

Barricade[™] g 2.4GHz 54 Mbps Wireless Cable/DSL Broadband Router

User Guide

SMC2804WBR



Barricade™ 2.4 GHz 54 Mbps Wireless Cable/DSL Broadband Router

From SMC's Barricade line of Broadband Routers

SMC®

Networks

38 Tesla

Irvine, CA 92618

Phone: (949) 679-8000

March 2003

Revision Number: R01

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.

Copyright © 2003 by
SMC Networks, Inc.
38 Tesla
Irvine, CA 92618

All rights reserved. Printed in Taiwan

Trademarks:

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

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, (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 RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

EC Conformance Declaration - Class B

SMC contact for these products in Europe is:

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

This information technology equipment 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:

- RFI * Limit class B according to EN 55022:1998
- Emission: * Limit class A for harmonic current emission according to EN 61000-3-2/1995
- * Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995
- Immunity: * Product family standard according to EN 55024:1998
- * Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ± 4 kV, Air Discharge: ± 8 kV)
- * Radio-frequency electromagnetic field according to EN 61000-4-3:1996 (80 - 1000MHz with 1kHz AM 80% Modulation: 3V/m)
- * Electrical fast transient/burst according to EN 61000-4-4:1995(AC/DC power supply: ± 1 kV, Data/Signal lines: ± 0.5 kV)
- * Surge immunity test according to EN 61000-4-5:1995(AC/DC Line to Line: ± 1 kV, AC/DC Line to Earth: ± 2 kV)
- * Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996(0.15 - 80MHz with 1kHz AM 80% Modulation: 3V/m)
- * Power frequency magnetic field immunity test according to EN 61000-4-8:1993(1A/m at frequency 50Hz)
- * Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994(>95% Reduction @ 10ms, 30% Reduction @ 500ms, >95% Reduction @ 5000ms)
- LVD: * EN60950(A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

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.

Australia AS/NZS 3548 (1995) - Class B



ACN 069 351 613

SMC contact for products in Australia is:

SMC Communications Pty. Ltd.
Suite 18, 12 Tryon Road,
Lindfield NSW2070,
Phone: 61-2-8875-7887
Fax: 61-2-8875-7777

Safety Compliance

Underwriters Laboratories Compliance Statement

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Operating Voltage	Cord Set Specifications
120 Volts	UL Listed/CSA Certified Cord Set
	Minimum 18 AWG
	Type SVT or SJT three conductor cord
	Maximum length of 15 feet
240 Volts (Europe only)	Parallel blade, grounding type attachment plug rated 15A, 125V
	Cord Set with H05VV-F cord having three conductors with minimum diameter of 0.75 mm ²
	IEC-320 receptacle
	Male plug rated 10A, 250V

The unit automatically matches the connected input voltage. Therefore, no additional adjustments are necessary when connecting it to any input voltage within the range marked on the rear panel.

Wichtige Sicherheitshinweise (Germany)

1. Bitte lesen Sie diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssigoder Aerosolreiniger. Am besten eignet sich ein angefeuchtetes Tuch zur Reinigung.
4. Die Netzanschluß Steckdose 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 EN 60950 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.

TABLE OF CONTENTS

About the Wireless Barricade g Router	1
LED Indicators	1
Features and Benefits	2
Installing the Wireless Barricade g Router	3
Package Contents	3
Hardware Description	4
System Requirements	6
Connect the System	7
Basic Installation Procedure	7
Configuring Client TCP/IP	12
Installing TCP/IP	12
Windows 95/98/ME	12
Windows 2000	13
Setting Up TCP/IP	15
Configuring Your Computer in Windows 95/98/Me	15
Configuring Your Computer in Windows NT 4.0	18
Configuring Your Computer in Windows 2000	20
Configuring Your Computer in Windows XP	21
Configuring a Macintosh Computer	22
Manual IP Configuration	23
Verifying Your TCP/IP Connection	24
Configuring the Wireless Barricade g Router	26
Browser Configuration	26
Disable Proxy Connection	27
Internet Explorer (5 or above)	27
Internet Explorer (For Macintosh)	27
Netscape (4 or above)	28
Navigating the Web Browser Interface	29
Making Configuration Changes	29

TABLE OF CONTENTS

Setup Wizard 30

 Time Zone 30

 Broadband Type 31

Advanced Setup 33

 System 34

 WAN 36

 LAN 42

 Wireless 43

 Network Address Translation (NAT) 47

 Firewall 50

 DDNS (Dynamic DNS) Settings 60

 UPnP (Universal Plug and Play) Setting 61

 Tools 62

Troubleshooting66

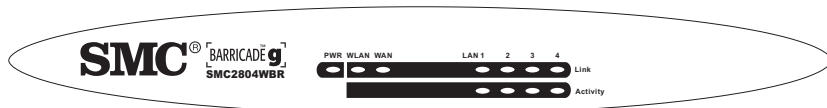
Specifications69

ABOUT THE WIRELESS BARRICADE G ROUTER

Congratulations on your purchase of the Wireless Barricade™ g Broadband Router. SMC is proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet at the lowest possible cost, this Router provides a convenient and powerful solution.

LED Indicators

The Wireless Barricade g Router includes status LED indicators, as described in the following figure and table.



LED	Status	Description
PWR (Green)	On	The Router is receiving power.
WLAN (Green)	On	The Router has established a valid wireless connection.
WAN (Green)	On	The WAN port has established a valid network connection.
LAN		
Link (Green)	On	The indicated LAN port has established a valid network connection.
	Flashing	The indicated LAN port is transmitting or receiving traffic.
Activity (Amber)	Off	The indicated LAN port has established a valid 10 Mbps network connection.
	On	The indicated LAN port has established a valid 100 Mbps network connection.

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 ports or 54 Mbps wireless interface (supporting up to 253 mobile users)
- 802.11g draft Compliant – interoperable with multiple vendors
- Provides seamless roaming within 802.11g draft WLAN environment
- 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 allow the user to restrict Web browsing
- Automatic email alerts when the network is being attacked
- Easy setup through a Web browser on any operating system that supports TCP/IP
- Compatible with all popular Internet applications

INSTALLING THE WIRELESS BARRICADE G ROUTER

Before installing the Wireless Barricade™ g Broadband Router, verify that you have all the items listed under “Package Contents.” If any of the items are missing or damaged, contact your local SMC distributor. Also be sure that you have all the necessary cabling before installing the Router. After installing the Router, refer to the Web-based configuration program in “Configuring the Wireless Barricade g Router” on page 26 for information on configuring the Router.

Package Contents

After unpacking the Wireless Barricade g Broadband Router, check the contents of the box to be sure you have received the following components:

- Wireless Barricade g Broadband Router
- Power adapter
- One CAT-5 Ethernet cable
- Four rubber feet
- Installation CD containing this User Guide and EZ 3-Click Installation Wizard
- 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.

Installing the Wireless Barricade g Router

Please register on SMC's Web site at www.smc.com The Wireless Barricade g Router is covered by a limited lifetime warranty.

Hardware Description

The Router can be connected to the Internet or to a remote site using its RJ-45 WAN port. It can be connected directly to your PC or to a local area network using any of the Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL can provide up to 8 Mbps downstream and 640 Kbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 Kbps upstream. Cable modems can provide up to 36 Mbps downstream and 2 Mbps upstream. ISDN can provide up to 128 Kbps when using two bearer channels. PSTN analog connections can now run up to 56 Kbps. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Although access speed to the Internet is determined by the modem type connected to the Router, data passing between devices connected to your local area network can run up to 100 Mbps over the Fast Ethernet ports.

The Router includes an LED display on the front panel for system power and port indications that simplifies installation and network troubleshooting. It also provides four RJ-45 LAN ports and one RJ-45 WAN port on the rear panel.

- 4 RJ-45 ports for connection to a 10BASE-T/100BASE-TX Ethernet Local Area Network (LAN). These ports can auto-negotiate the operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X

(i.e., allowing these ports to be connected to any network device with straight-through cable). These ports can be connected directly to a PC or to a server equipped with an Ethernet network interface card, or to a networking device such as an Ethernet hub or switch.

- One RJ-45 port for connection to a DSL or cable modem (WAN). This port also auto-negotiates operating speed to 10/100 Mbps, the mode to half/full duplex, and the pin signals to MDI/MDI-X.

The following figure shows the components of the Router:

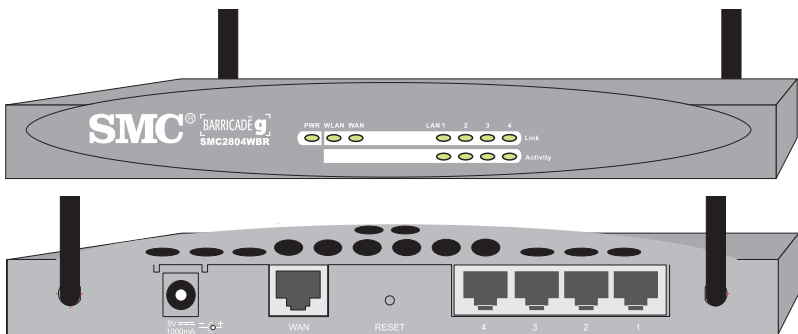


Figure 1. Front and Rear Panels

Item	Description
Reset Button	Use this button to reset the power and restore the default factory settings.
LEDs	Power, WAN and LAN port status indicators. (See “LED Indicators” on page 1.)
LAN Ports	Fast Ethernet ports (RJ-45). Connect devices (such as a PC, hub or switch) on your local area network to these ports.
WAN Port	WAN port (RJ-45). Connect your cable modem, DSL modem, or an Ethernet router to this port.
Power Inlet	Connect the included power adapter to this inlet. Warning: Using the wrong type of power adapter may cause damage.

System Requirements

You must have an ISP that meets the following minimum requirements:

- Internet access from your local telephone company or Internet Service Provider (ISP) using a DSL modem, cable modem, ISDN TA, or PSTN analog modem. You may also have access over the telephone system to an analog modem at another site.
- 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.

Connect the System

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

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

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

Basic Installation Procedure

1. **Connect the LAN:** Connect the Router to your PC, or to a hub or switch. Run Ethernet cable from one of the LAN ports on the rear of the Router to your computer's network adapter or to another network device.

You may also connect the Router to your PC (using a wireless client adapter) via radio signals. Position both antennas on the back of the Router into the desired positions. For more effective coverage, position one antenna along the vertical axis and the other antenna along the horizontal axis. **(The antennas emit signals along the toroidal plane – and thus provide more effective coverage when positioned along alternate axes.)**

2. **Connect the WAN:** Prepare an Ethernet cable for connecting the Router to a cable/xDSL modem or Ethernet router.

Installing the Wireless Barricade g Router

- 3. Power on:** Connect the power adapter to the Router.

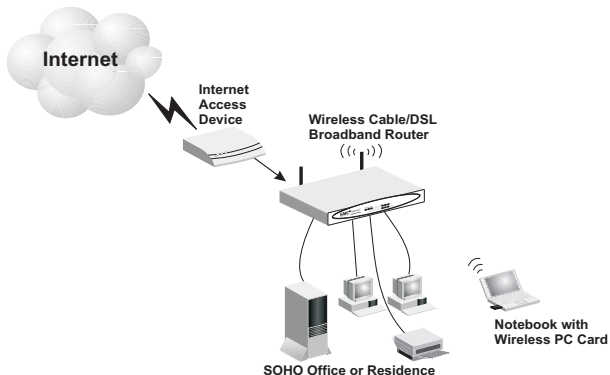


Figure 2. Connecting the Wireless Barricade g Router

Attach to Your Network Using Ethernet Cabling

The four LAN ports on the Router auto-negotiate the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, and the transmission mode to half duplex or full duplex.

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

Warning: Do not plug a phone jack connector into any RJ-45 port. This may damage the Router. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

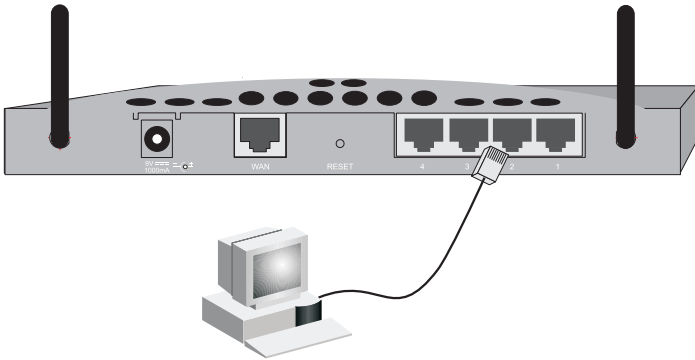


Figure 3. Making the LAN Connections

Attach to Your Network Using Radio Signals

Install a wireless network adapter in each computer that will be connected to the Internet or your local network via radio signals. SMC currently offers several wireless network cards, including the SMC2602W and SMC2632W Wireless cards.

Rotate both antennas on the back of the Router to the desired position. For more effective coverage, position one antenna along the vertical axis and the other along the horizontal axis. Try to place the Router in a position that is located in the center of your wireless network. Normally, the higher you place the antenna, the better the performance. Ensure that the Router's location provides optimal reception throughout your home or office.

Computers equipped with a wireless adapter can communicate with each other as an independent wireless LAN by configuring each computer to the same radio channel. However, the Router can provide access to your wired/wireless LAN or to the Internet for all wireless workstations. Each wireless PC in this network infrastructure can talk to any computer in the wireless group via a

Installing the Wireless Barricade g Router

radio link, or access other computers or network resources in the wired LAN infrastructure or over the Internet via the Router.

The wireless infrastructure configuration not only extends the accessibility of wireless PCs to the wired LAN, but also doubles the effective wireless transmission range for wireless PCs by retransmitting incoming radio signals through the Router.

A wireless infrastructure can be used for access to a central database, or for connection between mobile workers, as shown in the following figure:

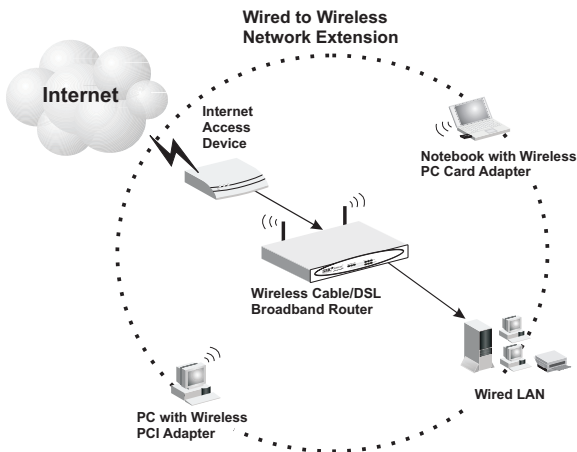


Figure 4. Making the WLAN Connections

Attach the Wireless Barricade g Router to the Internet

If Internet services are provided through an xDSL or cable modem, use unshielded or shielded twisted-pair Ethernet cable (Category 3 or greater) with RJ-45 plugs to connect the broadband modem directly to the WAN port on the Router.

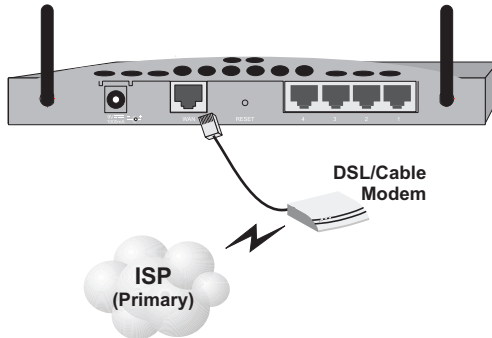


Figure 5. Making the WAN Connection

Note: When connecting to the WAN port, use 100-ohm Category 3, 4, or 5 shielded or unshielded twisted-pair cable with RJ-45 connectors at both ends for all connections.

Connecting the Power Adapter

Plug the power adapter into the power socket on the Router, and the other end into a power outlet. Check the indicator marked "PWR" on the front panel to be sure it is on. If the power indicator does not light, refer to "Troubleshooting" on page 66.

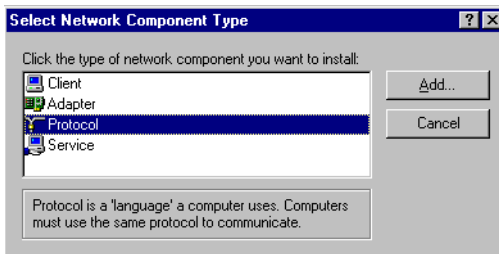
CONFIGURING CLIENT TCP/IP

If you have not previously installed the TCP/IP protocols on your client PCs, refer to the following section. If you need information on how to configure a TCP/IP address on a PC, refer to “Setting Up TCP/IP” on page 15.

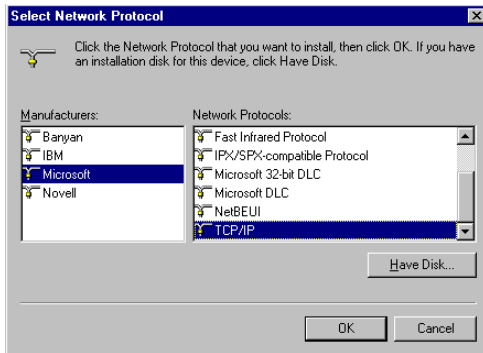
Installing TCP/IP

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.



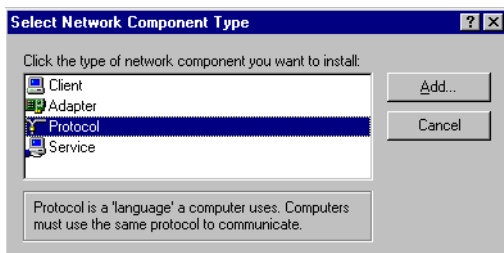
6. The TCP/IP protocol will be listed in the Network window. Click OK. The operating system may prompt you to restart your system. Click Yes and the computer will shut down and restart.

Windows 2000

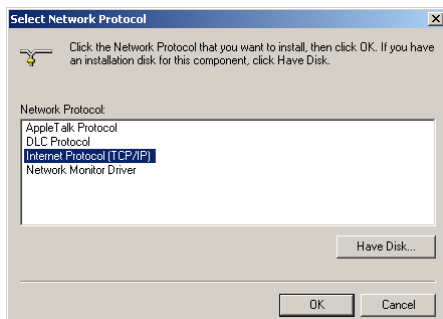
1. Click the Start button and choose Settings, then click the Network and Dial-up Connections icon.
2. Double-click the Local Area Connection icon, and click the Properties button on the General tab.
3. Click the install... button.

Configuring Client TCP/IP

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.

Setting Up TCP/IP

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

Gateway IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Note: These settings may be changed to suit your network requirements, but you must first configure at least one computer as described in this chapter to access the Router's Web configuration interface. See "Configuring the Wireless Barricade g Router" on page 26 for information on configuring the Router.)

If you have not previously configured TCP/IP for your computer, refer to "Configuring Client TCP/IP" on page 12. The IP address of the connected client PC should be 192.168.2.x (where x means 2–254). You can set the IP address for client PCs either by automatically obtaining an IP address from the Router's DHCP service or by manual configuration.

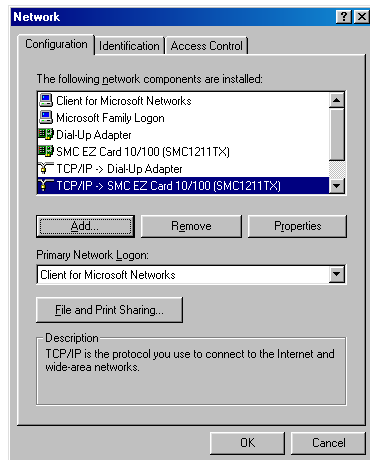
Configuring Your Computer in Windows 95/98/Me

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.

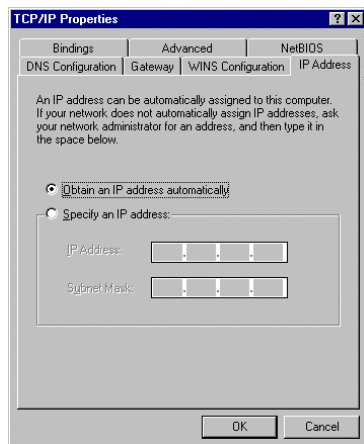
1. From the Windows desktop, click Start/Settings/Control Panel.
2. In the Control Panel, locate and double-click the Network icon.

Configuring Client TCP/IP

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.

Setting Up TCP/IP

8. On the Network Properties Window, click the OK button to save these new settings.

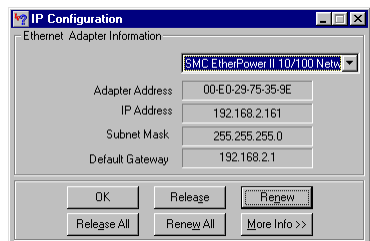
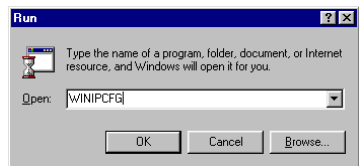
Note: Windows may ask you for the original Windows installation disk or additional files. Check for the files at c:\windows\options\cabs, or insert your Windows CD-ROM into your CDROM drive and check the correct file location, e.g., D:\win98, D:\win9x. (if D is the letter of your CD-ROM drive).

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.

Obtain IP Settings from Your Wireless Barricade g Router

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

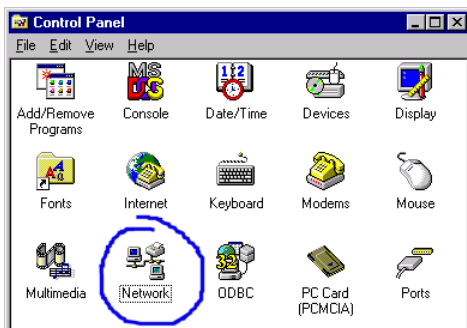
1. Click Start/Run.
2. Type WINIPCFG and click OK.
3. From the drop-down menu, select your network card. Click Release and then Renew. Verify that your IP address is now 192.168.2.xxx, your Subnet Mask is 255.255.255.0 and your Default Gateway is 192.168. 2.1. These values confirm that the Router is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



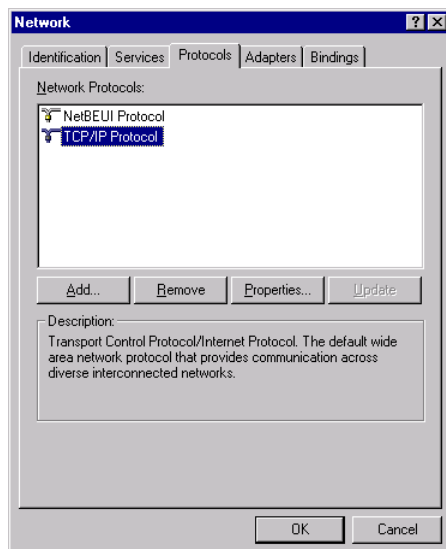
Configuring Client TCP/IP

Configuring Your Computer in Windows NT 4.0

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.



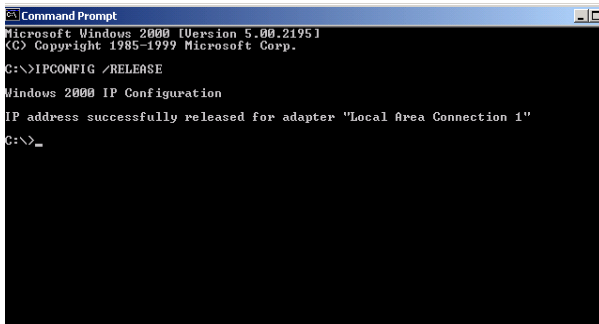
5. Click on the IP Address tab.
6. In the Adapter drop-down list, be sure your Ethernet adapter is selected.

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.

Obtain IP Settings From Your Wireless Barricade g Router

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

1. On the Windows desktop, click Start/Programs/Command Prompt.
2. In the Command Prompt window, type IPCONFIG /RELEASE and press the <ENTER> key.



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

C:\>IPCONFIG /RELEASE

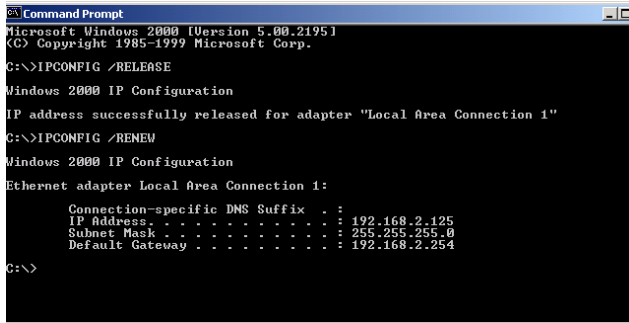
Windows 2000 IP Configuration

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

C:\>_
```

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

Configuring Client TCP/IP



```
C:\>IPCONFIG /RELEASE

Windows 2000 IP Configuration

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

C:\>IPCONFIG /RENEW

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 1:

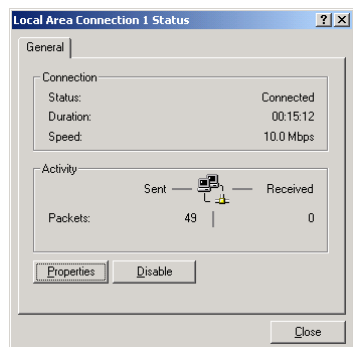
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.125
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.254

C:\>
```

4. Type EXIT and press <ENTER> to close the Command Prompt window.

Configuring Your Computer in Windows 2000

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.

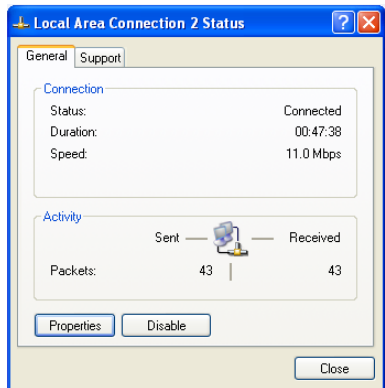


5. Select “Obtain an IP address automatically” to configure your computer for DHCP. Click the OK button to save this change and close the Properties window.
6. Click the OK button again to save these new changes.
7. Reboot your PC.
8. To obtain new network settings see “Obtain IP Settings from Your Wireless Barricade g Router” on page 17.

Configuring Your Computer in 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 Router. Next, click the Properties button.



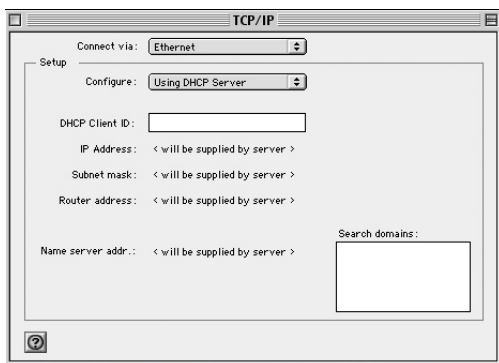
Configuring Client TCP/IP

3. 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.
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

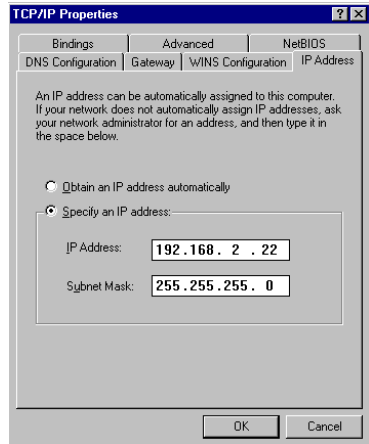
You may find that the instructions here do not exactly match your screen. This is because these steps and screenshots were created using Mac OS 8.5. Mac OS 7.x and above are all very similar, but may not be identical to Mac OS 8.5.

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.
3. Select Using DHCP Server in the Configure field.
4. Close the TCP/IP dialog box.

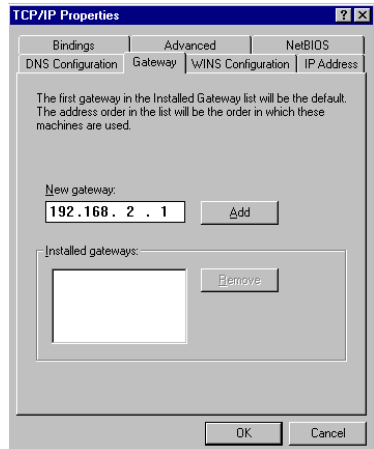


Manual IP Configuration

1. Check Specify an IP address on the IP Address tab. Enter an IP address based on the default network 192.168.2.x (where x is between 2 and 254), and use 255.255.255.0 for the subnet mask.

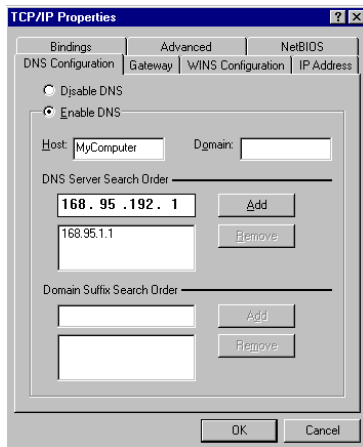


2. In the Gateway tab, add the IP address of the Router (default: 192.168.2.1) in the New gateway field and click Add.



Configuring Client TCP/IP

3. On the DNS Configuration tab, add the IP address for the Router and click Add. This automatically relays DNS requests to the DNS server(s) provided by your ISP. Otherwise, add specific DNS servers into the DNS Server Search Order field and click Add.
4. After finishing TCP/IP setup, click OK, and then reboot the computer. After that, set up other PCs on the LAN according to the procedures described above.



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,

Setting Up TCP/IP

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 - 192.168.2.254 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!

CONFIGURING THE WIRELESS BARRICADE G ROUTER

The Wireless Barricade g Router can be configured by any Java-supported browser including Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above. Using the Web management interface, you can configure the Router 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 and download the latest firmware update to ensure your Router is running the latest firmware.

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.

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. 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)

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)

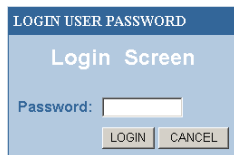
1. Open Internet Explorer. Click Edit/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.
3. Uncheck all checkboxes and click OK.

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.

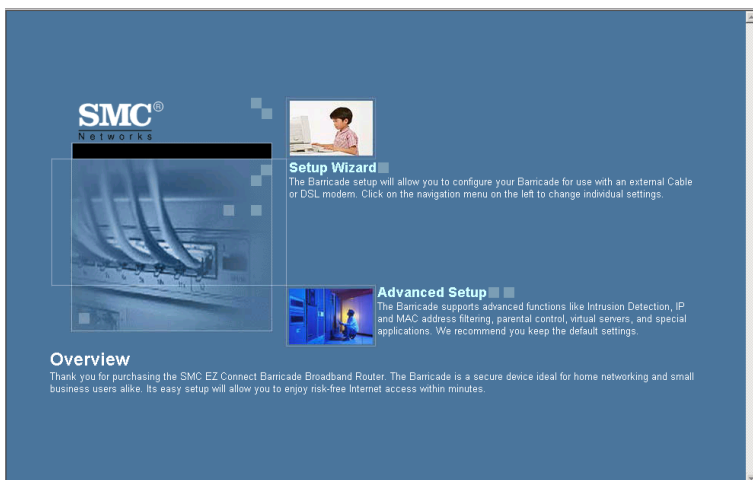
To access the Router’s management interface, enter the Router IP address in your Web browser

<http://192.168.2.1>. Then click LOGIN.
(By default, there is no password.)



A screenshot of the router's login screen. It has a blue header with the text 'LOGIN USER PASSWORD'. Below this is a light blue box with the title 'Login Screen'. Inside the box, there is a label 'Password:' followed by a text input field. At the bottom of the box are two buttons: 'LOGIN' and 'CANCEL'.

The home page displays the Setup Wizard and Advanced Setup options.



Navigating the Web Browser Interface

The Router's management interface features a Setup Wizard and an Advanced Setup section. Use the Setup Wizard if you want to quickly set up the Router 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, and 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.

Note: To ensure proper screen refresh after a command entry, ensure 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."

Setup Wizard

Time Zone

Click on the Setup Wizard picture. The first item in the Setup Wizard is Time Zone setup.

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, and click NEXT.



Broadband Type

Select the type of broadband connection you have.

For a cable modem connection see the following page. For a Fixed-IP xDSL connection see “Fixed-IP xDSL” on page 32, and for a PPPoE xDSL connection, see “PPPoE” on page 32.



Cable Modem

After selecting Cable Modem as the Broadband Type, a message will appear stating that your data has been successfully saved.

Note: Select Home to return to the home page, then select Advanced Settings/WAN to configure the required parameters. (See “WAN” on page 36.)

Configuring the Wireless Barricade g Router

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. Click FINISH to complete the setup.

IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Gateway IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
DNS IP Address	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Subnet Mask	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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.

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

Leave the Maximum Transmission Unit (MTU) at the default value (1454) 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)

Enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again. Click FINISH to complete the setup

Advanced Setup

Use the Web management interface to define system parameters, manage and control the Router and its ports, or monitor network conditions. The following table outlines the selections available from this program.

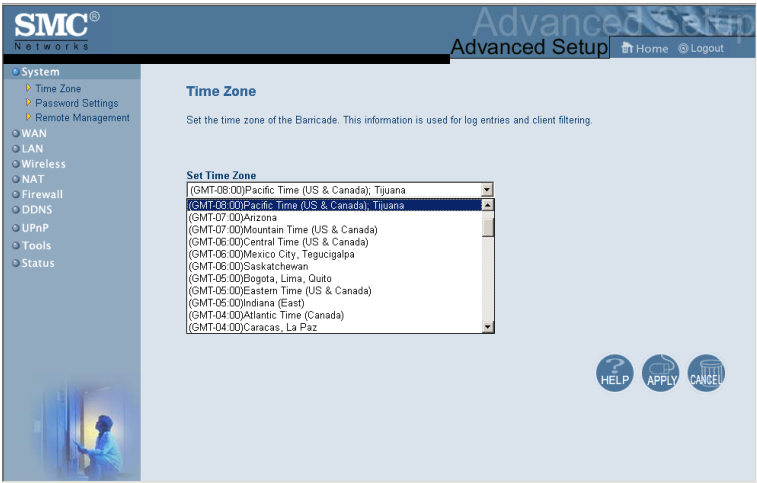
Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the Router remotely.
WAN	Specifies the Internet connection type: <ul style="list-style-type: none"> • Dynamic IP host configuration and the physical MAC address of each media interface • PPPoE configuration • PPTP • Static IP and ISP gateway address • Specifies DNS servers to use for domain name resolution.
LAN	Sets the TCP/IP configuration of the Router's LAN interface and all DHCP clients.
NAT	Shares a single ISP account with multiple users, sets up virtual servers.
Wireless	Configures the radio frequency, SSID, and encryption for wireless communications.
Firewall	Configures a variety of security and specialized functions, including: Access Control, Hacker Prevention, and DMZ.
DDNS	Dynamic DNS provides users on the Internet with a method to tie their domain name(s) to computers or servers.
UPnP	With Universal Plug and Play, a device can automatically dynamically join a network, obtain an IP address, communicate its capabilities, and learn about the presence and capabilities of other devices. Devices can then directly communicate with each other. This further enables peer to peer networking.
Tools	Contains options to backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.

Configuring the Wireless Barricade g Router

Menu	Description
Status	<p>Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and Firewall information.</p> <p>Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number.</p> <p>Shows the security and DHCP client log.</p>

System

Time Zone



Sets the time zone for the Router. This information is used for log entries and client access control.

Password Settings

The screenshot shows the 'Password Settings' page in the SMC Networks Advanced Setup interface. The left sidebar contains a menu with 'System' expanded, showing options like Time Zone, Password Settings (highlighted), Remote Management, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Password Settings' and includes the instruction 'Set a password to restrict management access to the Barricade.' Below this, there are three fields: 'Current Password', 'New Password', and 'Re-Enter Password for Verification'. To the right of these fields is an 'Idle Time Out' setting, currently set to 10 minutes, with a note '(Idle Time =0 : NO Time Out)'. At the bottom right, there are three buttons: 'HELP', 'APPLY', and 'CANCEL'.

Use this menu to restrict access based on a password. By default, there is no password. For security you should assign one before exposing the Router to the Internet.

Passwords can contain from 3–12 alphanumeric characters and are not case sensitive.

Note: If your password is lost, or you cannot gain access to the user interface, press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults. (The default is no password.)

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

Configuring the Wireless Barricade g Router

Remote Management

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System (Time Zone, Password Settings, Remote Management), WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The 'Remote Management' option is selected. The main content area is titled 'Remote Management' and contains the following text: 'Set the remote management of the Barricade. If you want to manage the Barricade from a remote location (outside of the local network), you must also specify the IP address of the remote PC.' Below this text is a form with a 'Host Address' field containing four input boxes, each with a '0' inside, and an 'Enabled' checkbox. At the bottom right of the form are three buttons: 'HELP', 'APPLY', and 'CANCEL'.

Remote Management allows a remote PC to configure, manage, and monitor the Router using a standard Web browser. Check Enable and enter the IP address of the remote host. Click APPLY.

Note: If you specify 0.0.0.0 as this IP address, any host can manage the Router.

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 screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE, PPTP, Static IP, DNS, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Dynamic IP" and includes a descriptive paragraph: "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 Blamcade. 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." Below this text are two input fields: "Host Name" (a text box) and "MAC Address" (a segmented box with the default value 00 - E0 - 29 - BF - 69 - F0). A "Clone Mac Address" button is positioned below the MAC Address field. At the bottom right of the page are three circular buttons labeled "HELP", "APPLY", and "CANCEL".

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.

Configuring the Wireless Barricade g Router

Point-to-Point Over Ethernet (PPPoE)

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing options: Dynamic IP, PPPoE (highlighted), Static IP, and DNS. 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.' Below this text is a sub-header 'Use PPPoE Authentication' followed by a form with the following fields: 'User Name' (text input), 'Password' (text input), 'Please retype your password' (text input), 'Service Name' (text input), 'MTU' (set to 1454, with a note '(1440 <= MTU Value <= 1492)'), 'Maximum Idle Time' (set to 10), and a checked 'Auto-reconnect' checkbox. At the bottom right of the interface are three buttons: '? HELP', 'APPLY', and 'CANCEL'.

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.

The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1454) 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 minutes)

Point-to-Point Tunneling Protocol (PPTP)

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing sub-options: Dynamic IP, PPPoE, PPTP (which is highlighted in yellow), Static IP, and DNS. The main content area is titled 'PPTP' and contains a descriptive sentence: 'Point-to-Point Tunneling Protocol is a common connection method used for xDSL connections in Europe.' Below this is a configuration form with the following fields: IP Address (0.0.0.0), Subnet Mask (0.0.0.0), Default Gateway (0.0.0.0), User ID (empty), Password (empty), PPTP Gateway (0.0.0.0), and Idle Time Out (10 min). At the bottom right of the form are three buttons: HELP, APPLY, and CANCEL.

IP Address	0	0	0	0
Subnet Mask	0	0	0	0
Default Gateway	0	0	0	0
User ID				
Password				
PPTP Gateway	0	0	0	0
Idle Time Out	10	(min)		

Point-to-Point Tunneling Protocol (PPTP) can be used to join different physical networks using the Internet as an intermediary. 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.

Enter the assigned IP address, subnet mask and default gateway IP address (usually supplied by your ISP), and then the PPTP User ID, Password and PPTP Gateway IP address.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the PPTP connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, it will be dropped. (Default: 10 minutes)

Configuring the Wireless Barricade g Router

Static IP Address

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

Dynamic IP

PPPoE

PPTP

Static IP

DNS

LAN

Wireless

NAT

Firewall

DDNS

UPnP

Tools

Status

Static IP

If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided.

Has your Service Provider given you an IP address and Gateway address?

IP address assigned by your Service Provider :

Subnet Mask :

Service Provider Gateway Address :

HELP

APPLY

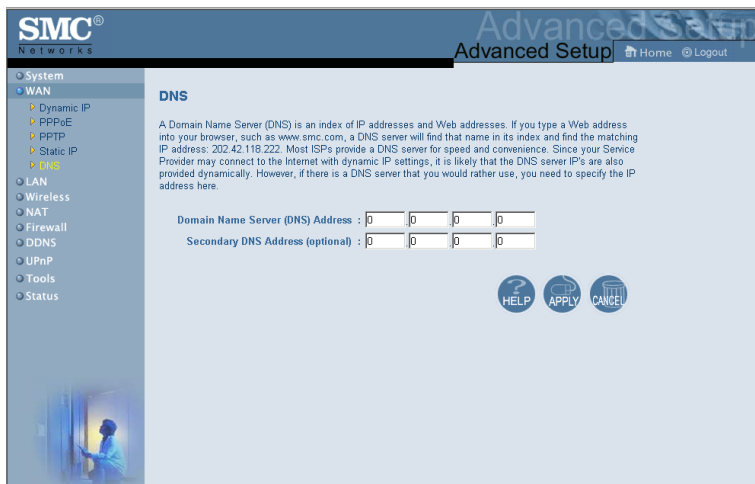
CANCEL

If your Internet Service Provider has assigned a fixed IP address, enter the assigned address and subnet mask for the Router, 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.

40

DNS



The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, Firewall, DDNS, UPnP, Tools, and Status. Under WAN, options include Dynamic IP, PPPoE, PPPoE, Static IP, and a highlighted option. The main content area is titled 'DNS'. It contains a paragraph explaining DNS: 'A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 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 this text are two input fields: 'Domain Name Server (DNS) Address' and 'Secondary DNS Address (optional)'. Each field consists of four small boxes for entering the octets of an IP address. At the bottom right of the form are three circular buttons labeled 'HELP', 'APPLY', and 'CANCEL'. A small image of a person at a computer is visible in the bottom left corner of the interface.

SMC® Networks Advanced Setup Home Logout

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 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.

Domain Name Server (DNS) Address :

Secondary DNS Address (optional) :

HELP APPLY CANCEL

Domain Name Servers map numerical IP addresses to the equivalent domain name (e.g., www.smc.com). Your ISP should provide the IP address of one or more domain name servers. Enter those addresses in this screen.

Configuring the Wireless Barricade g Router

LAN

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN (selected), Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'LAN Settings' and includes a descriptive paragraph about DHCP. Below this is the 'LAN IP' section with fields for IP Address (192.168.2.1), IP Subnet Mask (255.255.255.0), and a DHCP Server toggle set to 'Enabled'. The 'Lease Time' is set to 'One Week'. The 'IP Address Pool' section includes fields for Start IP (192.168.2.100), End IP (192.168.2.199), and a Domain Name field.

SMC® Networks Advanced Setup Home Logout

LAN Settings

You can enable DHCP to dynamically allocate IP addresses to your client PCs, or configure filtering functions based on specific clients or protocols. The Barricade must have an IP address for the local network.

LAN IP

IP Address: 192 . 168 . 2 . 1

IP Subnet Mask: 255 255 255 0

DHCP Server: ☒ Enabled ☐ Disabled

Lease Time: One Week

IP Address Pool

Start IP: 192 . 168 . 2 . 100

End IP: 192 . 168 . 2 . 199

Domain Name:

- **LAN IP** – Use the LAN menu to configure the LAN IP address for the Router and to enable the DHCP server for dynamic client address 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). Once this start IP address has been assigned, IP addresses running from 192.168.2.100 to 192.168.2.199 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.

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.

Wireless

To configure the Router as a wireless access point for wireless clients (either stationary or roaming), all you need to do is define the radio channel, the Service Set identifier (SSID), and encryption options.

Channel and SSID

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless (selected), NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Channel and SSID'. It includes a descriptive paragraph: 'This page allows you to define SSID, Transmission Rate, Basic Rate and Channel ID for wireless connection. In the wireless environment, the Baramcade can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.' Below this are four configuration fields: ESSID (text input with 'default'), Wireless Mode (dropdown menu with '11g Only' selected), Transmission Rate (dropdown menu with 'Fully Automatic' selected), and Channel (dropdown menu with '9' selected). At the bottom right are three circular buttons: HELP, APPLY, and CANCEL.

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

ESSID: The Service Set ID. This should be set to the same value as other wireless devices in your network.

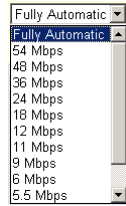
Note: The SSID is case sensitive and can consist of up to 32 alphanumeric characters.

Wireless Mode: Set the communication mode for the Router. (Default: 11g only.)

A close-up of the 'Wireless Mode' dropdown menu. It shows three options: '11g Only' (highlighted), 'Mixed (11b+11g)', and '11g Only'.

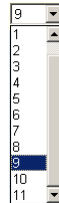
Configuring the Wireless Barricade g Router

Transmission Rate: Set the data rate transmitted from the Router. The lower the data rate, the longer the transmission distance. (Default: Fully Automatic.)



A dropdown menu for Transmission Rate. The top option is 'Fully Automatic'. Below it is a scrollable list of data rates: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 11 Mbps, 9 Mbps, 6 Mbps, and 5.5 Mbps.


Channel: The radio channel through which the Router communicates with PCs in its BSS. (Default: "Auto")



A dropdown menu for Channel. It shows a list of channels from 1 to 11. Channel 9 is currently selected and highlighted in blue.

Note: The available channel settings are limited by local regulations.

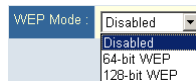
Encryption



The screenshot shows the 'Advanced Setup' page for an SMC Networks router, specifically the 'Encryption' section. On the left is a navigation menu with options: System, WAN, LAN, Wireless (selected), Channel and SSID, Encryption (sub-selected), NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area has the title 'Encryption' and a description: 'Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Barricade and wireless client devices to use encryption. Do you want to use encryption?'. Below this is a 'WEP Mode' dropdown menu set to 'Disabled'. At the bottom right are three circular buttons: HELP, APPLY, and CANCEL.

Advanced Setup

If you are transmitting sensitive data across wireless channels, you should enable Wired Equivalent Privacy (WEP) encryption.



Encryption requires you to use the same set of encryption/decryption keys for the Router and all of your wireless clients. You can choose between standard 64-bit or the more robust 128-bit encryption.

You may automatically generate encryption keys or manually enter the keys. For automatic 64-bit security, enter a passphrase and click Generate. Four keys will be generated (as shown below). Choose a key from the dropdown list or accept the default key. Automatic 128-bit security generates a single key.

A screenshot of a web-based configuration interface for WEP encryption. At the top, there is a 'WEP Mode' dropdown menu set to '64-bit WEP'. Below this, a text instruction reads: 'Enter a passphrase and click the Generate button, or manually enter a key into the table.' The main section contains a 'Passphrase' input field with a 'Generate' button to its right. Below the passphrase field is a table for key configuration. The table has four rows, labeled 'Key 1:', 'Key 2:', 'Key 3:', and 'Key 4:'. Each row contains five input fields for key characters, each preceded by two asterisks (**). To the right of the 'Key 1' row is a 'Default' label. Below the 'Key 1' row is a 'Key: 1' dropdown menu. At the bottom of the table is a 'Clear All Keys' button. At the bottom right of the interface are three circular buttons: 'HELP' (with a question mark icon), 'APPLY' (with a checkmark icon), and 'CANCEL' (with an 'X' icon).

Configuring the Wireless Barricade g Router

WEP Mode : 128-bit WEP

Enter a passphrase and click the Generate button, or manually enter a key into the table.

Passphrase:	<input type="text"/>	Generate
Key:	<div><div>**</div><div>**</div><div>**</div><div>**</div><div>**</div></div>	
	<div><div>**</div><div>**</div><div>**</div><div>**</div><div>**</div></div>	
	<div><div>**</div><div>**</div><div>**</div></div>	
		Clear Key

?

HELP

APPLY

CANCEL

If you use encryption, configure the same keys used for the Router on each of your wireless clients. Note that Wired Equivalent Privacy (WEP) protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

Network Address Translation (NAT)

From this section you can configure the Address Mapping, 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

Address Mapping

The screenshot shows the SMC Networks Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, Wireless, NAT (selected), Address Mapping (sub-item), Virtual Server, Special Applications, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Address Mapping' and includes a descriptive paragraph: 'Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.' Below this, there is a table with 6 rows for configuring address mappings. Each row contains a 'Global IP' field, a 'Local IP' range field, and a description. The fields are currently empty, showing only the IP address format (e.g., 0.0.0.0).

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

Allows one or more public IP addresses to be shared by multiple internal users. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP.

Configuring the Wireless Barricade g Router

Virtual Server

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless, NAT (selected), Address Mapping, Virtual Server (selected), Special Applications, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'Virtual Server' and contains a descriptive paragraph: '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 Barricade redirects the external service request to the appropriate server (located at another internal IP address).' Below this text is a table for configuring virtual servers.

	Private IP	Private Port	Type	Public Port
1.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
2.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
3.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
4.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
5.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
6.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
7.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
8.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
9.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
10.	192.168.2. <input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

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

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

The more common TCP service ports include:

HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

Special Applications

Some applications, such as Internet gaming, videoconferencing, Internet telephony and others, 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.

Special Applications

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

Note: The range of the Trigger Ports is from 0 to 65535.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7.	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, then enter the ports that the application requires. The ports may be in the format 7, 11, 57, or in a range, e.g., 72-96, or a combination of both, e.g., 7, 11, 57, 72-96.

Popular applications requiring multiple ports are listed in the Popular Applications field. From the drop-down list, choose the application and then choose a row number to copy this data into.

Note: Choosing a row that already contains data will overwrite the current settings.

Configuring the Wireless Barricade g Router

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

Firewall

The Router firewall can provide 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. The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network users.

Access Control

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall (selected), DDNS, UPnP, Tools, and Status. The Firewall section is expanded, showing sub-options: Access Control (selected), MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, and DMZ. The main content area is titled 'Access Control' and contains the following text: 'Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.'

Below the text, there are two settings:

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

The Normal Filtering Table is a table with the following data:

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Normal User	192.168.2.101 ~ 120	WWW, E-mail Sending, HTTPS, PPTP, L2TP	Always Blocking	Edit Delete

Below the table is a link: [Add PC](#). At the bottom right of the interface are three buttons: HELP, APPLY, and CANCEL.

Using this option allows you to specify different privileges based on IP address for the client PCs.

Note: Click on Add PC and define the appropriate settings for client PC services (as shown in the following screen).

Access Control Add PC

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

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

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8001	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

User Define Service

Protocol: ☐ TCP ☐ UDP
 Port Range: ~ , ~ , ~ , ~ , ~

- Scheduling Rule (Ref. Schedule Rule Page): Always Blocking ▾

Configuring the Wireless Barricade g Router

MAC Filtering Table

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

- Access Control
- MAC Filter
- URL Blocking
- Schedule Rule
- Intrusion Detection
- DMZ

DDNS

UPnP

Tools

Status

MAC Filtering Table

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

MAC Address Control :

☐ Yes ☒ No

MAC Filtering Table (up to 32 computers)

ID	MAC Address										
1	00	:	E0	:	29	:	8F	:	69	:	F0
2		:		:		:		:		:	
3		:		:		:		:		:	
4		:		:		:		:		:	
5		:		:		:		:		:	
6		:		:		:		:		:	
7		:		:		:		:		:	
8		:		:		:		:		:	
9		:		:		:		:		:	
10		:		:		:		:		:	
11		:		:		:		:		:	
12		:		:		:		:		:	
13		:		:		:		:		:	

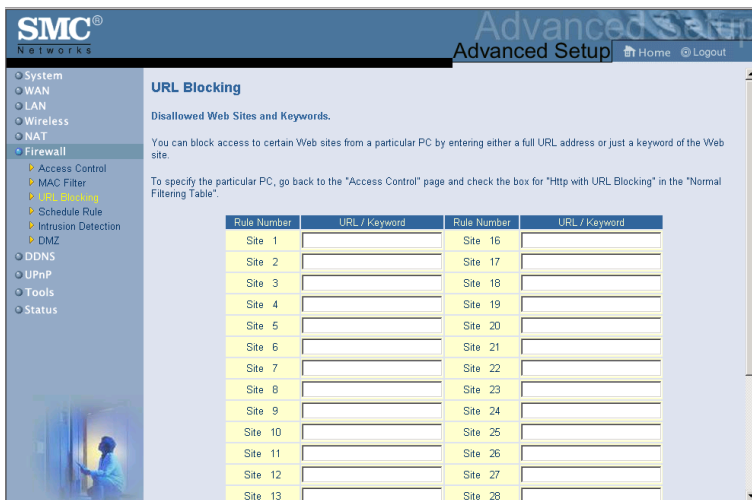
The MAC Filtering feature of the Router allows you to control access to your network to up to 32 clients based on the MAC (Media Access Control) Address of the client machine. This ID is unique to each network adapter. If the MAC address is listed in the table, that client machine will have access to the network.

URL Blocking

To configure the URL Blocking feature, use the table below to specify the websites (www.somesite.com) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in “Access Control” on page 50. To modify an existing rule, click the Edit option next to the rule you want to modify. To create a new rule, click on the Add PC option.

From the Access Control Add PC section check the option for WWW with URL Blocking in the Client PC Service table to filter out the websites and keywords specified below.



URL Blocking

Disallowed Web Sites and Keywords.

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

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

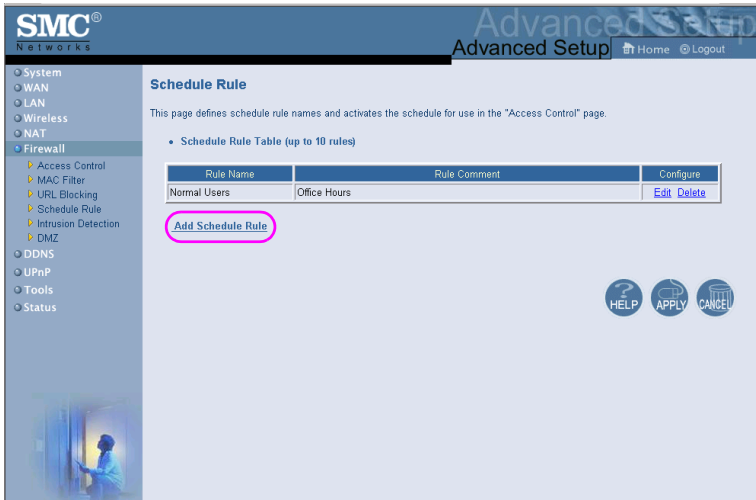
Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	
Site 13		Site 28	

Use the above screen to block access to Web sites or to Web URLs containing the keyword specified in the table.

Configuring the Wireless Barricade g Router

Schedule Rule

The Schedule Rule feature allows you to configure specific rules based on Time and Date. These rules can then be used to configure more specific Access Control.



Enables Schedule-based Internet access control.

1. Click Add Schedule Rule.
2. Define the settings for the schedule rule (as shown on the following screen).
3. Click OK and then click the APPLY button to save your settings.

Edit Schedule Rule

Name:

Comment:

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	00 : 00	00 : 00
Sunday	00 : 00	00 : 00
Monday	08 : 00	17 : 00
Tuesday	08 : 00	17 : 00
Wednesday	08 : 00	17 : 00
Thursday	08 : 00	17 : 00
Friday	08 : 00	17 : 00
Saturday	00 : 00	00 : 00

OK Cancel

Intrusion Detection

Advanced Setup

Home Logout

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall**
 - Access Control
 - MAC Filter
 - URL Blocking
 - Schedule Rule
 - Intrusion Detection**
 - DMZ
- DDNS
- UPnP
- Tools
- Status

Intrusion Detection

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

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

- Intrusion Detection Feature**

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

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

Configuring the Wireless Barricade g Router

The screenshot shows the SMC Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, Wireless, NAT, Firewall (selected), Access Control, MAC Filter, URL Blocking, Schedule Rule, DMZ, DDNS, UPnP, Tools, and Status. The main content area is titled 'Advanced Setup' and includes a 'Home' link and a 'Logout' button. The 'Firewall' section is active, displaying several configuration options:

- When hackers attempt to enter your network, we can alert you by e-mail**
 - Your E-mail Address: [text box]
 - SMTP Server Address: [text box]
 - POP3 Server Address: [text box]
 - User name: [text box]
 - Password: [text box]
- Connection Policy**
 - Fragmentation half-open wait: [10] secs
 - TCP SYN wait: [30] sec
 - TCP FIN wait: [5] sec
 - TCP connection idle timeout: [3600] sec
 - UDP session idle timeout: [30] sec
 - H.323 data channel idle timeout: [180] sec
- DoS Detect Criteria:**
 - Total incomplete TCP/UDP sessions HIGH: [300] session
 - Total incomplete TCP/UDP sessions LOW: [250] session
 - Incomplete TCP/UDP sessions (per min) HIGH: [250] session
 - Incomplete TCP/UDP sessions (per min) LOW: [200] session
 - Maximum incomplete TCP/UDP sessions number from same host: [10]
 - Incomplete TCP/UDP sessions detect sensitive time period: [300] msec
 - Maximum half-open fragmentation packet number from same host: [30]
 - Half-open fragmentation detect sensitive time period: [10000] msec
 - Flooding cracker block time: [300] sec

- **SPI and Anti-DoS firewall protection (Default: Enabled)**
 - The Intrusion Detection Feature limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked with a check in the Stateful Packet Inspection section.
- **RIP Defect (Default: Enabled)** – If an RIP request packet is not replied to by the Router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets accumulating.
- **Discard Ping from WAN (Default: Disabled)**
 - Prevents a PING on the Router's WAN port from being routed to the network.

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

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

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

- **When hackers attempt to enter your network, we can alert you by e-mail** – Enter your E-mail address. Specify your SMTP and POP3 servers, user name, and password.
- **Connection Policy** – Enter the appropriate values for TCP/UDP sessions as described in the following table.

Configuring the Wireless Barricade g Router

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

DoS Criteria and Port Scan Criteria

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

Parameter	Defaults	Description
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of newly unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of newly unestablished sessions that will cause the software to <i>stop</i> deleting half-open sessions.
Incomplete TCP/UDP sessions (per min.) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min.) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute. Set this to "0" if no minimum setting is required.
Maximum incomplete TCP/UDP sessions number from same host	10 sessions	Maximum number of incomplete TCP/UDP sessions from the same host.

Parameter	Defaults	Description
Incomplete TCP/UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	1sec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 sec	Length of time from detecting a flood attack to blocking of the attack.

DMZ

SMC® NETWORKS Advanced Setup

Home Logout

DMZ(Demilitarized Zone)

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

Enable DMZ: ☐ Yes ☒ No

Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

Public IP Address	Client PC IP Address
1. 10.1.28.90	192.168.2.0
2.	192.168.2.0
3.	192.168.2.0
4.	192.168.2.0
5.	192.168.2.0
6.	192.168.2.0
7.	192.168.2.0
8.	192.168.2.0

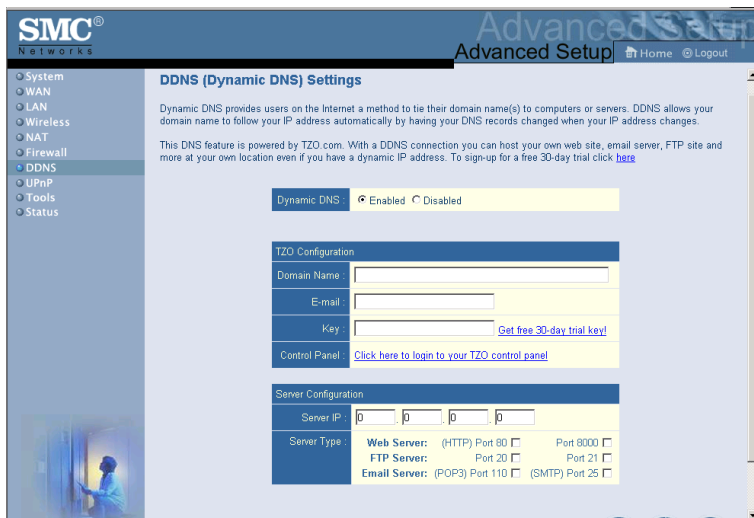
HELP APPLY CANCEL

If you have a client PC that cannot run an Internet application properly from behind the firewall, then you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ host to this screen. Adding a client to the DMZ

Configuring the Wireless Barricade g Router

(Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

DDNS (Dynamic DNS) Settings



SMC® Networks Advanced Setup | Home | Logout

DDNS (Dynamic DNS) Settings

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

This DNS feature is powered by TZO.com. With a DDNS connection you can host your own web site, email server, FTP site and more at your own location even if you have a dynamic IP address. To sign-up for a free 30-day trial click [here](#)

Dynamic DNS: ☒ Enabled ☐ Disabled

TZO Configuration

Domain Name:

E-mail:

Key: [Get free 30-day trial key!](#)

Control Panel: [Click here to login to your TZO control panel](#)

Server Configuration

Server IP:

Server Type:

Web Server: (HTTP) Port 80 <input type="checkbox"/>	Port 8000 <input type="checkbox"/>
FTP Server: Port 20 <input type="checkbox"/>	Port 21 <input type="checkbox"/>
Email Server: (POP3) Port 110 <input type="checkbox"/>	(SMTP) Port 25 <input type="checkbox"/>

Domain Name – A series of alphanumeric strings separated by periods, that is the address of a the Router network connection and that identifies the owner of the address.

Dynamic DNS provides users on the Internet with 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 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).

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

UPnP (Universal Plug and Play) Setting



Enable UPnP by checking ON in the screen above. UPnP allows the device to automatically:

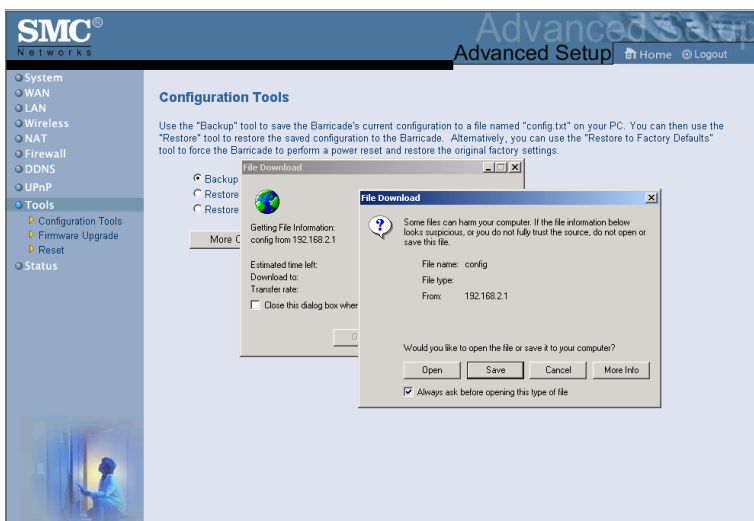
- dynamically join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices. (Default: OFF)

Configuring the Wireless Barricade g Router

Tools

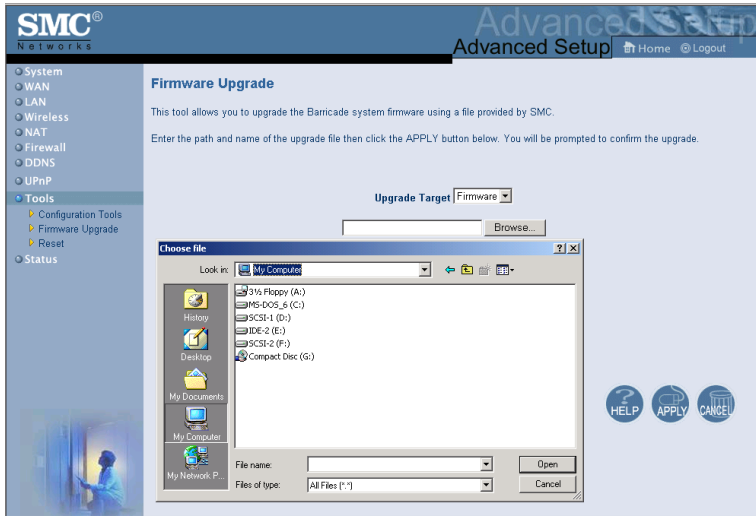
Use the Tools menu to backup the current configuration, restore a previously saved configuration, restore factory settings, update firmware, and reset the Router.

Tools - Configuration Tools



- Backup – saves the Router's configuration to a file.
- Restore – restores settings from a saved backup configuration file.
- Restore to factory defaults – restores the Router settings back to the factory default original.
- Firmware Upgrade

Tools - Firmware Upgrade



Use this screen to update the firmware or user interface to the latest versions. Download the upgrade file from the SMC Web site (www.smc.com) and save it to your hard drive. In the Upgrade Target field, choose Firmware. Then click Browse to look for the previously downloaded file. Click APPLY. Check the Status page Information section to confirm that the upgrade process was successful.

Configuring the Wireless Barricade g Router

Tools - Reset



Click APPLY to reset the Router. The reset will be complete when the power LED stops blinking.

Note: If you use the Reset button on the front panel, the Router performs a power reset. If the button is held depressed for over five seconds, all the LEDs will illuminate and the factory settings will be restored.

Status

The Status screen displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network.

SMC Networks Advanced Setup Home Logout

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.

Current Time: 03/07/2003 02:27:58 am

INTERNET	GATEWAY	INFORMATION
Cable/DSL: CONNECTED	IP Address: 192.168.2.1	Numbers of DHCP Clients: 1
WAN IP: 10.1.20.90	Subnet Mask: 255.255.255.0	Runtime Code Version: 0.52 (Feb 19 2003 21:14:28)
Subnet Mask: 255.255.252.0	DHCP Server: Enabled	Boot Code Version: V1.2T2
Gateway: 10.1.20.254	Firewall: Enabled	LAN MAC Address: 00-04-E2-78-A6-D6
Primary DNS: 10.1.3.5	UPnP: Disabled	WAN MAC Address: 00-E0-29-8F-69-FD
Secondary DNS: 10.2.3.4	Wireless: Enabled	WLAN MAC Address: 00-00-00-00-00-00
		Hardware Version: 0B
		Serial Num: A307039407

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

Date/Time	Source IP	Destination IP	Port	Protocol	Result
03/07/2003 02:23:27	192.168.2.1	192.168.2.1	80	HTTP	Success
03/07/2003 02:23:25	192.168.2.1	192.168.2.1	80	HTTP	Success
03/07/2003 02:12:52	192.168.2.1	192.168.2.1	80	HTTP	Success
03/07/2003 01:48:48	192.168.2.1	192.168.2.1	80	HTTP	Success
03/07/2003 01:48:21	192.168.2.1	192.168.2.1	80	HTTP	Success
03/07/2003 01:41:52	192.168.2.1	192.168.2.1	80	HTTP	Success
01/01/2002 00:00:17	192.168.2.1	192.168.2.1	80	HTTP	Success
01/01/2002 00:00:09	Can't find				
01/01/2002 00:00:00	DHCP Client				

DHCP Client Log View information on LAN DHCP clients currently linked to the Barricade.

IP	MAC
192.168.2.100	mac=00-20-29-...

The following items are included on this screen:

Section	Description
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, 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.
Save	Click on this button to save the security log file.
Clear	Click on this button to delete the access log.
Refresh	Click on this button to refresh the screen.
DHCP Client Log	Displays information on all DHCP clients on your network.

TROUBLESHOOTING

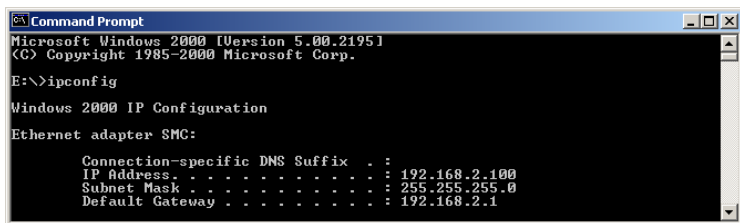
The information outlined in this section describes some useful steps for getting your computer and the Router online.

A. Verify 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. 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



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

E:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter SMC:

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

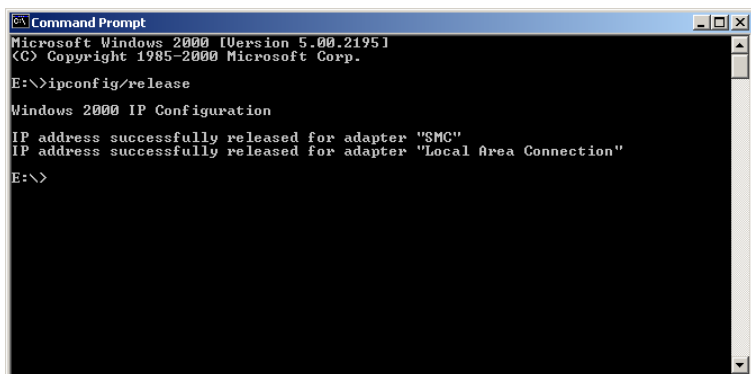
If you are still unable to get an IP Address from the Router, reinstall your network adapter. Please refer to your adapter manual for information on how to do this.

C. 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 Client TCP/IP” on page 12 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`.



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

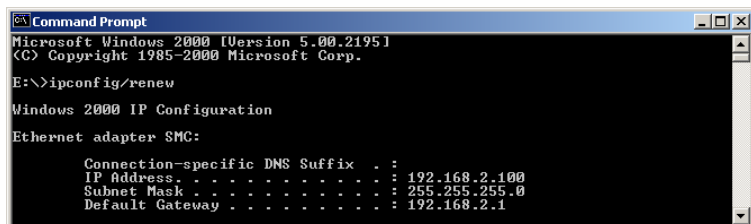
E:\>ipconfig/release

Windows 2000 IP Configuration

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

E:\>
```

3. Then type `ipconfig/renew`.



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

E:\>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter SMC:

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

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

1. Check that the host computer and hub 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 hub/switch port, network card, or cable may be defective.

SPECIFICATIONS

Below is an outline of the Technical Specifications for the SMC2804WBR.

Standards

IEEE 802.3 10BASE-T Ethernet

IEEE 802.3u 100BASE-TX FastEthernet

IEEE 802.11b

IEEE 802.11g draft

WAN Interface

10BASE-T/100BASE-TX

LAN Interfaces

10BASE-T/100BASE-TX

4 RJ-45 ports: LAN data transfer rate is up to 10/20Mbps (10BASE-T half/full duplex) or 100/200Mbps (100BASE-TX with half/full duplex)

Antenna

2 Detachable Antennas with Reversed SMA Connectors

Management

Browser-based management

Both DHCP Server and Client provided

Advanced Features

Dynamic IP Address Configuration – DHCP, DNS

Firewall – Access Control, hacker prevention, logging

Virtual Server via NAT & NAPT

Virtual Private Network – PPTP, L2TP, IPSec pass-through

Intrusion Detection, Email Alerts, Parental Control

Indicator Panel

Power, WLAN, WAN (Link, Activity), LAN (Link/Activity, 10/100 Mbps)

Dimensions

130 x 85 x 32 mm (5.12 x 3.35 x 1.26 in.)

Weight

370 g (13.05 oz)

Specifications

Input Power

9 V, 1 A

Maximum Current

0.04 A RMS max. @ 110V/240V

Power Consumption

5 Watts max. @ 100-240 VAC

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 854-859 TELNET, RFC 1321 MD5, RFC 1497 BOOTP Extension, RFC 1570 PPP LCP Extension, RFC 1631 NAT, RFC1661 PPP, RFC 1700 Assigned Numbers, RFC 1866 HTML, RFC 1945 HTTP, RFC 1994 CHAP, RFC 2131 DHCP, RFC 2637 PPTP

Temperature

Operating 0 to 40 °C (32 to 104 °F)

Storage -40 to 70 °C (-40 to 158 °F)

Humidity

5% to 95% (noncondensing)

Compliances

CE Mark

Emissions

FCC Class B

VCCI Class B

Industry Canada Class B

EN55022 (CISPR 22) Class B

C-Tick - AS/NZS 3548 (1995) Class B

Immunity

EN 61000-3-2/3

EN 61000-4-2/3/4/5/6/8/11

Safety

CSA/NRTL (UL1950, CSA 22.2.950)

GS (EN60950)

CB (IEC60950)

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 (8:00 AM - 5:30 PM UK Time)

44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:

techsupport@smc.com

european.techsupport@smc-europe.com

Driver updates:

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

World Wide Web:

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

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

For Literature or Advertising Response, Call:

U.S.A. and Canada:	(800) SMC-4-YOU	Fax (949) 679-1481
Spain:	34-93-477-4935	Fax 34-93-477-3774
UK:	44 (0) 118 974 8700	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32	Fax 33 (0) 41 38 01 58
Italy:	39 02 739 12 33	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0	Fax 49 (0) 89 92861-230
Switzerland:	41 (0) 1 9409971	Fax 41 (0) 1 9409972
Nordic:	46 (0) 868 70700	Fax 46 (0) 887 62 62
Northern Europe:	44 (0) 118 974 8700	Fax 44 (0) 118 974 8701
Eastern Europe:	34 -93-477-4920	Fax 34 93 477 3774
Sub Saharan Africa:	27-11 314 1133	Fax 27-11 314 9133
North Africa:	34 93 477 4920	Fax 34 93 477 3774
Russia:	7 (095) 290 29 96	Fax 7 (095) 290 29 96
PRC:	86-10-6235-4958	Fax 86-10-6235-4962
Taiwan:	886-2-2659-9669	Fax 886-2-2659-9666
Asia Pacific:	(65) 238 6556	Fax (65) 238 6466
Korea:	82-2-553-0860	Fax 82-2-553-7202
Japan:	81-3-5645-5715	Fax 81-3-5645-5716
Australia:	61-2-8875-7887	Fax 61-2-8875-7777
India:	91-22-8204437	Fax 91-22-8204443

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



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

Model Number: SMC2804WBR
Revision Number E03003-R01 F 1.0