is connected to the Router. When the Status dialog box window opens, click the Properties button.
4. In 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.

6.3 | Obtaining an IP Address

Windows 95/98/Me

1. Click Start/Run.
2. Type WINIPCFG and click OK.
3. From the drop-down menu, select your network card. Click Release and then Renew. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168. 2.1. These values confirm that the Router is functioning. Click OK to close the IP Configuration window

Windows 2000/XP

1. On the Windows desktop, click Start/Programs/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 192.168.2.254. These values confirm that the Router is functioning
4. Type EXIT and press <ENTER> to close the Command Prompt window.

6.4 | Configuring a Macintosh Computer

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

1. Pull down the Apple Menu. Click System Preferences and select Network.
2. Make sure that Built-in Ethernet is selected in the Show field.
3. On the TCP/IP tab, select Using DHCP in the Configure field.
4. Close the TCP/IP dialog box.

6.5 | Verifying Your TCP/IP Connection

After installing the TCP/IP communication protocols and configuring an IP address in the same network as the Router, use the ping command to check if your computer has successfully connected to the Router. The following example shows how the ping procedure can be executed in an MS-DOS window. First, execute the ping command:

Ping 192.168.2.1

If a message similar to the following appears:

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=2ms TTL=64

…a communication link between your computer and the Router has been successfully established.

If you get the following message:

Pinging 192.168.2.1 with 32 bytes of data: Request timed out.

…there may be something wrong in your installation procedure.

Check the following items in sequence:

1. Is the Ethernet cable correctly connected between the Router and the computer? The LAN LED on the Router and the Link LED of the network card on your computer must be on.
2. Is TCP/IP properly configured on your computer? If the IP address of the Router is 192.168.2.1, the IP address of your PC must be from 192.168.2.2 - 254 and the default gateway must be 192.168.2.1. If you can successfully ping the Router you are now ready to connect to the Internet!

7 | Configuring Your Broadband Router

Before you attempt to log into the 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 Router. If you don't have a link light, then try another cable until you get a good link.

7.1 | 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.

You will also need to verify that the HTTP Proxy feature of your web browser is disabled. This is so that your web browser will be able to view the Router 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 (For Windows)

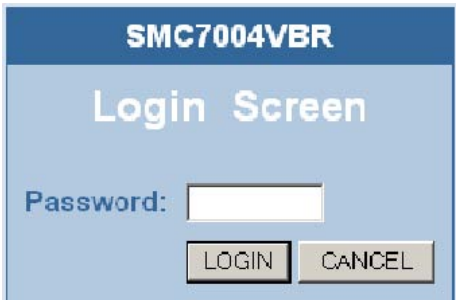
1. Open Internet Explorer. Click Tools, and then select Internet Options.
2. In the Internet Options window, click the Connections tab.
3. Click the LAN Settings button.
4. Clear all the check boxes and click OK to save these LAN settings changes.
5. Click OK again to close the Internet Options window.

Internet Explorer (For Macintosh)

1. Open Internet Explorer. Click Explorer/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.
3. Uncheck all check boxes and click OK.

7.2 | Web Management

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



To log in to the management, enter the system default password "**smcadmin**" and click the **LOGIN** button. If you typed the password correctly, the left panel of the Web user interface changes to the administrator configuration mode as shown in the following figures.

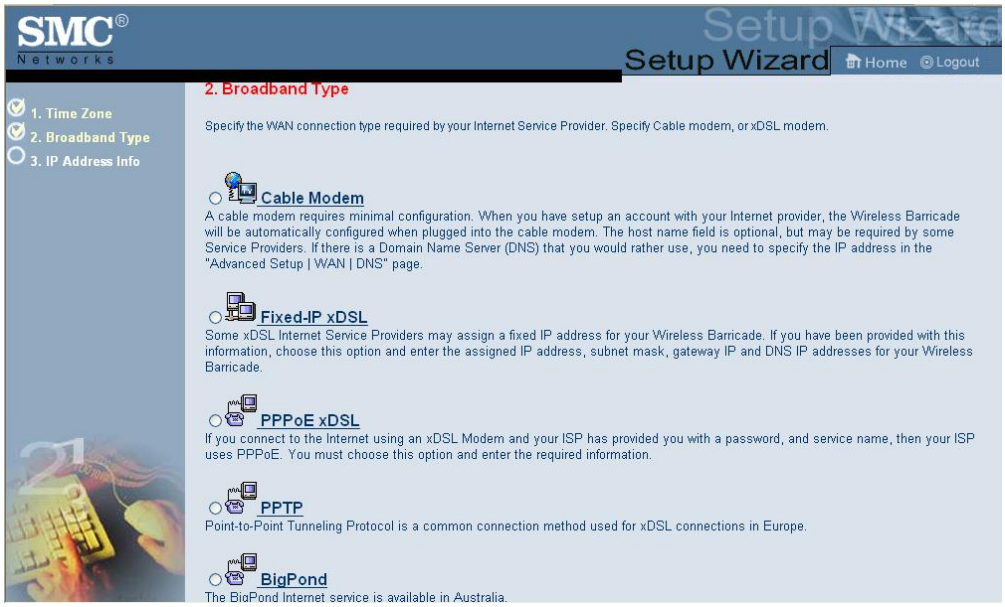
7.3 | Setup Wizard

7.3.1 Time Zone

After logging into the web management, click on SETUP WIZARD on the top left navigation panel. The first item is Time Zone. For accurate timing of client filtering and log events, you need to set the time zone. Select your time zone from the drop-down list.

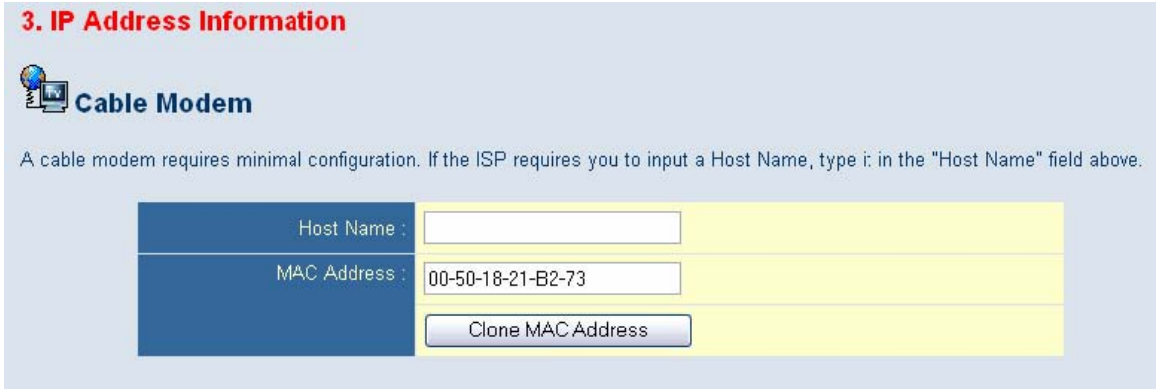
7.3.2 Broadband Type

The following screen lets you select a WAN type. Click one of the options and then click [Next].



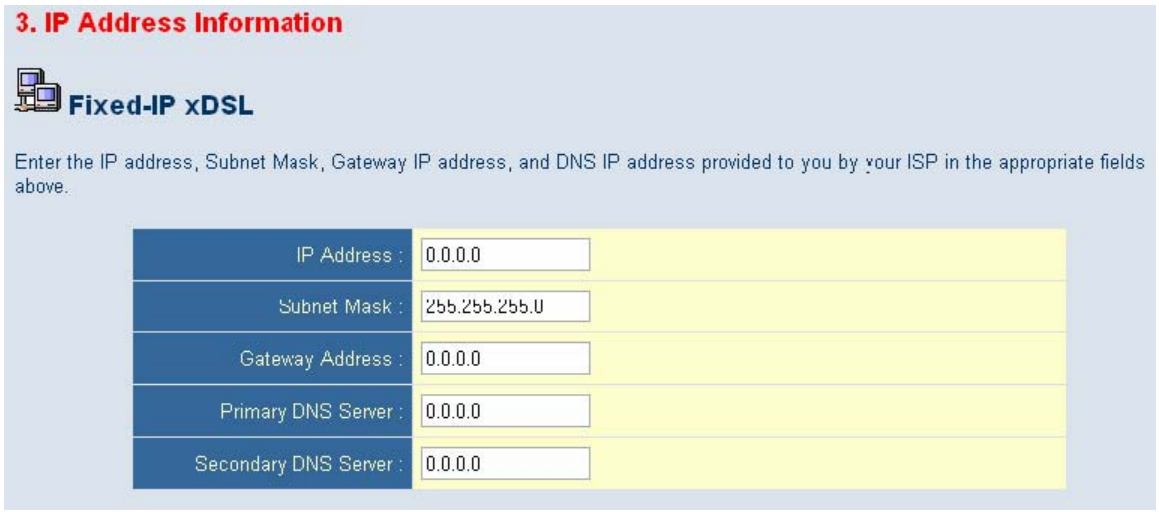
7.3.4 Cable Modem

The cable modem option allows you to configure a host name and MAC Address. The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Router. 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, only connect the PC with the registered MAC address to the Router and click the Clone MAC Address button. This will replace the current Router MAC address with the already registered Ethernet card MAC address. If you are unsure of which PC was originally set up by the broadband technician, call your ISP and request that they register a new MAC address for your account. Register the default MAC address of the Router.



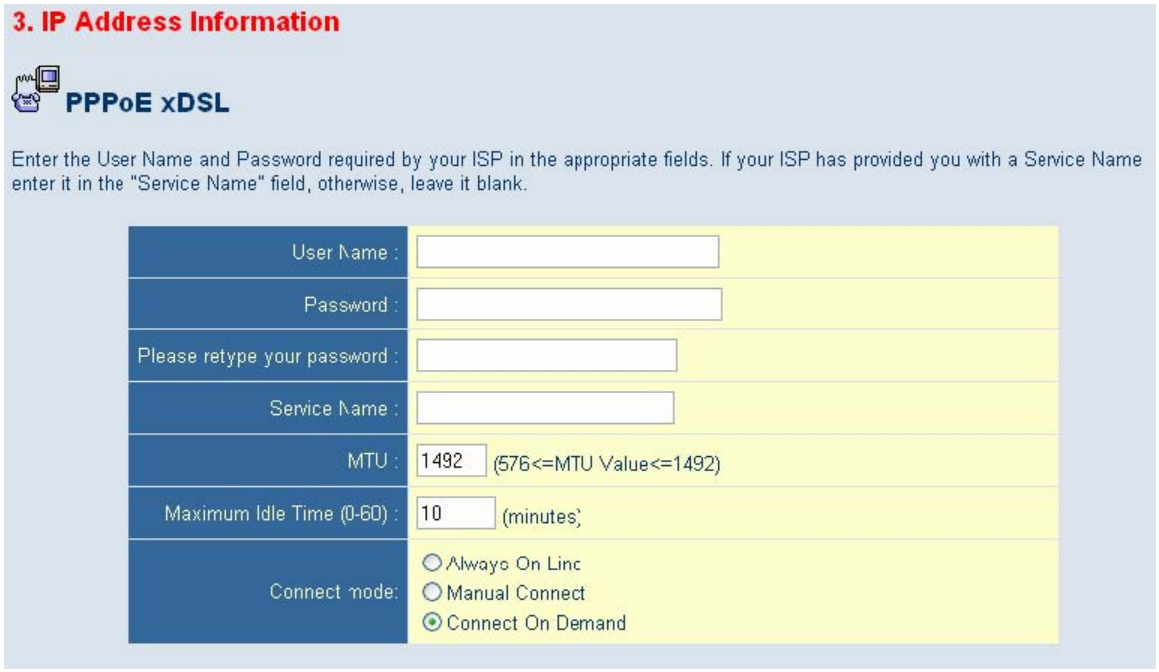
7.3.5 Fixed-IP xDSL

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



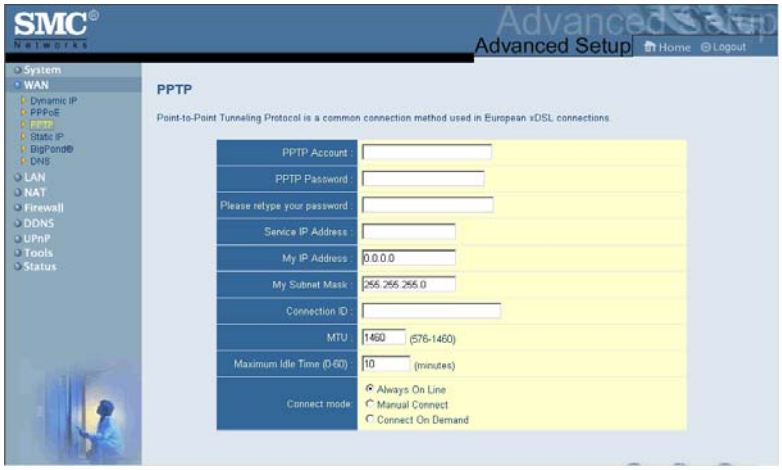
7.3.6 PPPoE xDSL

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) at the default value 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. (Default: 10) Configure the Connect mode option to the desired settings. “Always On Line” signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. “Manual Connect” signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the “Connect” button. While using the “Connect On Demand” option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.



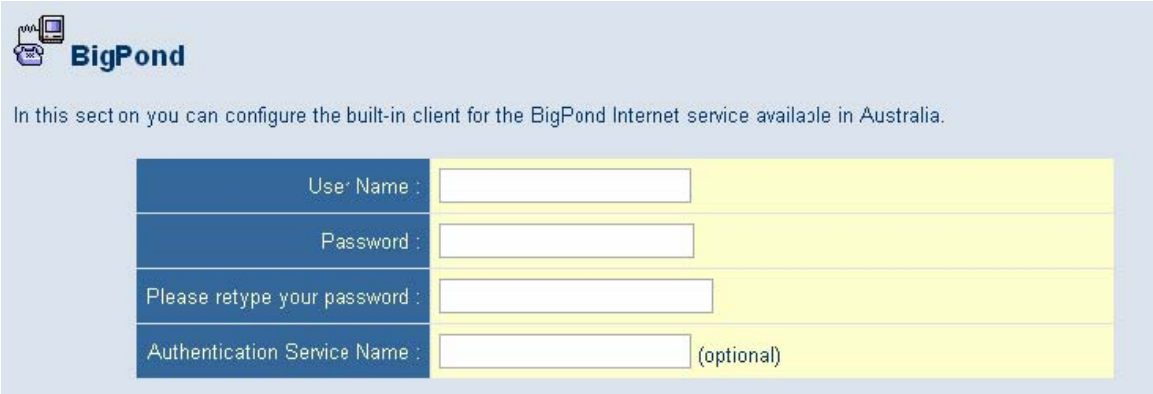
7.3.7 PPTP

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary. If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and PPTP Gateway. Configure the Connect mode option to the desired settings. “Always On Line” signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. “Manual Connect” signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the “Connect” button. While using the “Connect On Demand” option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.



7.3.8 BigPond

If you use the BigPond Internet Service which is available in Australia, enter your username and password and apply the changes.

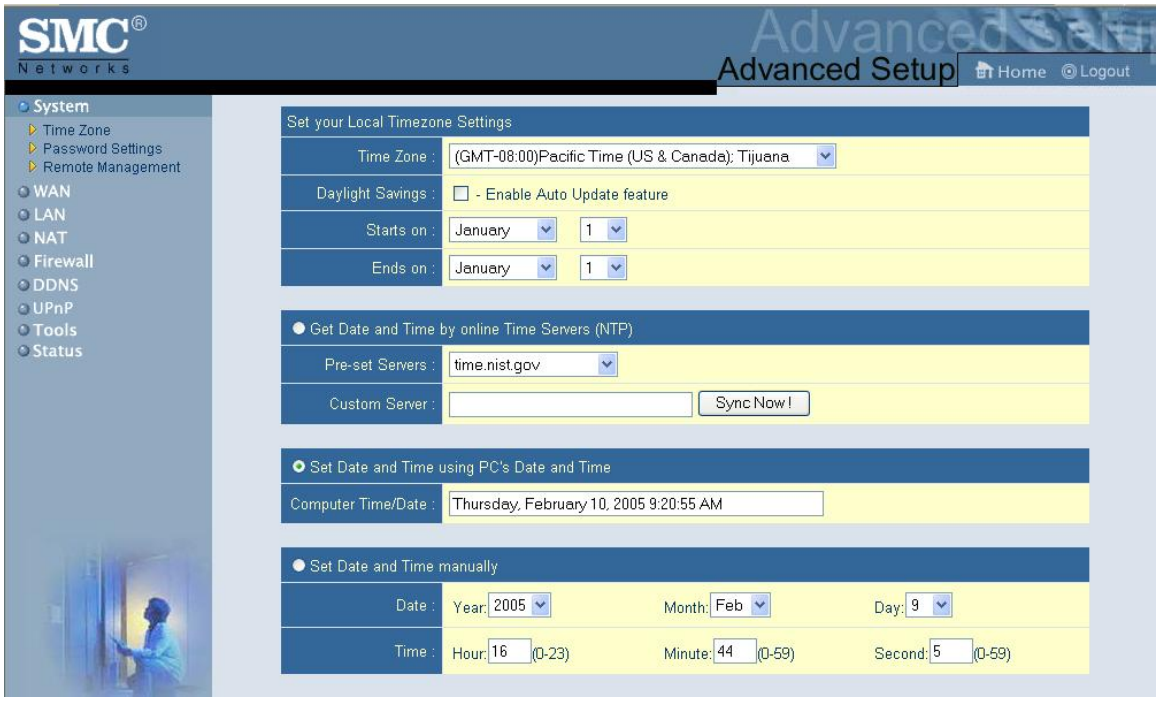


7.4 | Advanced Setup – SYSTEM

7.4.1 Time Zone

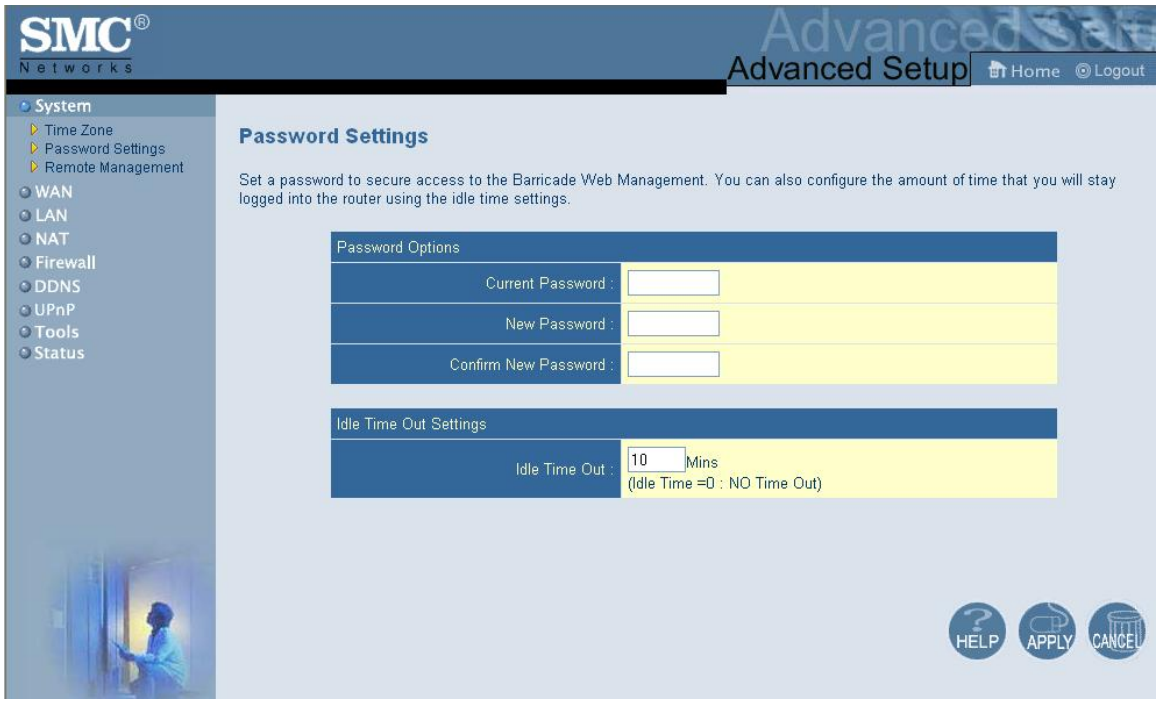
Use the section below to configure the Barricade's system time. Select your timezone and configure the daylight savings option based on your location. This information is used for the time/date parental rules you can configure with the Barricade's Advanced Firewall. This information is also used for your network logging.

Once you set you time zone, you can automatically update the Barricade's internal clock by synchronizing with a public time server over the Internet. To configure this setting, choose one of the options below - each option allows a different method of updating.



7.4.2 Password Settings

Use this section to configure the password and idle time-out setting for your Barricade Router. The default password for this router is "smcadmin".



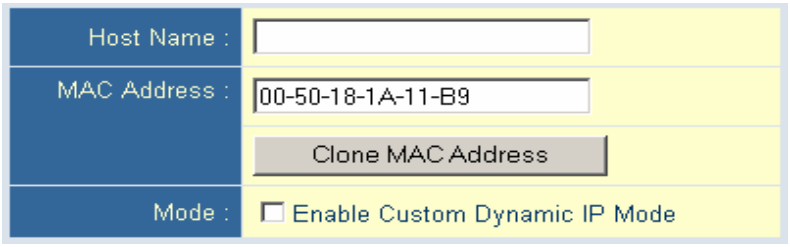
7.4.3 Remote Management

Use this section to configure the remote management feature of your Barricade Router so the web-management can be accessed from the Internet (WAN). You can restrict access to a single IP or a range of IP addresses. If the specified IP address is 0.0.0.0, any host can connect to the router to perform these tasks. You can use the subnet mask bits' /nn notation to specify a group of trusted IP addresses. For example, 10.1.2.0/24. You can also change the remote port that the administrator uses to gain access to the web management.

7.5 | Advanced Setup - WAN

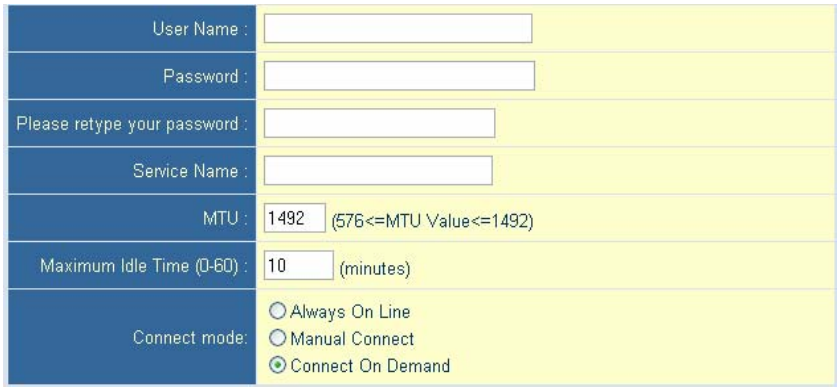
7.5.1 Dynamic IP

The cable modem option allows you to configure a host name and MAC Address. The Host Name is optional, but may be required by some ISPs. The default MAC address is set to the WAN's physical interface on the Router. 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, only connect the PC with the registered MAC address to the Router and click the Clone MAC Address button. This will replace the current Router MAC address with the already registered Ethernet card MAC address. If you are unsure of which PC was originally set up by the broadband technician, call your ISP and request that they register a new MAC address for your account. Register the default MAC address of the Router.



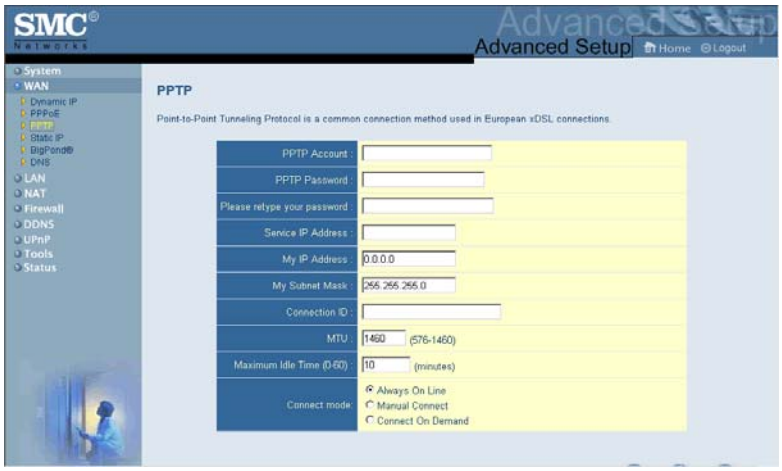
7.5.2 PPPoE

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) at the default value 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. (Default: 10) Configure the Connect mode option to the desired settings. "Always On Line" signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. "Manual Connect" signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the "Connect" button. While using the "Connect On Demand" option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.



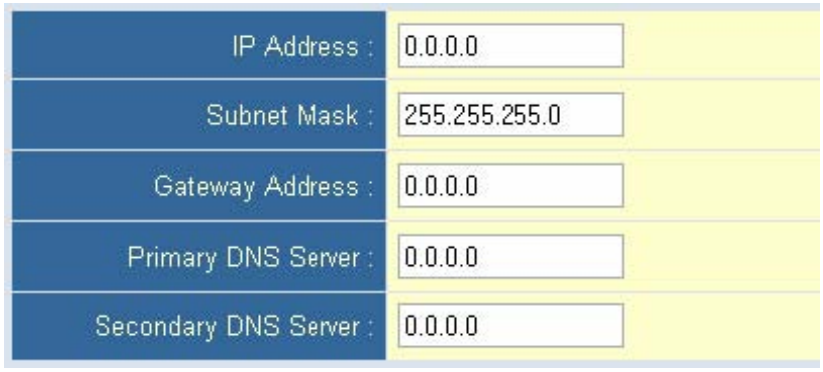
7.5.3 PPTP

Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe. It can be used to join different physical networks using the Internet as an intermediary. If you have been provided with the information as shown on the screen, enter the assigned IP address, subnet mask, default gateway IP address, user ID and password, and PPTP Gateway. Configure the Connect mode option to the desired settings. “Always On Line” signifies that the broadband router will maintain your Internet connection consistently and automatically connect to the Internet after any disconnection. “Manual Connect” signifies that the broadband router will establish an Internet connection only when the administrator logs into the web management and manually presses the “Connect” button. While using the “Connect On Demand” option, if the connection is inactive for longer than the Maximum Idle Time, it will be dropped and will automatically re-establish the connection as soon as you attempt to access the Internet again.



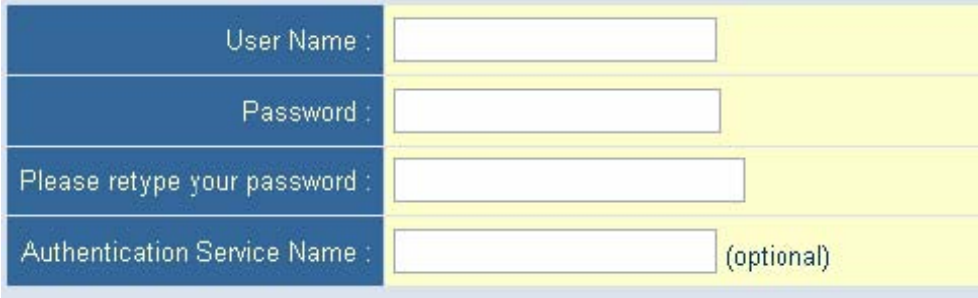
7.5.4 Static IP

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



7.5.6 BigPond

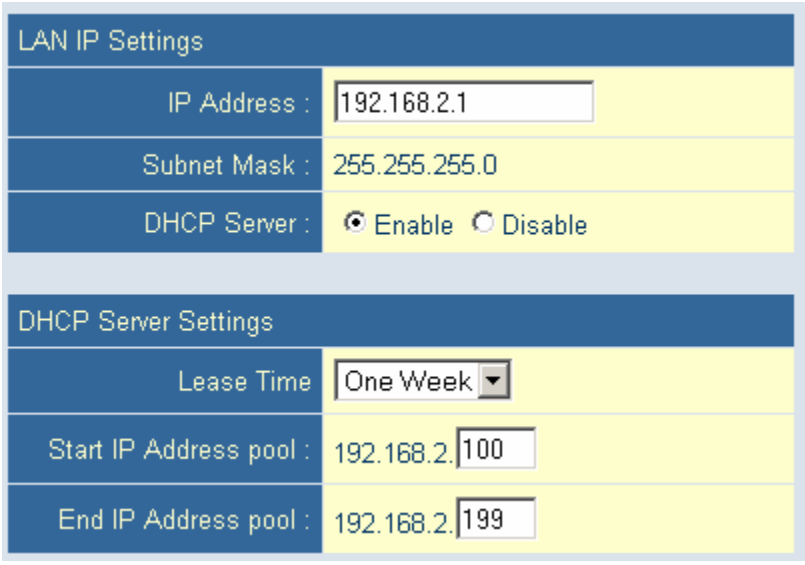
If you use the BigPond Internet Service which is available in Australia, enter your username and password and apply the changes.



7.6 | Advanced Setup - LAN

This is the local IP address of the router. All networked computers must use the LAN IP address of the router as their default Gateway. However, if necessary, it can be changed. Here you can configure the LAN IP address for the router and enable/disable the DHCP server for dynamic client address allocation. You can change the lease time if necessary as well. By default this is set to “One Week”. The other options are Half Hour, One Hour, Two Hours, Half Day, One Day, Two Days, and Forever. “Forever” signifies that there is no time limit on the IP address lease.

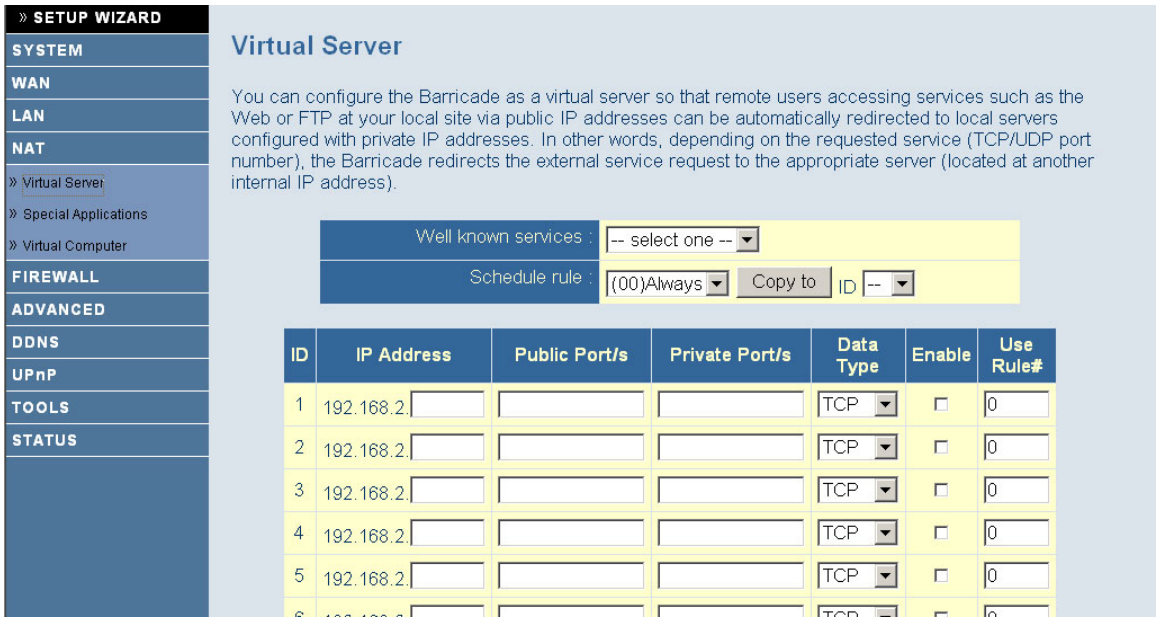
For the IP address pool, a dynamic IP address range may be specified (Default: 192.168.2.100-199). Once the IP addresses, e.g. 192.168.2.100–199, have been assigned, these IP addresses will be part of the dynamic IP address pool. IP addresses from 192.168.2.2–99, and 192.168.2.200–254 will be available as static IP addresses. Remember not to include the address of the Router in the client address pool. Also remember to configure your client PCs for dynamic IP address allocation.



7.7 | Advanced Setup - NAT

7.7.1 | Virtual Server

The firewall of the router filters out unrecognized packets to protect your intranet. This means that all network hosts are invisible to the outside world. However, some of the hosts can be made accessible by enabling the Virtual Server mapping. A virtual server is defined as a Service Port. All requests to this port will be redirected to the computer specified by the Server IP. The virtual server can work with scheduling rules as well. This gives you more flexibility for access control.



For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a server at 192.168.123.6, you need to specify the following virtual server mapping as shown in the table below:

Service Port	Server IP	Enable
21	192.168.123.1	X
80	192.168.123.2	X
1723	192.168.123.6	X

The “IP Address” section should contain the IP of the server computer in the LAN network that will be providing the virtual services. The “Public Port” is the port number or port range on the WAN side that will be used to access the virtual service. The “Private Port” is the port number of the service used by the server computer. “Data Type” can be User Datagram Protocol (UDP), Transmission Control Protocol (TCP) or both. This depends on the type of service you are running. TCP is connection-oriented protocol and UDP is connectionless. Since most services are connection-oriented, you will most likely need to select TCP. For example, FTP and HTTP are connection-oriented services while DNS and many streaming radio servers are connectionless.

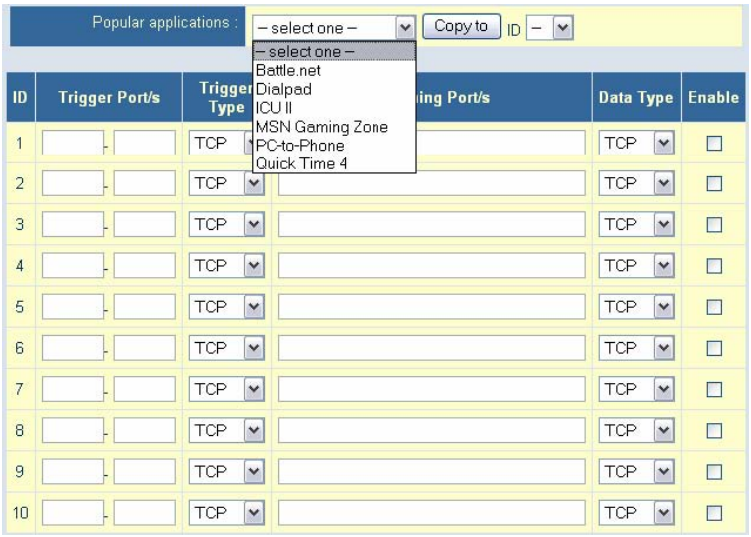
7.7.2 | Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, and Internet telephony. These applications cannot work with a pure NAT router because of the firewall function. However, the Special Applications feature allows some of these applications to work with the router. Should the Special Applications feature fail to make an application work, you can try setting your computer as a DMZ host.

Trigger: This is the outbound port number issued by the application.
Incoming Ports: When the trigger packet is detected, the inbound packets sent to specified port numbers are allowed to pass through the firewall.

The router provides some predefined settings. To add a predefined setting to your list, select an application and click “Copy to”.

Note: Only one computer can use the Special Application tunnels at any given time.



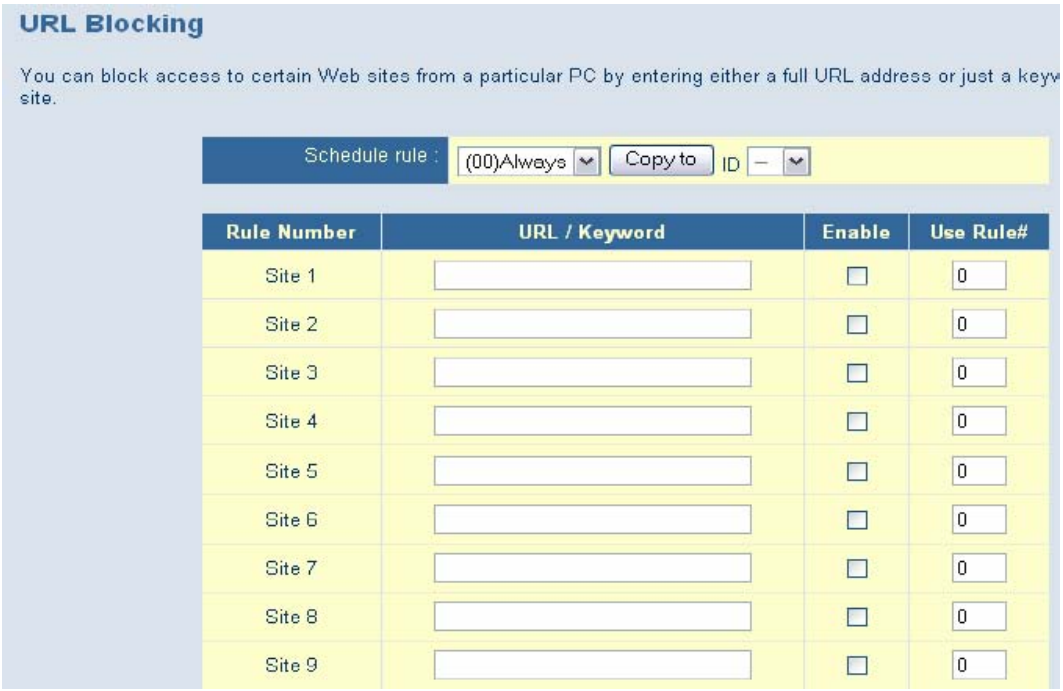
For a full list of ports and the services that run on them, see http://www.iana.org/assignments/port-numbers

7.8 | Advanced Setup - FIREWALL

7.8.1 | URL Blocking

URL Blocking blocks LAN computers from accessing pre-defined Websites. The difference between the Domain Filter and URL Blocking is that the Domain filter requires you to enter a suffix (.com or .org), while URL Blocking requires you to enter only a keyword. In other words, the Domain Filter can block specific Websites, while URL Blocking can block hundreds of Websites simply by using a keyword.

- URL Blocking: Check the box next to Enable if you want to enable the URL Blocking option.
- URL / Keyword: If any part of a Website's URL matches the pre-defined word you have entered here, the connection will be blocked. For example, if you type the word "firewall" into the URL text field, all URLs containing that word will be blocked.
- Enable: Check the box to enable the rules.
- Use Rule #: Applies a configured schedule rule



7.8.2 | MAC Filter

MAC Address Filtering allows you assign different access rights to various users and you can also assign a specific IP address to a certain MAC address.

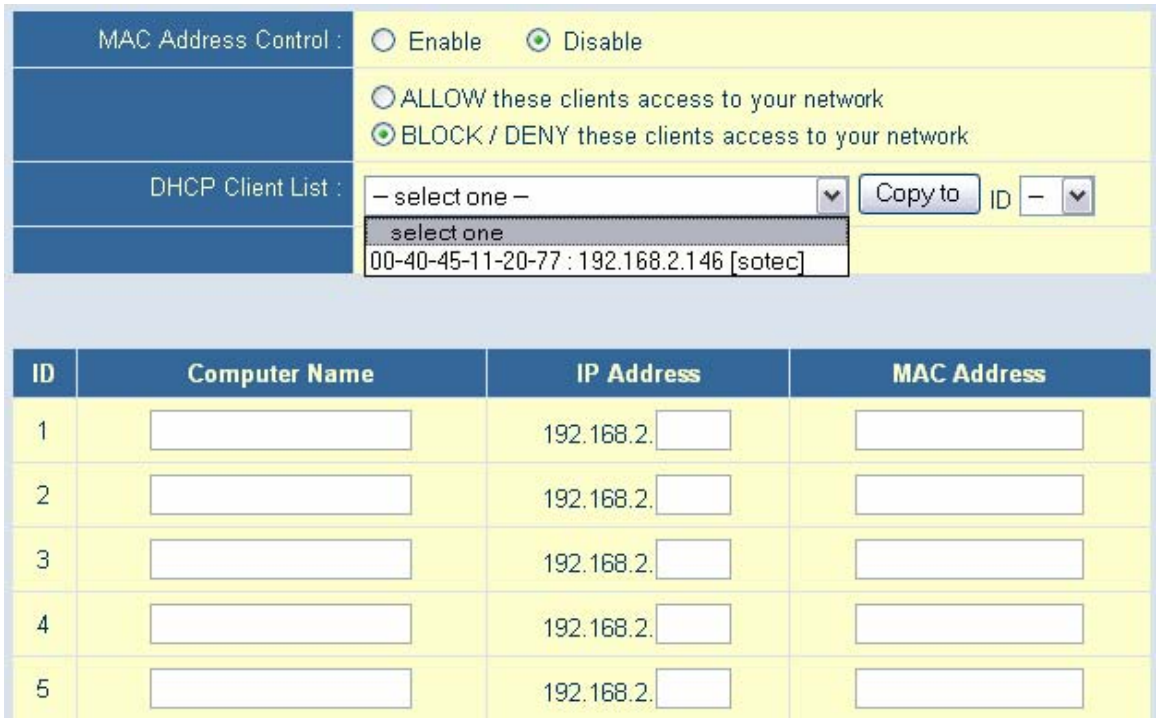
Select the Enable radio button to enable the MAC Address Control. All of the settings on this screen take effect when Enable is checked.

- MAC Address: This is the unique address of a specific client.
- IP Address: Expected IP address of the corresponding client. You can keep this text field blank if blank if you do not know the address.

The DHCP pull-down menu lets you select specific clients.

Select clients from the DHCP clients list and click "Copy to", to copy the MAC addresses to the selected ID, chosen from the ID pull-down menu.

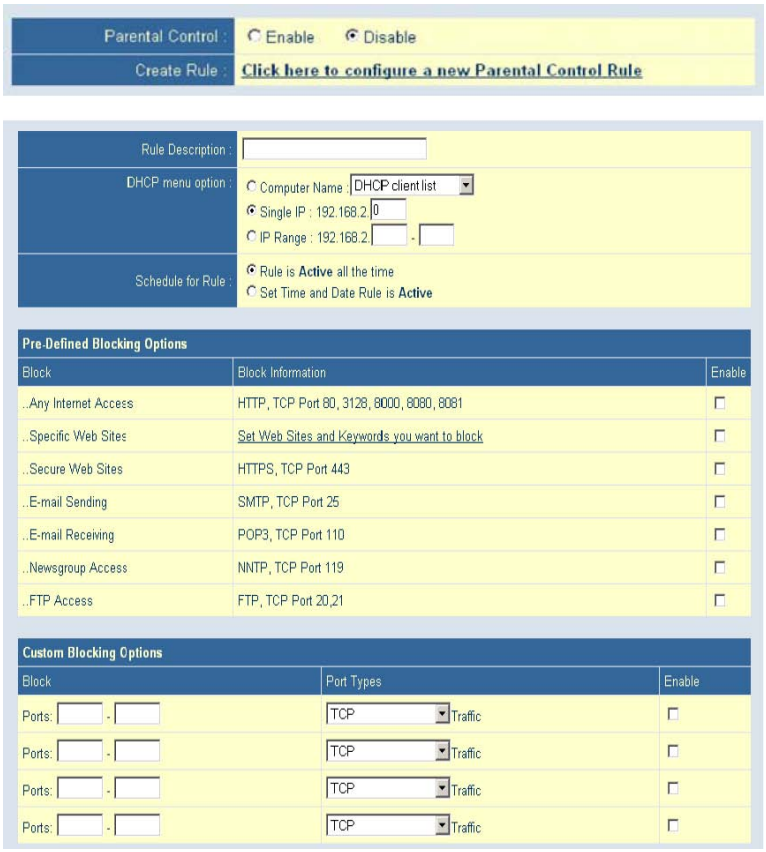
- Previous Page / Next Page: Use these links to navigate to different pages. The router supports up to 32 MAC filters.



7.8.3 | 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.



- **[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.

- **[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.

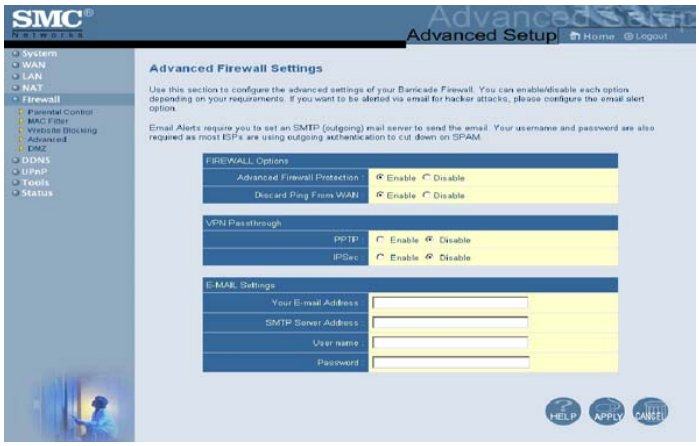
  For time, set the start time you want the Rule to active, and then set how long you want the rule to run.

7.8.4 | DMZ

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

7.8.5 | 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.

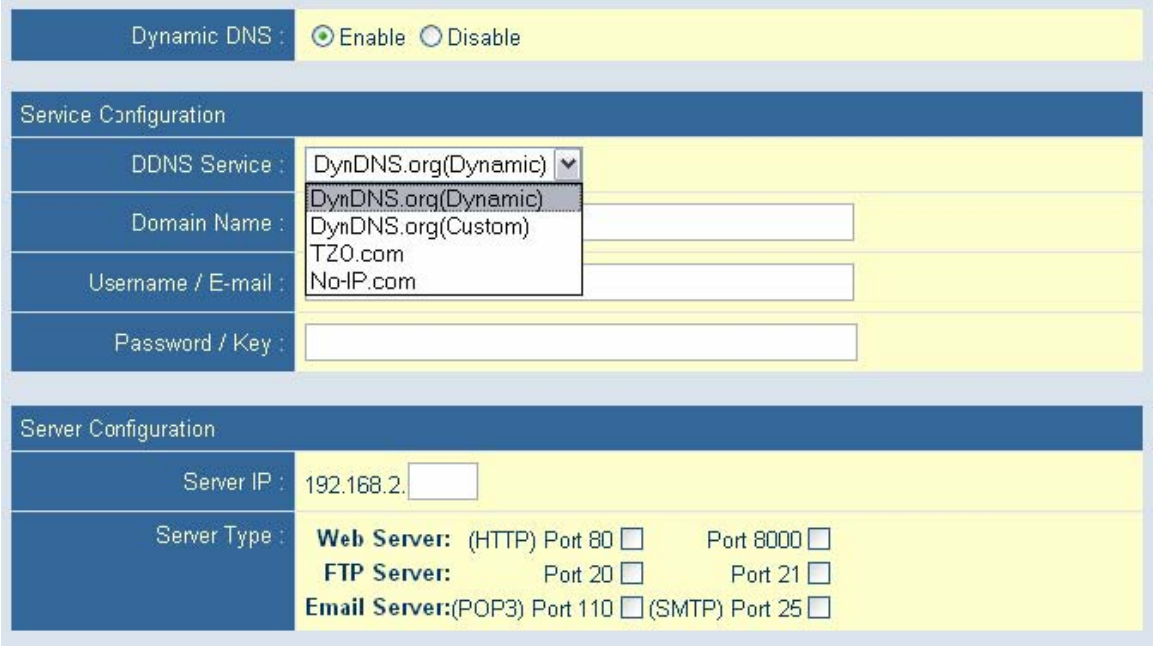
[Discard Ping from WAN:]
When this feature is enabled, any host on the WAN cannot ping this product. This helps avoid unnecessary attacks from the WAN side because your connection is invisible. It is recommended that you enable this option for security.

[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

7.9 | DDNS (Dynamic DNS)

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. Before you can enable the Dynamic DNS, you need to register an account with one of the Dynamic DNS servers that are listed in the Provider field.

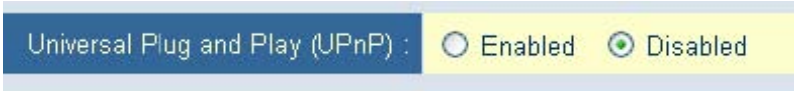


7.10 | UPnP (Universal Plug-and-Play)

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 networking in addition to control and data transfer among networked devices in the home, office and everywhere in between.

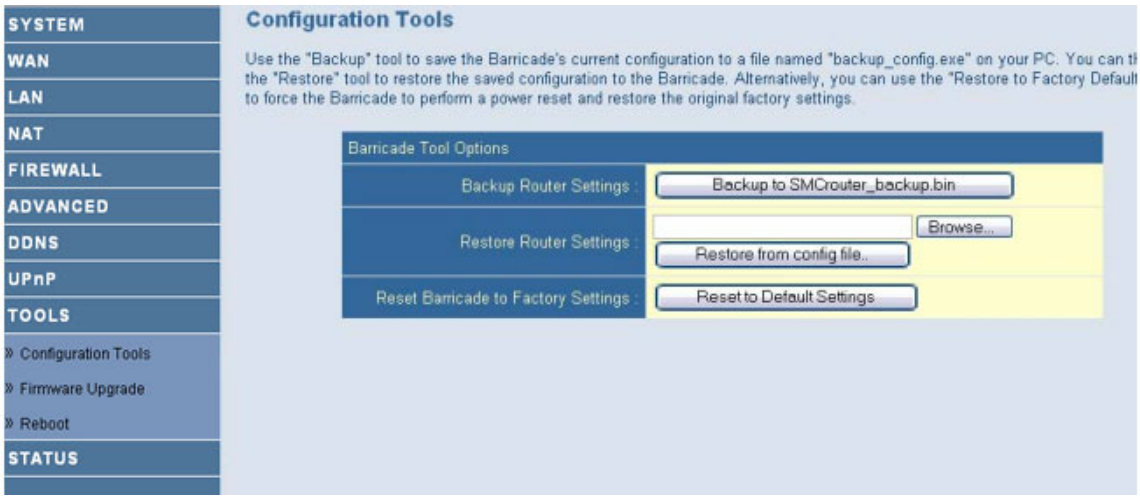
Enable UPnP by checking ON in the screen above. UPnP allows the device to automatically:
• dynamically join local network
• obtain an IP address
• convey its capabilities and learn about the presence and capabilities of other devices.

Dynamically open ports for UPnP aware software, such MSN messenger advanced features (voice, remote control).



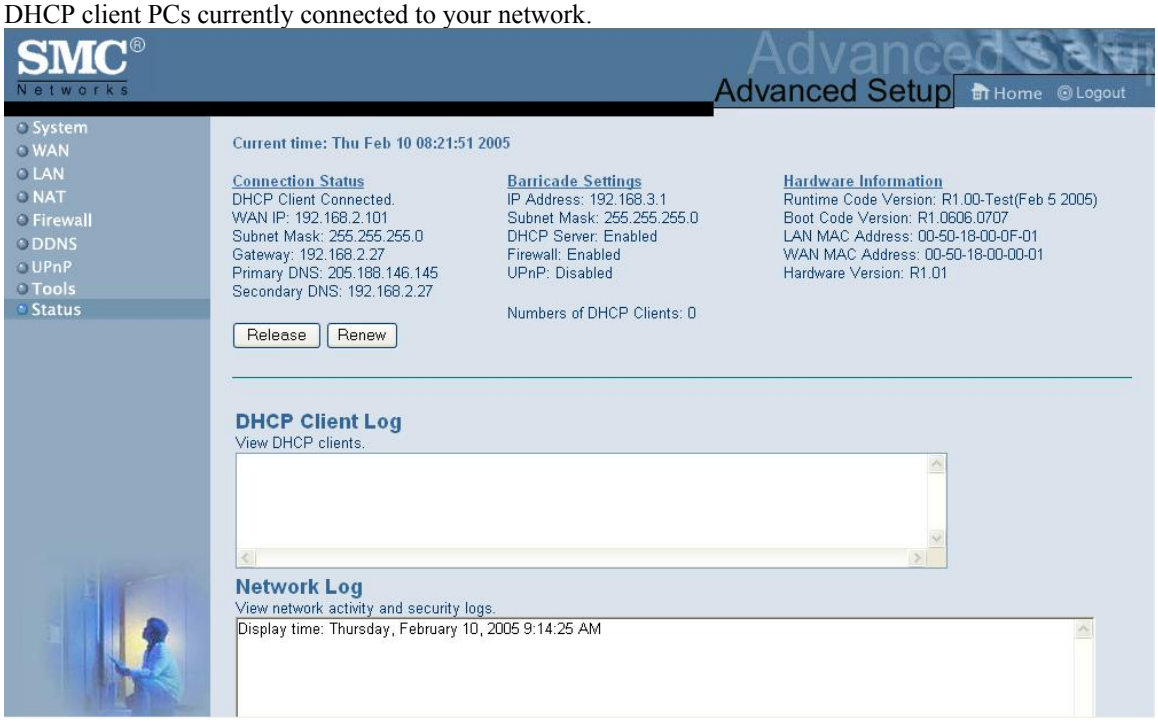
7.11 | Tools

The Toolbox menu allows you to view your system logs, upgrade firmware, backup settings, restore settings to defaults, reboot the router, and access miscellaneous settings.



7.12 | Status

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



8 | Troubleshooting

A. Verifying your connection to the router

If you are unable to access the Router's web-based administration pages, then you may not be properly connected or configured.

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 set up 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 by default.)
    - 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 the next section. If you have another IP address configured, then see section C

B. 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 Router. Confirm that you have a good link light on the Router for the port this computer is connected to. If not, please try another cable. If you have a good link light, please open up a DOS window as described in the previous section and type ipconfig/renew. If you are still unable to get an IP Address from the Router, reinstall your network adapter. Please refer to your adapter manual for information on how to do this.

C. My computer's IP Address is incorrect

If you have another IP address listed then the PC may not be configured for a DHCP connection. 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.
3. Then type ipconfig/renew.

D. The 10/100 LED does not light after a connection is made

1. Check that the host computer and the Router are both powered on.
2. Be sure the network cable is connected to both devices.
3. Verify that Category 5 cable is used if you are operating at 100 Mbps, and that the length of any cable does not exceed 100 m (328 ft).
4. Check the network card connections.
5. The 10BASE-T/100BASE-TX port, network card, or cable may be defective.

E. I can't get an Internet game, server, or application to work

If you are having an issue getting any Internet server, application or game to function properly, you can expose the PC to the Internet using the DeMilitarized Zone (DMZ) function. This option is useful when an application requires too many ports or when you are not sure which ports to use. See section 7.8.6 to successfully configure this option

F. I am having problems establishing a PPPoE xDSL WAN connection

Some ISP's require you to enter the domain name in addition to your username and password. For instance, for SBC Global, enter username@sbcglobal.net. For Ameritech users, enter username@ameritech.net. BellSouth users may need to enter username@bellsouth.net and Mindspring subscribers enter username@mindspring.com. Lastly, EarthLink subscribers should enter either username@earthlink.net or ELN/username@earthlink.net.

G. Can I use this router with AOL DSL?

This is true in most scenarios. Please verify with AOL that your particular connection type is PPPoE. If yes, then the SMC Broadband Router should work with your WAN connection. Follow the normal procedures as described in Section 7.3 of this manual, but while doing so, set the MTU value to 1400. AOL DSL does not allow for anything higher than 1400.

H. I forgot my password and can no longer log into the router

You should restore your router to factory defaults via its hardware reset button. Locate the reset button (to the right of the power input). While the device is powered on, use a paper clip to depress this button for about 5-7 seconds and then release. Now you have completed the reset to factory defaults.

I. Upgrading the firmware

New firmware revisions will be made available as necessary when new product features or functionality is released. You should check http://www.smc.com on a periodic basis for these updates. If a new version is available, check the release notes to be sure of what has been changed/added and then you can decide if you wish to complete the upgrade. Then download and unzip the firmware file. Log into the web-based administration of the SMC Router, click TOOLS, then click FIRMWARE UPGRADE and browse to the new firmware file. Then click the "BEGIN UPGRADE" button to upload the firmware to the SMC Router. Once this is completed, be sure to reset the router to factory defaults and reconfigure your WAN connection before continuing to use it.

9 | Terminology

10BaseT - Physical Layer Specification for Twisted-Pair Ethernet using Unshielded Twisted Pair wire at 10Mbps. This is the most popular type of LAN cable used today because it is very cheap and easy to install. It uses RJ-45 connectors and has a cable length span of up to 100 meters. There are two versions, STP (Shielded Twisted Pair) which is more expensive and UTP (Unshielded Twisted Pair), the most popular cable. These cables come in 5 different categories. However, only 3 are normally used in LANs, Category 3, 4 and 5. CAT 3 TP (Twisted Pair) cable has a network data transfer rate of up to 10Mbps. CAT 4 TP cable has a network data transfer rate of up to 16Mbps. CAT 5 TP cable has a network data transfer rate of up to 100Mbps.

Access Point - A device that is able to receive wireless signals and transmit them to the wired network, and vice versa - thereby creating a connection between the wireless and wired networks.

Ad Hoc - An ad hoc wireless LAN is a group of computers, each with LAN adapters, connected as an independent wireless LAN.

Adapter - A device used to connect end-user nodes to the network; each contains an interface to a specific type of computer or system bus, e.g. EISA, ISA, PCI, PCMCIA, CardBus, etc.

Auto-Negotiation - A signaling method that allows each node to define its operational mode (e.g., 10/100 Mbps and half/full duplex) and to detect the operational mode of the adjacent node.

Backbone - The core infrastructure of a network. The portion of the network that transports information from one central location to another central location where it is unloaded onto a local system.

Base Station - In mobile telecommunications, a base station is the central radio transmitter/receiver that maintains communications with the mobile radiotelephone sets within its range. In cellular and personal communications applications, each cell or micro-cell has its own base station; each base station in turn is interconnected with other cells' bases.

Bitmap – A Windows and OS/2 bitmapped graphics file format. Bitmap files provide formats for 2, 16, 256, or 16 million colors. It uses the extension .BMP.

BSS - BSS stands for "Basic Service Set". It is an Access Point and all the LAN PCs that are associated with it.

CHAP - When authenticating using Challenge Handshake Authentication Protocol (CHAP), the knowledge of the password, rather than the password itself is what is sent by the client. With CHAP, the Broadband Router sends the remote client a challenge string. The remote client uses the challenge string and the password, and creates a Message Digest-5 (MD5) hash which is then forwarded to the server. The server computes the same hash calculation and compares the result with the hash sent by the client. If they match, the remote client is considered an authentic user.

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DES - Data Encryption Standard. A cryptographic encryption algorithm that is part of many standards.
DHCP - Dynamic Host Configuration Protocol. This protocol automatically configures the TCP/IP settings of every computer on your home network.

DMZ - Allows a networked computer to be fully exposed to the Internet. This function is used when the special application sensing tunnel feature is insufficient to allow an application to function correctly.

DNS - DNS stands for Domain Name System, which allows Internet host computers to have a domain name (such as www.smc.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of host computers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing " www.smc.com" into your Internet browser), the user is sent to the proper IP address. The DNS server address used by the computers on your home network is the location of the DNS server your ISP has assigned.

DSL - DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet - A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10 million bits per second (Mbps).

ESS - ESS (ESS-ID, SSID) stands for "Extended Service Set". More than one BSS is configured to become an Extended Service Set. LAN mobile users can roam between different BSSs in an ESS (ESS-ID, SSID).

Fast Ethernet NIC - Network interface card that is in compliance with the IEEE 802.3u standard. This card functions at the media access control (MAC) layer, using carrier sense multiple access with collision detection (CSMA/CD).

Fixed IP – (see Static IP)

Full-Duplex - Transmitting and receiving data simultaneously. In pure digital networks, this is achieved with two pairs of wires. In analog networks, or digital networks using carriers, it is achieved by dividing the bandwidth of the line into two frequencies, one for sending, one for receiving.

Hub - Central connection device for shared media in a star topology. It may add nothing to the transmission (passive hub) or may contain electronics that regenerate signals to boost strength as well as monitor activity (active/intelligent hub). Hubs may be added to bus topologies; for example, a hub can turn an Ethernet network into a star topology to improve troubleshooting.

ID3 – The data fields in an MP3 that hold the artist name, track titles, album titles, genre, etc are known as ID3 tags.

IP Address - IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies an single, unique Internet computer host. Example: 192.34.45.8.

IP Security - Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

ISAKMP - Internet Security Association and Key Manangement Protocol. The basis for IKE.
ISP - Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

JPEG – Joint Photographic Experts Group. JPEG is a standard for compressing still images and it provides compression with ratios up to 100:1. File extensions are .JPG or .JPEG.

LAN - A communications network that serves users within a confined geographical area. It is made up of servers, workstations, a network operating system and a communications link. Servers are high-speed machines that hold programs and data shared by network users. The workstations (clients) are the users' personal computers, which perform stand-alone processing and access the network servers as required.

Diskless and floppy-only workstations are sometimes used, which retrieve all software and data from the server. Increasingly, "thin client" network computers (NCs) and Windows terminals are also used. A printer can be attached locally to a workstation or to a server and be shared by network users. Small LANs can allow certain workstations to function as a server, allowing users access to data on another user's machine. These peer-to-peer networks are often simpler to install and manage, but dedicated servers provide better performance and can handle higher transaction volume. Multiple servers are used in large networks.

The message transfer is managed by a transport protocol such as TCP/IP and NetBEUI. The physical transmission of data is performed by the access method (Ethernet, Token Ring, etc.), which is implemented in the network adapters that are plugged into the machines. The actual communications path is the cable (twisted pair, coax, optical fiber) that interconnects each network adapter.

MAC Address - MAC (Media Access Control) A MAC address is the hardware address of a device connected to a network.

MDI / MDI-X - Medium Dependent Interface - Also called an "uplink port," it is a port on a network hub or switch used to connect to other hubs or switches without requiring a crossover cable. The MDI port does not cross the transmit and receive lines, which is done by the regular ports (MDI-X ports) that connect to end stations. The MDI port connects to the MDI-X port on the other device. There are typically one or two ports on a device that can be toggled between MDI (not crossed) and MDI-X (crossed).

Medium Dependent Interface – X (crossed) - A port on a network hub or switch that crosses the transmit lines coming in to the receive lines going out.

MP3 – MPEG Audio Layer 3. This is an audio compression technology that is included in the MPEG-1 and -2 specifications. MP3 encoding can allow you to compress CD-quality sound by a factor of 12.

MPEG – Moving Pictures Experts Group. MPEG is a standard for compressing video. MPEG-1 can provide resolution of 352x240 at 30 frames/second (fps) with 24-bit color and CD-quality sound. MPEG-2 can provide resolution of 704x480. MPEG uses the same intraframe coding as JPEG for individual frames, but also uses interframe coding which can help to further compress the video data, thereby reducing the overall size of the video.

NAT – (Network Address Translation) This process allows all of the computers on your home network to use one IP address. The NAT capability of the Barricade, allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP. Network Address Translation can be used to give multiple users access to the Internet with a single user account, or to map the local address for an IP server (such as Web or FTP) to a public 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. NAT must be enabled to provide multi-user access to the Internet or to use the Virtual Server function.

Packet Binary Convulational Code(tm) (PBCC) - A modulation technique developed by Texas Instruments Inc. (TI) that offers data rates of up to 22Mbit/s and is fully backward compatible with existing 802.11b wireless networks.

PAP - This is a simple authentication protocol where the username and password data are both handled in a cleartext or unencrypted format. We do not recommend using PAP because your passwords are easily readable from the Point-to-Point Protocol (PPP) packets exchanged during the authentication process.

PCI - Peripheral Component Interconnect - Local bus for PCs from Intel that provides a high-speed data path between the CPU and up to 10 peripherals (video, disk, network, etc.). The PCI bus runs at 33MHz, supports 32-bit and 64-bit data paths, and bus mastering.

PPPoE - Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a method of secure data transmission originally created for dial-up connections. PPPoE is for Ethernet connections.

PPTP - PPTP stands for Point-to-Point Tunneling Protocol. It provides a means for tunneling IP traffic in Layer 2. For instance, it allows you to establish a connection to a corporate network and share files or other data as if your machine were actually on that local network.

Roaming - A function that allows your to move through a particular domain without losing network connectivity.

SNMP - Format used for network management data. Data is passed between SNMP agents (processes that monitor activity in hubs, switches, etc.) and the workstation used to oversee the network. SNMP uses Management Information Bases (MIBs), which are databases that define what information is obtainable from a networked device and what can be controlled (turned off, on, etc.).

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

SPI - Stateful Packet Inspection ensures that the data coming into your network was requested by an end node computer on your LAN. The Barricade examines the incoming data and compares it to a database of trusted information. As traffic leaves the network it is defined by certain characteristics. Incoming information is then compared to these sets of characteristics. If the incoming data matches the predefined set of characteristics the incoming traffic is allowed. If no match is found the incoming traffic is discarded.

Subnet Mask - A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet.

TCP/IP - Transmission Control Protocol/Internet Protocol. This is the standard protocol for data transmission over the Internet.
TCP - Transmission Control Protocol - TCP and UDP (User Datagram Protocol) are the two transport protocols in TCP/IP. TCP ensures that a message is sent accurately and in its entirety. However, for real-time voice and video, there is really no time or reason to correct errors, and UDP is used instead.

UDP - User Datagram Protocol - A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required. For example, UDP is used for real-time audio and video traffic where lost packets are simply ignored, because there is no time to retransmit. If UDP is used and a reliable delivery is required, packet sequence checking and error notification must be written into the applications.

10 | 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 IP addresses

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

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

Upgrade method
Web-based

LEDs
Power
WAN
Link
Activity

Power
Input Power DC 9V 1A
AC power consumption → 2.25 watt (AC 0.25A/9volt)

Operating Temperature

0°~40°C , humidity 10%~90% non-condensing

Storage Temperature

-200~700C , -20~70oC, Humidity: 0~95% non-condensing

Compliance

FCC
CE
UL

Dimensions

131mm(L)x86mm(W)x 32 mm(H) (5.15x3.38x1.25 in)

Weight

115g

11 | 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 theCouncil 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:

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:
UL 1950
EN60950
CSA 22.2 No. 950

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. Ambesten 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 authorisiertem Servicepersonal geöffnet werden.

14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
    a. Netzkabel oder Netzstecker sind beschädigt.
    b. Flüssigkeit ist in das Gerät eingedrungen.
    c. Das Gerät war Feuchtigkeit ausgesetzt.
    d. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
    e. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
    f. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

15. Stellen Sie sicher, daß die Stromversorgung dieses Gerätes nach der 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.

12 | 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 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, 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 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.com (section support).

Firmware and Drivers

For latest driver, technical information and bug-fixes please visit www.smc.com (section support).

Contact SMC

Contact details for your relevant countries are available on 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.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

Trademarks

Model Number: SMC7004VBR

FOR TECHNICAL SUPPORT, CALL:
From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; Phn: (949) 679-8000; Fax: (949) 679-1481
From Europe : Contact details can be found on www.smc.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/

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-91-352-00-40	Fax 34-93-477-3774
UK:	44 (0) 871 277 98 02	Fax 44 (0) 1234 831 413
France:	33 (0) 1 55 64 04 55	Fax 33 (0) 1 45 34 68 58
Italy:	39 02 739 12 68	Fax 39 02 739 14 17
Benelux:	31 (0) 654 776 790	Fax 31 (0) 172 242 393
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Nordics and Baltics:	45 (0) 566 622 83	Fax 45 (0) 566 622 86
Eastern Europe:	420 266 794 421	Fax 420 266 794 423
Sub-Saharan Africa:	27 012 661 02 32	Fax 34 93 477 3774
North West Africa:	34 93 477 4920	Fax 34 93 477 3774
CIS:	34 93 477 4920	Fax 34 93 477 3774
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-87978006	Fax 886-2-87976288
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-45-224-2332	Fax 81-45-224-2331
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

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

Model Number: SMC7004VBR

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