

Barricade™

Wireless TURBO Cable/DSL Broadband Router

Barricade Turbo 11/22 Mbps Auto-Sensing Wireless Cable/DSL Broadband Router

- Multi-user Internet access via single user account
- EZ 3-Click Installation Wizard
- IEEE 802.11b compliant
- Wireless operation at 22, 11, 5.5, 2, or 1 Mbps
- Integrated 3-port 10/100 Mbps switch
- Configurable parental control
- Stateful Packet Inspection (SPI) and Denial of Service (DoS) support
- Supports a wide variety of Internet applications
- Virtual Private Network (VPN) using PPTP, L2TP, IPsec pass-through
- High Performance and High Security

SMC®
Networks

User Guide

SMC2404WBR

[NEXT - Technical Specifications](#)

Technical Specifications

Standards:

IEEE 802.3 10BaseT Ethernet
IEEE 802.3u 100BaseTX Fast Ethernet
IEEE 802.11b

WAN Interface:

10Base-T/100Base-TX

LAN Interfaces:

10Base-T/100Base-TX
3 RJ-45 ports
LAN data transfer rate is up to 10/20Mbps (10BaseT half/full duplex) or
100/200Mbps (100BaseTX half/full duplex)

Management:

Web-based management

Protocol Support:

TCP/IP, PPTP/L2TP/IPSec Passthrough (VPN)
DNS
SNTP
NAT
HTTP
DHCP
Point-to-Point Protocol
PPP Internet Control Protocol
PPP Authentication Control

Internet Sharing Methods:

Static IP

Dynamic IP

PPPoE

Advanced Features:

Dynamic IP Address Configuration - DHCP, DNS

Firewall - Client Privileges, hacker prevention, logging

Virtual Server via NAT and NAPT

Virtual Private Network - IPsec and PPTP pass-through

Intrusion Detection, Email Alerting, Parental Control

Indicator Panel:

PWR (Power), WLAN (Wireless LAN), WAN (Wide Area Network)

Link Lights - LAN1, LAN2, LAN3 (10/100 lights are solid when linked at 100, and off when linked at 10)

Wireless Data Rates (Auto-Sensing/Automatic Fall-back):

1/2/5.5/11/22Mbps

Data Modulation Techniques:

BPSK (1 Mbps), QPSK (2 Mbps), CCK (5.5/11 Mbps), PBCC (5.5/11/22 Mbps)

Media Access Protocol:

CSMA/CA (Collision Avoidance) with ACK

RF Frequency:

2471 MHz - 2497 MHz (Japan Band)

2400 MHz - 2483 MHz (North America, Europe, and extended Japan Band)

2455 MHz - 2475 MHz (Spain)

2446.5 MHz - 2483.5 MHz (France)

Operating Channel:

11 Channels (US, Canada)

13 Channels (Europe)

14 Channels (Japan)

Wired Equivalent Privacy (WEP) Algorithm:

64/128/256-bit RC4

Input Power:

5V 2.5A

Firmware Upgrade:

Via Web Interface

Warranty:

Limited Lifetime

Technical Support

You can download and upgrade to the latest version of software from SMC's Technical Support site,

http://www.smc.com/index.cfm?action=tech_support_support_tools. For more technical information, please refer to the link listed below or contact SMC Technical Support Department at 1-800-SMC-4YOU.

Complete warranty information for all SMC products is available on SMC's website. Please register this product and upgrade the product warranty at www.smc.com

Cable Modem

Most users who have cable modems are set up for DHCP. These include Internet Service Providers (ISP) such as Comcast, AT&T Broadband and Rogers Cable service. At most, your ISP may have contacted you to register the Media Access Control (MAC) address of your network interface card (NIC) in the machine. A cable modem is used to connect a computer to a cable service that provides Internet access. Cable modems can dramatically increase the bandwidth between the user's computer and the Internet service provider. However, cable service is a shared mode of Internet connectivity, and thus the speed will vary depending on how many people on that cable segment are using the Internet at the same time. The cable modem transmission system (CMTS) is responsible for converting radio frequency (RF) signals into data packets for the Internet.

[Setup Wizard for Cable Connection](#)

DSL Modem

Most users with DSL modems require a username and password in order to log onto the Internet. These include Internet Service Providers (ISP) such as PacBell, Earthlink or Sympatico. The Digital Subscriber Line (DSL) is a technology that increases the digital capacity of PSTN lines. DSL is different from ISDN in that it provides an “always-on” connection. ADSL (Asymmetric-DSL) and SDSL (Symmetric-DSL) are the two main types of DSL service provided.

[Setup Wizard for DSL Connection](#)

Static (Fixed) IP Address

If you have been provided a Fixed IP from your Internet Service Provider, they should have given you the IP Address, Subnet Mask, Gateway, and DNS Addresses. In this case, you can configure your broadband router with a Static IP on the WAN interface. This IP address is constant and the ISP will not change it. If you are unsure of any of the necessary IP Addresses, please contact your ISP before proceeding with the installation of the router.

[Setup Wizard for Static IP Connection](#)

Connecting To Your SMC2404WBR 11/22 Mbps Wireless Broadband Router

There are 3 major segments that you will connect together: Modem to Router to Computer.



Figure 1.0 The picture above illustrates the hardware needed to set up your network. (Shown above from left to right is the SM8002CM and SMC2404WBR. The picture of the monitor symbolizes the connection coming from your router to your computer.)

Step 1: You must connect your computer to the router using the RJ45 cable that came with the router. Then connect the modem to the WAN port of the router using the cable that came with your modem. Make sure that the BNC connection to the cable modem is secure at all times. Plug the appropriate power adapter into the router.

Step 2: Double-check to be sure that the RJ45 connection coming from the modem connects to the WAN port at the back of the router. Once the RJ45 connector is plugged into the WAN port, you should hear it click into the RJ45

port. This will indicate that the connection is firmly attached. Then look at the front of your router, and you will see a WAN LED. If this light is lit, it will indicate that you have a connection coming from your modem. This is vital to successfully establishing an internet connection through the router.

Troubleshooting Tip 1: If this light does not come on, you should check if your cables are firmly inserted. Also try switching cables as well. If the light still does not appear, try using a crossover RJ45 cable.

Step 3: You can plug from ports 1, 2, 3 or 4 into your network card. Double-check to be sure that the RJ45 connection coming from that particular port is firmly inserted into your network card. Once this connection is locked in, you will see a link light on the router indicating that there is a connection between your computer and router.

Troubleshooting Tip 2: If you do not see a link light, make sure that the connection coming from your computer is not loose. Try switching the cables as well.

Troubleshooting Tip 3: Try using a different port on the router if you continue to have problems getting a link light on the first port you have tried. Also check your operating system and verify that your network card is working properly. You can check this through the Device Manager.

Step 4: Now that the link lights indicate all connections are valid, you are ready to begin configuring your PC.

Configuring your Personal Computer (PC)



This section will assist you in configuring your browser and computer settings.

Before you start configuring your PC, make sure that you have properly connected your Modem to the WAN port of the Wireless Barricade Turbo router. The router should then be connected to your computer.

This section will allow you to configure your browser settings for:



[Internet Explorer](#)



[Netscape](#)

If you use any other browser, please consult the help guide on how to configure your browser settings when using a router.

Note: Internet Explorer is a registered trademark of Microsoft and Netscape is a registered trademark of Netscape.

See also:

[Configure TCP/IP - Windows 9x/Me](#)

[Configure TCP/IP - Windows NT](#)

[Configure TCP/IP - Windows 2000](#)

[Configure TCP/IP - Windows XP](#)

Configuring Internet Explorer

Configuring Windows 9x/Me/NT/2000:

This set up will allow you to set up your Internet Explorer (Note: Shown below is Internet Explorer version 5.5) to access SMC's login page with the EZ 3-Click Installation Wizard software. (Note: When configuring your browser to connect to your router, initially, you are not online until you have configured the WAN connection on your router.)

Step 1: Launch your Internet Explorer Browser. Click on “Tools”.



Figure 1.0

Step 2: Click on “Internet Options”.



Figure 1.1

Step 3: This will bring up your Internet Options menu. Now, click on the “Connections” tab.

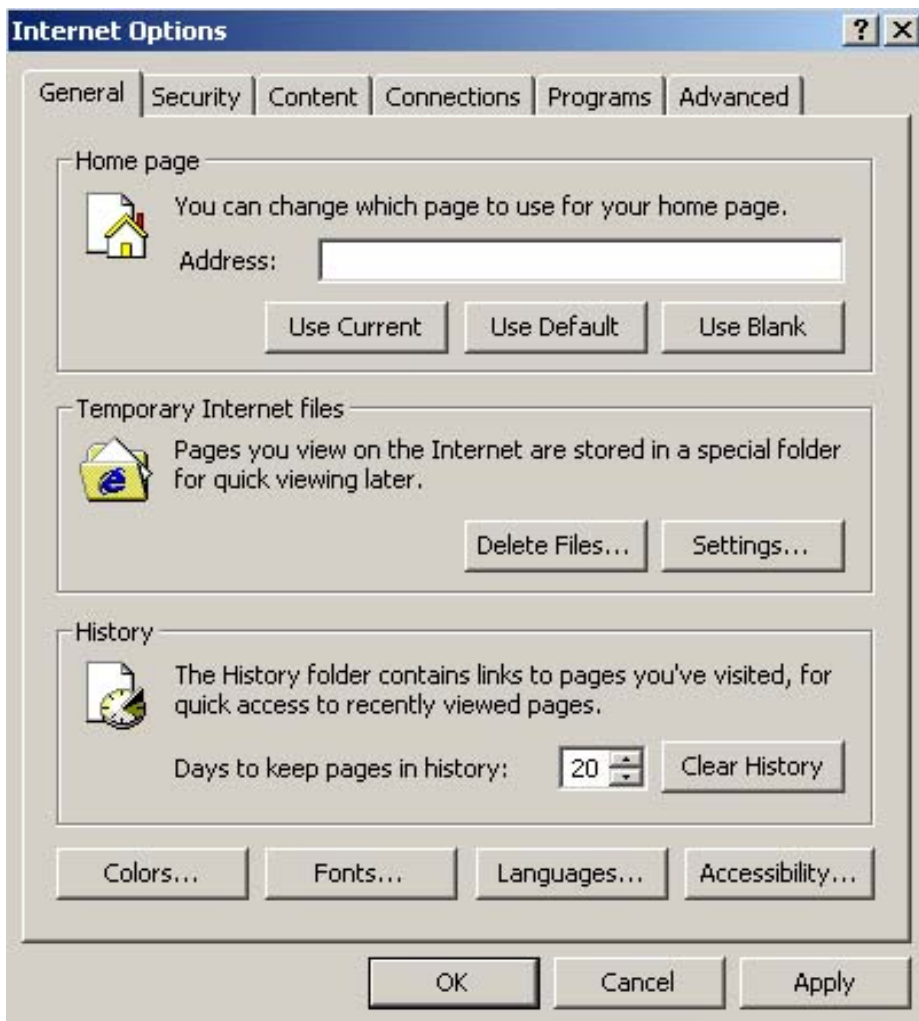


Figure 1.2

Step 4: Select “Never dial a connection”. Now, click on the “LAN Settings” button.



Figure 1.3

Step 5: In the “Local Area Network (LAN) Settings” menu, uncheck all checkbox settings. (Note: Includes un-checking “Automatically detect settings”). Once everything is unchecked, click “OK” to close the “Local Area Network (LAN) Settings” window. This will bring you to the “Internet Options” window, click on “OK” to close that window also.

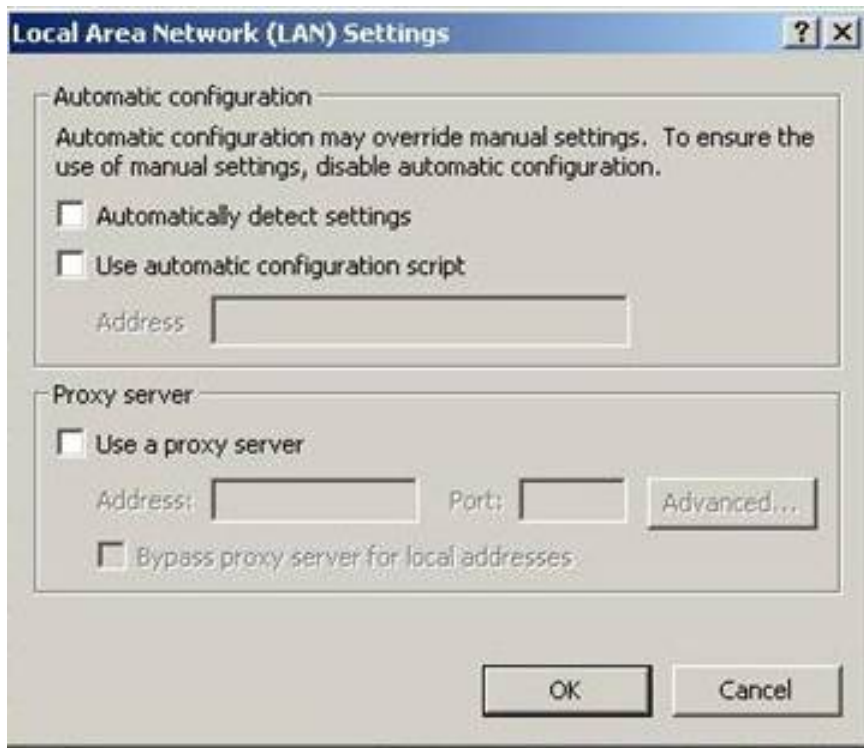


Figure 1.4

See also:

[Configure TCP/IP - Windows 9x/Me](#)

[Configure TCP/IP - Windows NT](#)

[Configure TCP/IP - Windows 2000](#)

[Configure TCP/IP - Windows XP](#)

Configuring Netscape

Step 1: Launch Netscape by double-clicking on the Netscape icon (Note: Shown below is Netscape Navigator version 4.79):



Figure 1.0

Step 2: Click the Edit button on the top menu bar.



Figure 1.1

Step 3: Go to the "Preferences" selection.



Figure 1.2

Step 4: Click on “Advanced” section.

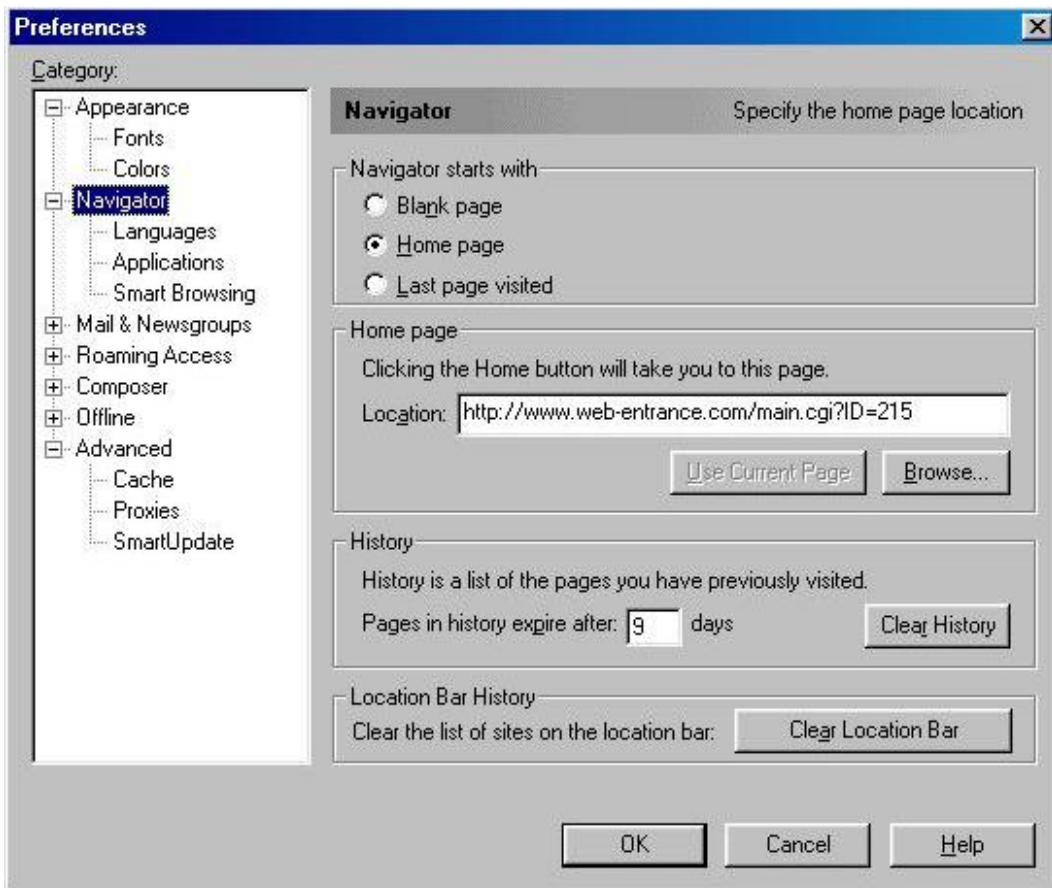


Figure 1.3

Step 5: Click on the “Advanced” section and then click on "Proxies". Make sure that the proxies are disabled and direct connection is selected.

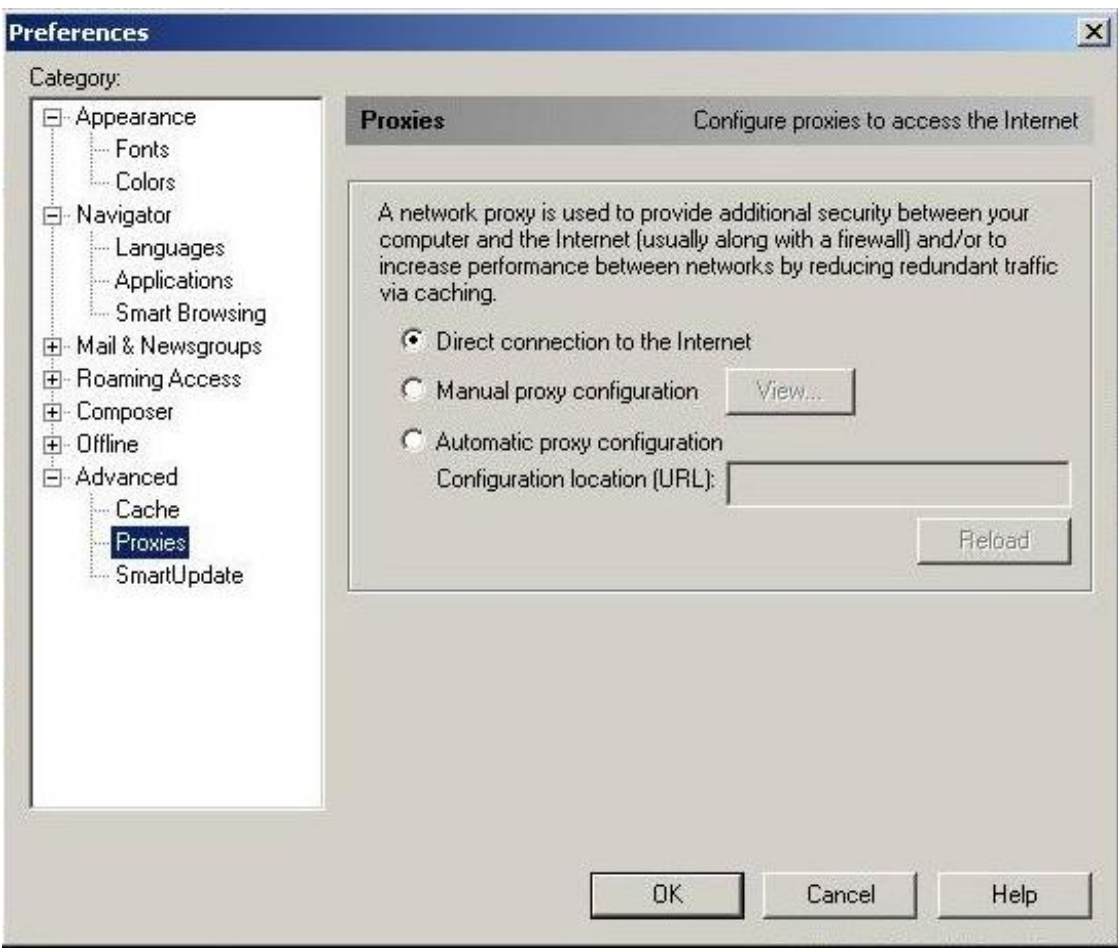


Figure 1.4

Configuring Windows 9X and Millennium

Please click on the icon that corresponds to your Operating System:



Note: Windows 95, 98, and Millennium are registered trademarks of Microsoft.

Installing TCP/IP Protocol: Windows 9x/Me

Step 1: Click on the "Start" button and choose "Settings", and then "Control Panel".



Figure 1.0

Step 2: Double-click the "Network" icon and select the "Configuration" tab in the Network window.



Figure 1.1



Figure 1.2

Step 3: Click the "Add" button to add the TCP/IP network component to your PC.

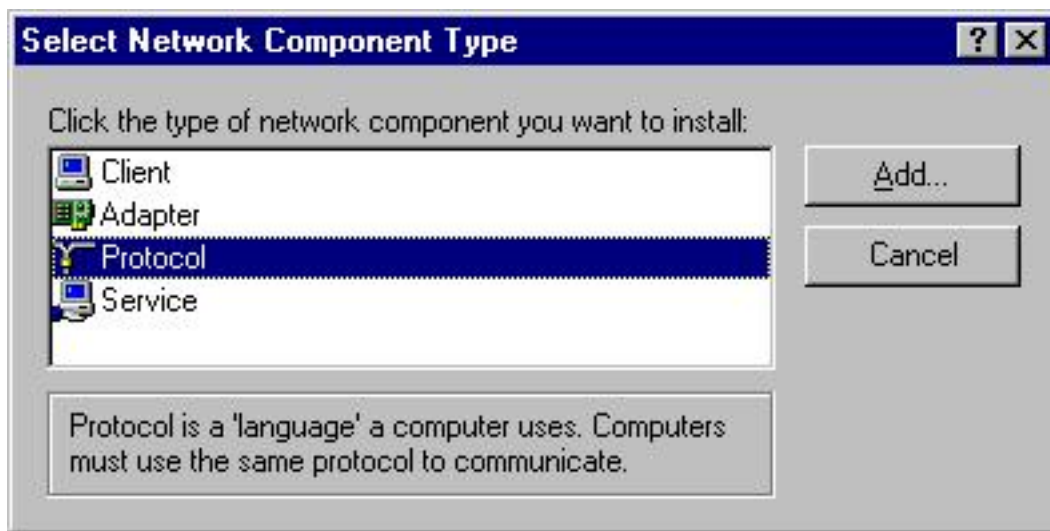


Figure 1.3

Step 4: Double-click "Protocol" to add the TCP/IP protocol.

Step 5: Select the "Microsoft" item in the manufacturer's list. Then choose "TCP/IP" in the Network Protocols. Click the "OK" button to return the Network window.

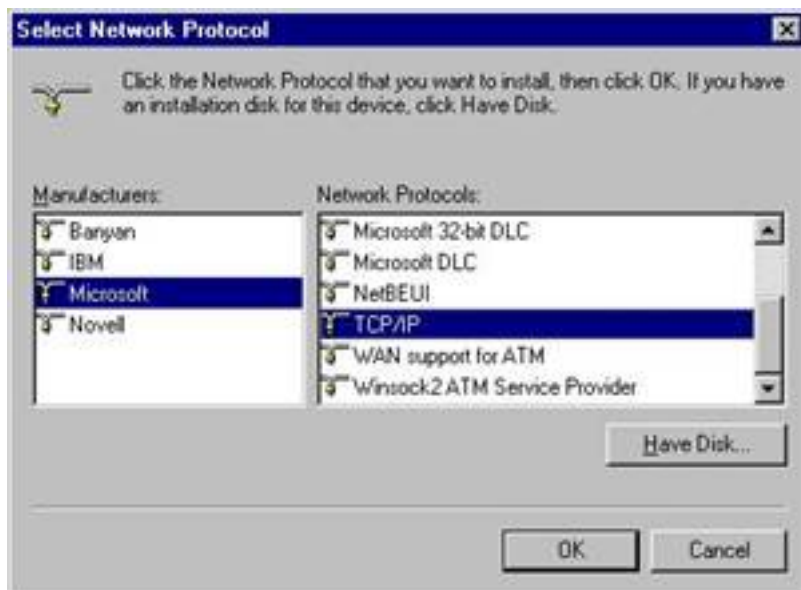


Figure 1.4

Step 6: The TCP/IP Protocol will be listed in the Network window. Click "OK" to complete the install procedure and restart your PC to enable the TCP/IP protocol.

Configuring TCP/IP: Dynamic IP on Windows 9x/Me

Step 1: Click on the "Start" button and choose "Settings", and then click on "Control Panel".



Figure 1.0

Step 2: Double-click the "Network" icon.



Figure 1.1

Step 3: Select the TCP/IP that is bound to the network adapter that you are currently using to plug directly into the Wireless Broadband Router. Click "Properties".



Figure 1.2

Step 4: Select "Obtain an IP address automatically" in the IP Address tab. Make sure that there are no values set under the "Gateway" tab, and choose "Disable DNS" on the "DNS Configuration" tab. These settings will all be automatically configured by the DHCP Services that are built-into the router.



Figure 1.3

Step 5: Press "OK" to save the changes. The system should start copying files. Then press "Yes" when prompted to reboot the system.

Configuring TCP/IP: Static IP for Windows 9x/Me

NOTE: Set up your machine statically **ONLY** if you have already tried the Dynamic IP addressing and you were unable to obtain an IP address. Also, some Windows 9x/ME systems will request that you insert your Windows CD in order to complete the following configuration. Please have this CD ready.

Step 1: Click the "Start" button and choose "Settings", then click "Control Panel".



Figure 1.0

Step 2: Double-click the "Network" icon.



Figure 1.1

Step 3: Select the TCP/IP that is bound to the network adapter that you are currently using to plug directly into the Wireless Broadband Router. Click "Properties".



Figure 1.2

Step 4: Select the Specify an IP option and insert an IP address that is not in the range of the DHCP LAN address. For example, you might want to insert 192.168.2.50 for the IP address if the DHCP LAN address pool is 192.168.2.100 to 192.168.2.199. Then insert 255.255.255.0 for the subnet mask.

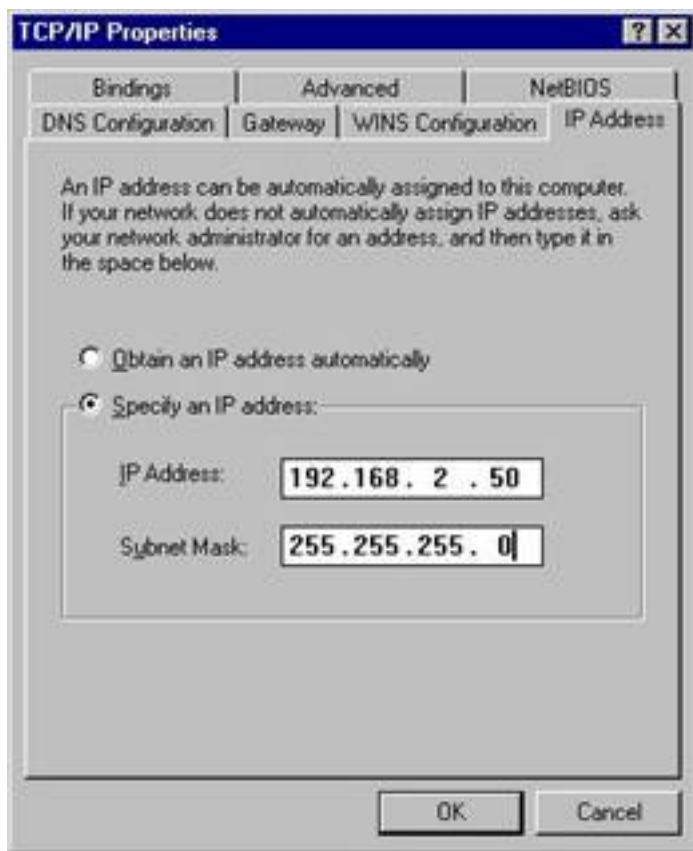


Figure 1.3

Step 5: Click on the Gateway tab and then insert the Wireless Barricade Turbo's IP address, 192.168.2.1, and then press the "Add" option. You should see the gateway IP appear in the "Installed Gateways" section at this point.

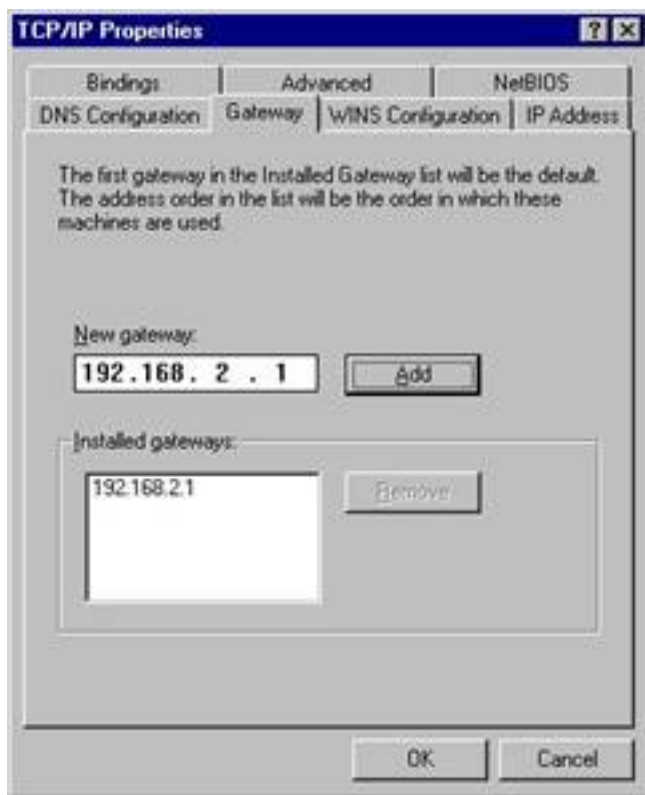


Figure 1.4

Step 6: Click on the DNS Configuration tab and check the Enable option. Insert a host name (it can be any name you choose). Then insert the Wireless Barricade Turbo's IP address, 192.168.2.1, where it says DNS Server Search Order and press "Add". Then click the "OK" button and you may have to click "OK" one more time to save the changes.

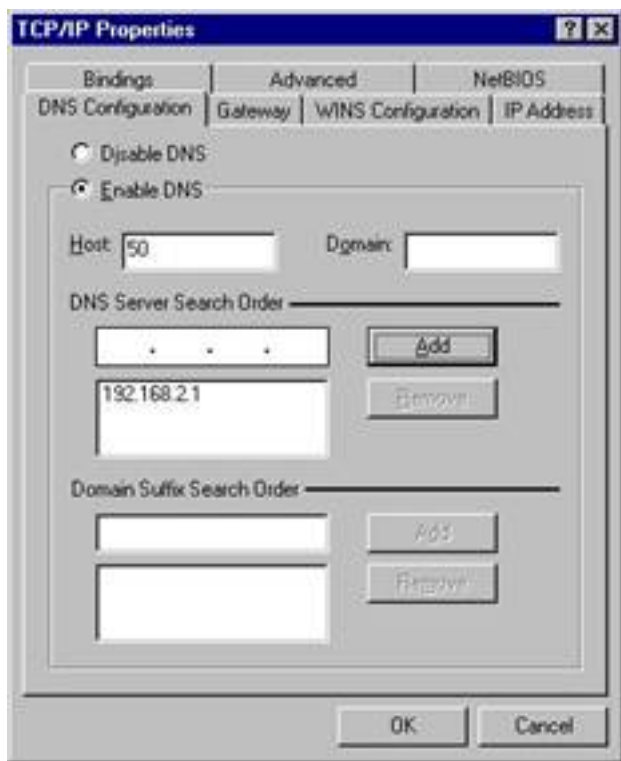


Figure 1.5

Step 7: Reboot the machine when prompted to do so.

Configuring Windows NT/2000/XP

Please click on the icon that corresponds to your Operating System:



Note: Windows NT, 2000 and XP are registered trademarks of Microsoft.

Installing TCP/IP on Windows NT/2000/XP

In NT-based systems, the TCP/IP protocol is automatically configured during the installation of your network interface card (NIC). Simply confirm that this protocol is set up to obtain an IP from the router. See the steps below:

WINDOWS NT

Step 1: Right-click on the Network icon on your desktop, and click "Properties".



Figure 1.0

Step 2: Go to the Protocols tab and verify that TCP/IP is showing in the window. Once your network adapter is installed correctly, this TCP/IP option will allow you to configure the adapter for DHCP or a fixed IP address.



Figure 1.1

WINDOWS 2K/XP

Step 1: Right-click the "Network Places" icon on your desktop and click "Properties".



Figure 1.2

Step 2: Right-click the "Local Area Connection" that refers to the Ethernet adapter that is plugged into the router, and click "Properties".

Step 3: Make sure that there is an "Internet Protocol TCP/IP" option and that it has a check mark beside it. If it is not checked, then you do not have this protocol instead. Check the box and press the "Close" button.

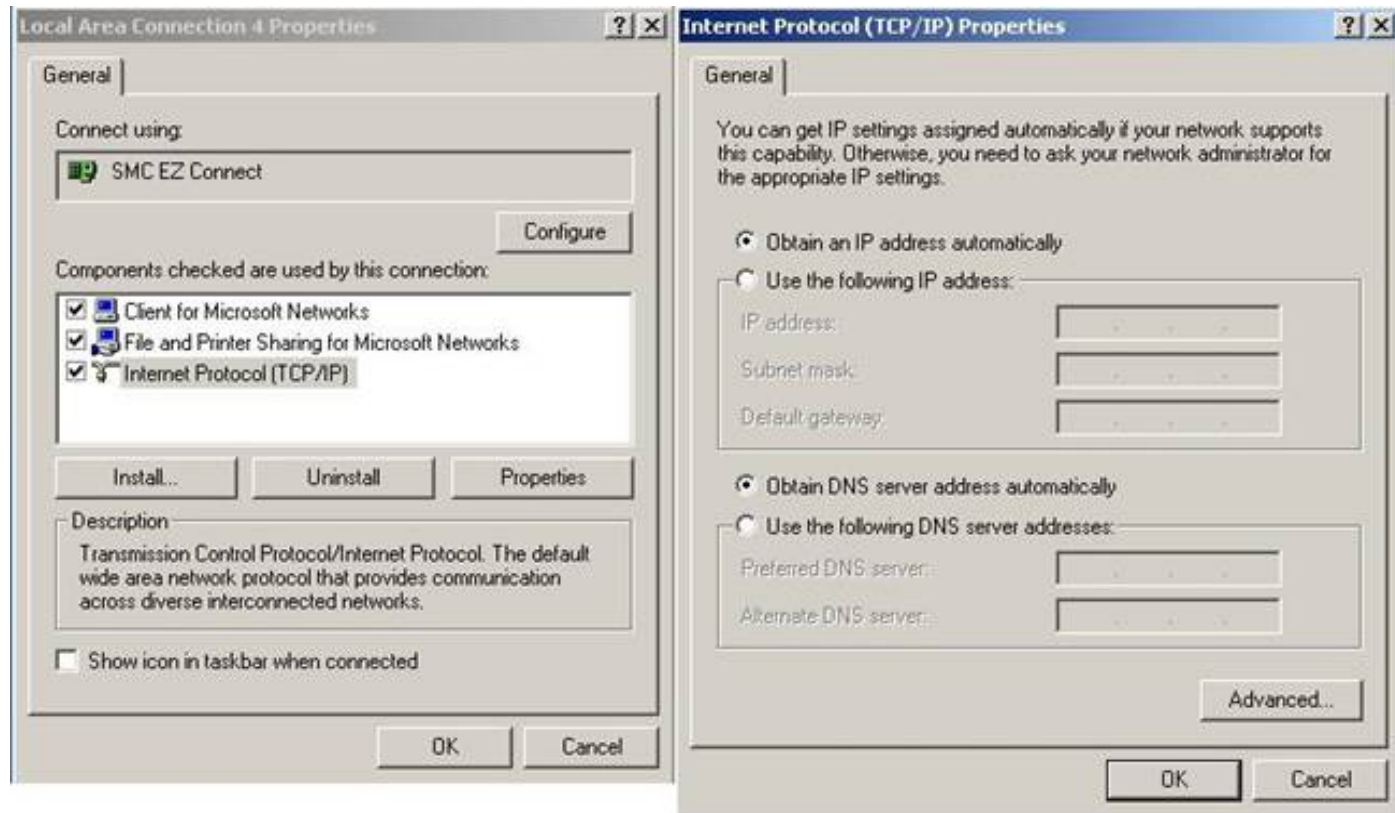


Figure 1.3

Configuring TCP/IP: Dynamic IP on Windows NT

Step 1: Right-click the Network icon on your desktop and click "Properties".



Figure 1.0

Step 2: Go to the Protocols tab and select the TCP/IP Protocol and then click on the "Properties" button. Make sure that they are set to obtain an IP address automatically.



Figure 1.1

Step 3: Go to the DNS tab and make sure that you are set up to obtain DNS automatically as well.

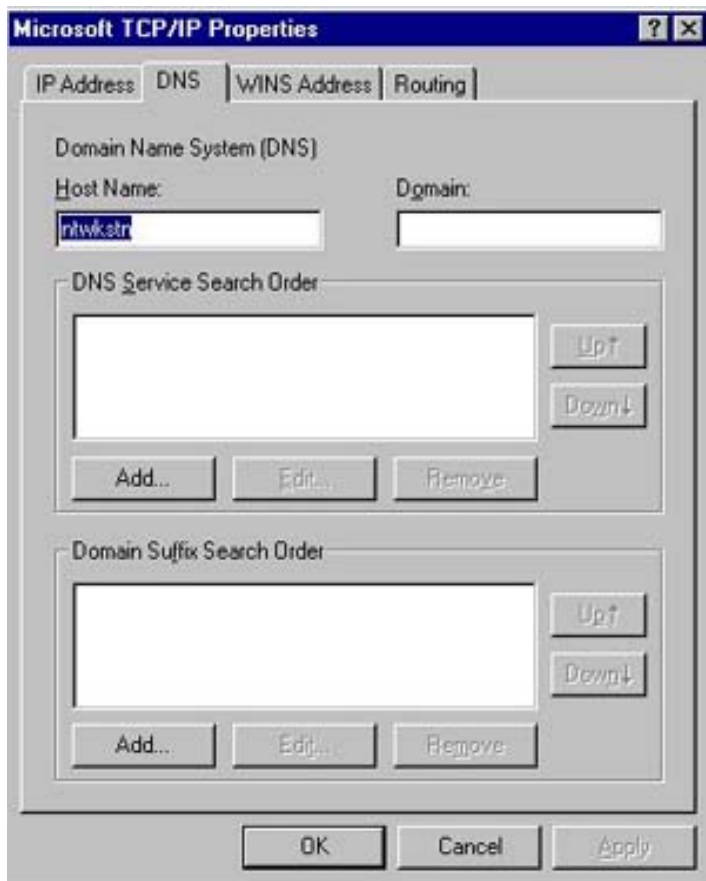


Figure 1.2

Step 4: Click "OK" to close the TCP/IP properties window. Click "OK" again to close the Network properties window.

Configuring TCP/IP: Static IP on Windows NT

Step 1: Right-click the Network icon on your desktop and click "Properties".



Figure 1.0

Step 2: Click on the "Protocols" tab and check the properties of the TCP/IP. Select your adapter from the drop-down menu. Select the Specify an IP option and insert an IP address that is not in the range of the DHCP LAN address. For example, you might want to insert 192.168.2.50 for the IP address if the DHCP LAN address pool is 192.168.2.100 to 192.168.2.199. The subnet mask is 255.255.255.0 and the gateway is 192.168.2.1.

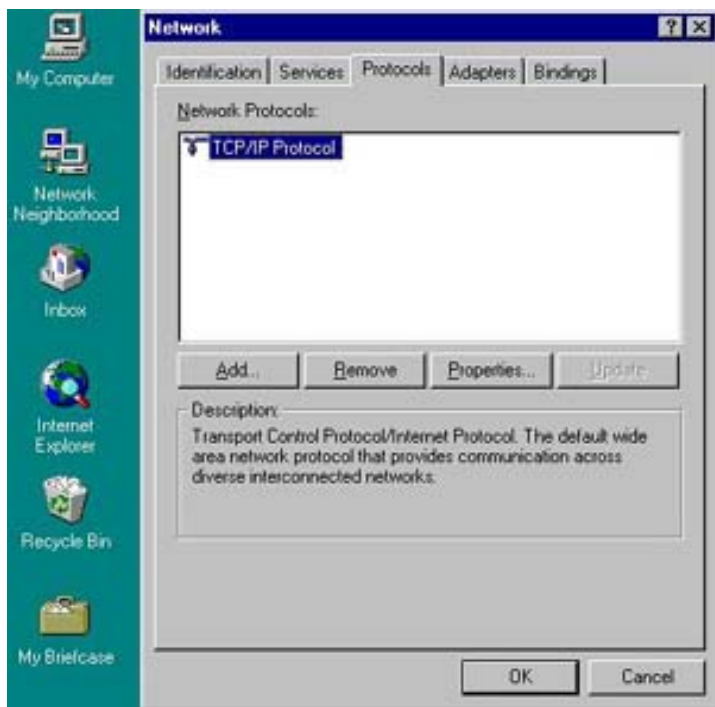


Figure 1.1

Step 3: Click on "Specify an IP address" and then set a static IP address as previously directed. (Note: The IP address in this figure is for illustration purposes only.)



Figure 1.2



Figure 1.3

Step 4: Go to the DNS tab and make sure that the router's IP is listed, 192.168.2.1 and a Hostname is entered. (Note: Your hostname can be any naming scheme you chose your machine to be called unless specified by a System administrator or ISP.)

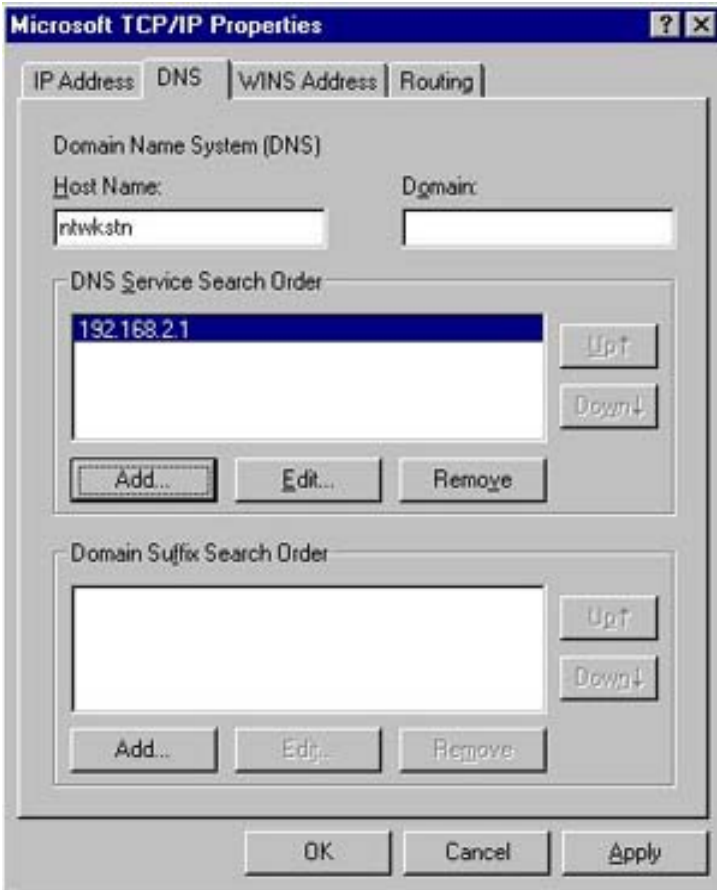


Figure 1.4

Step 5: Click "OK" and click "Close" to continue and save the changes.

Configuring TCP/IP: Dynamic IP on Windows 2000

Step 1: Right-click the "Network Places" icon on your desktop and click "Properties".



Figure 1.0

Step 2: Right-click the "Local Area Connection" that refers to the Ethernet adapter that is plugged into the router, and click "Properties".

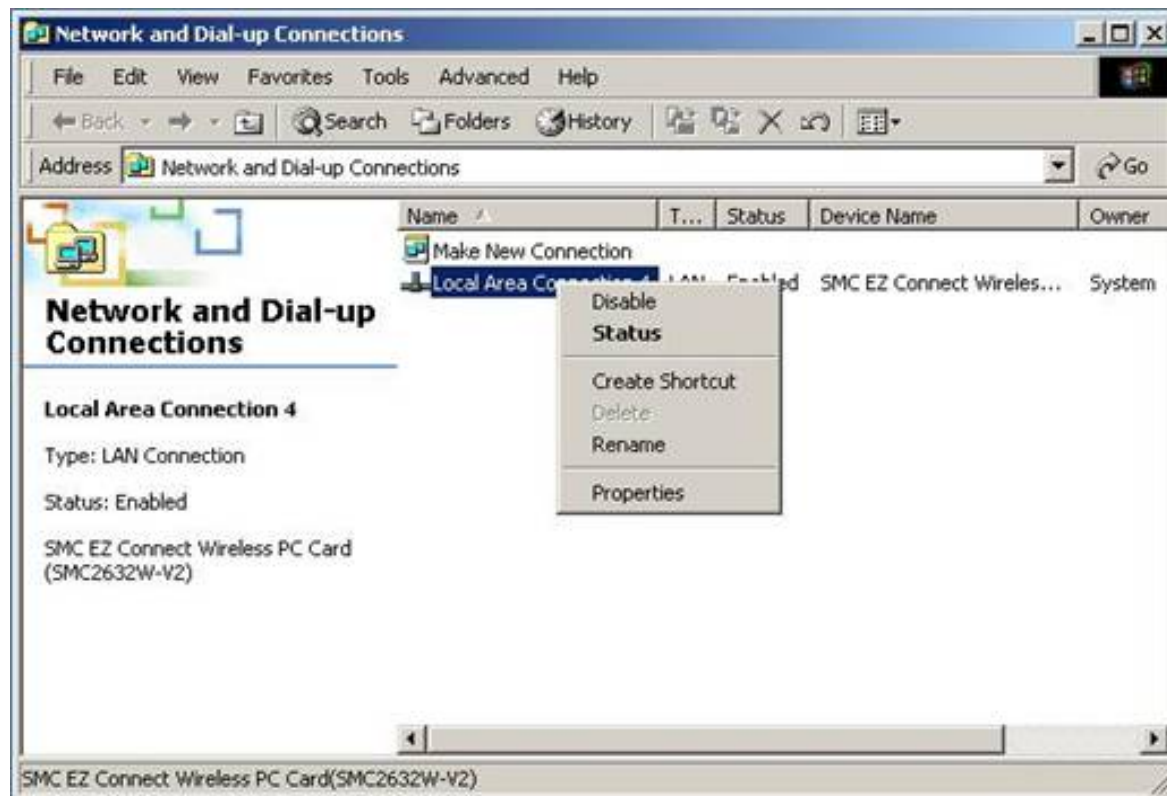


Figure 1.1

Step 3: Click the "Internet Protocol: TCP/IP" option and click "Properties". Then make sure that everything is set to obtain an IP address automatically (including DNS).

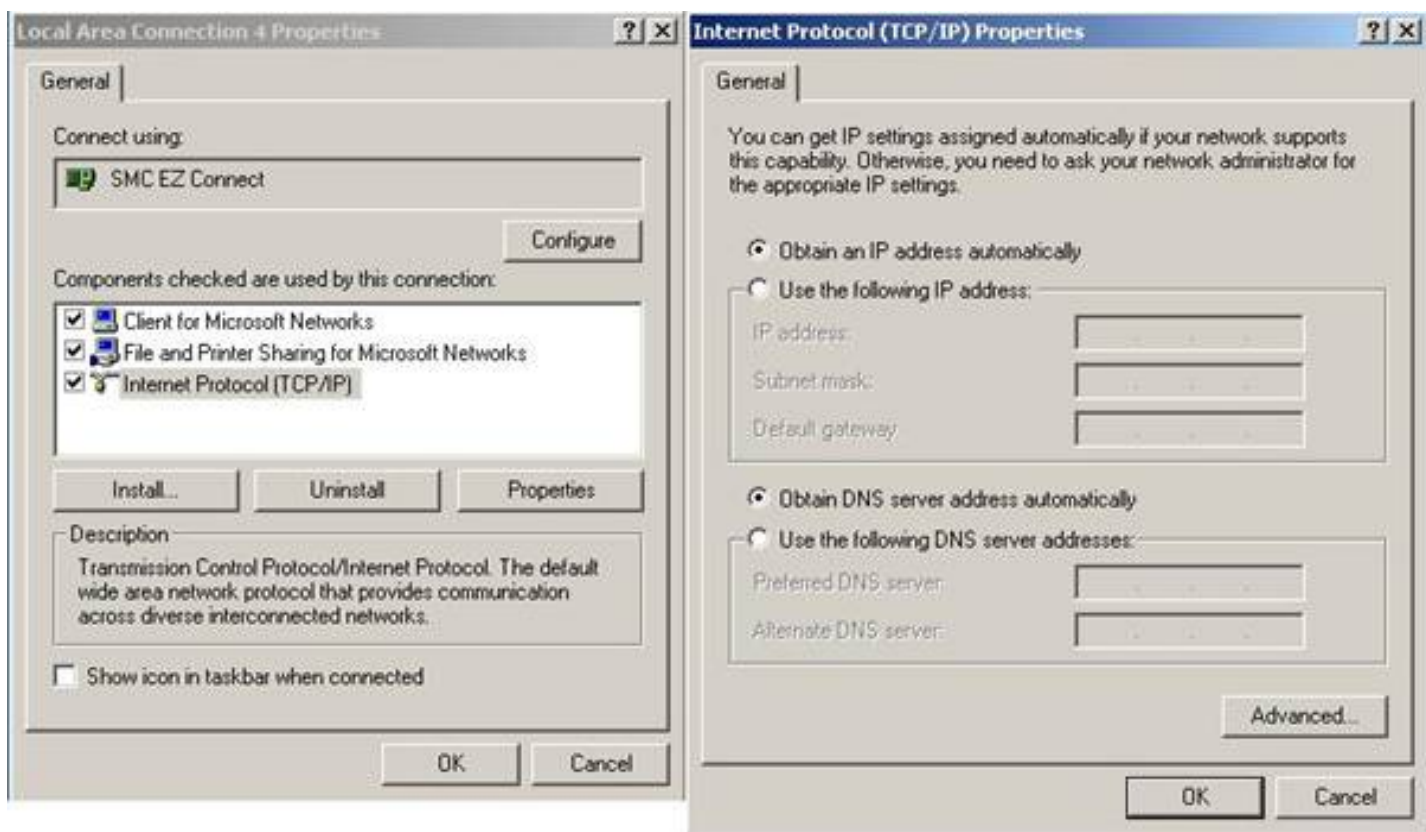


Figure 1.2

Configuring TCP/IP: Static IP on Windows 2000

Step 1: Right-click the "Network Places" icon on your desktop and click "Properties".



Figure 1.0

Step 2: Right-click your Local Area Connection and click "Properties".



Figure 1.1

Step 3: Click "Internet Protocol TCP/IP" and click "Properties". Select the "Use the following IP Address" option and insert an IP address that is not in the range of the DHCP LAN address. For example, you might want to insert 192.168.2.50 for the IP address if the DHCP LAN address pool is 192.168.2.100 to 192.168.2.199. The gateway and preferred DNS server will be 192.168.2.1.

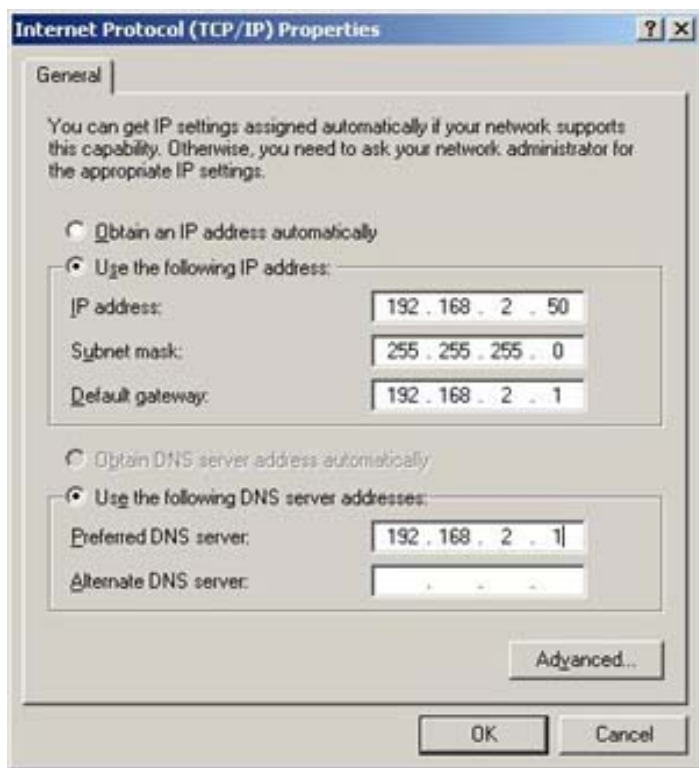


Figure 1.2

Step 4: Click "OK" and click "Close" to continue and save the changes.

Configuring TCP/IP: Dynamic IP on Windows XP

Step 1: Click the "Start" button and choose "Control Panel".

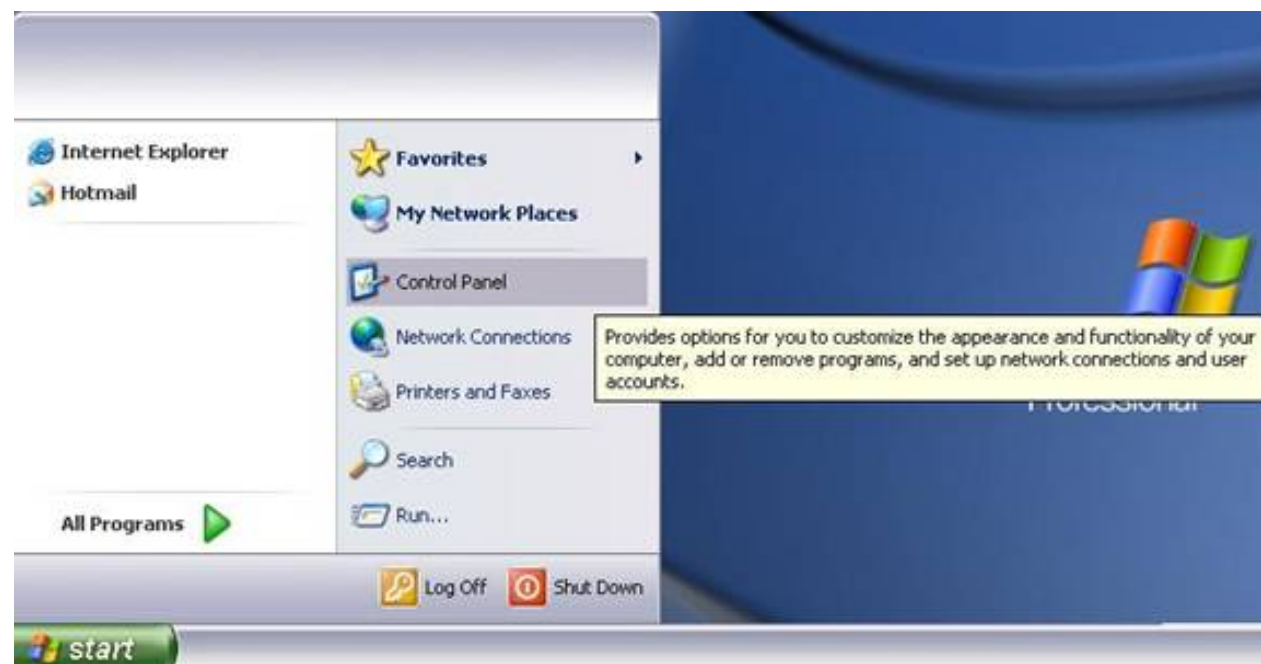


Figure 1.0

Step 2: Double-click the "Network and Internet Connections" option, and then click "Network Connections".



Figure 1.1



Figure 1.2

Step 3: Then right-click the Local Area Connection and click "Properties".

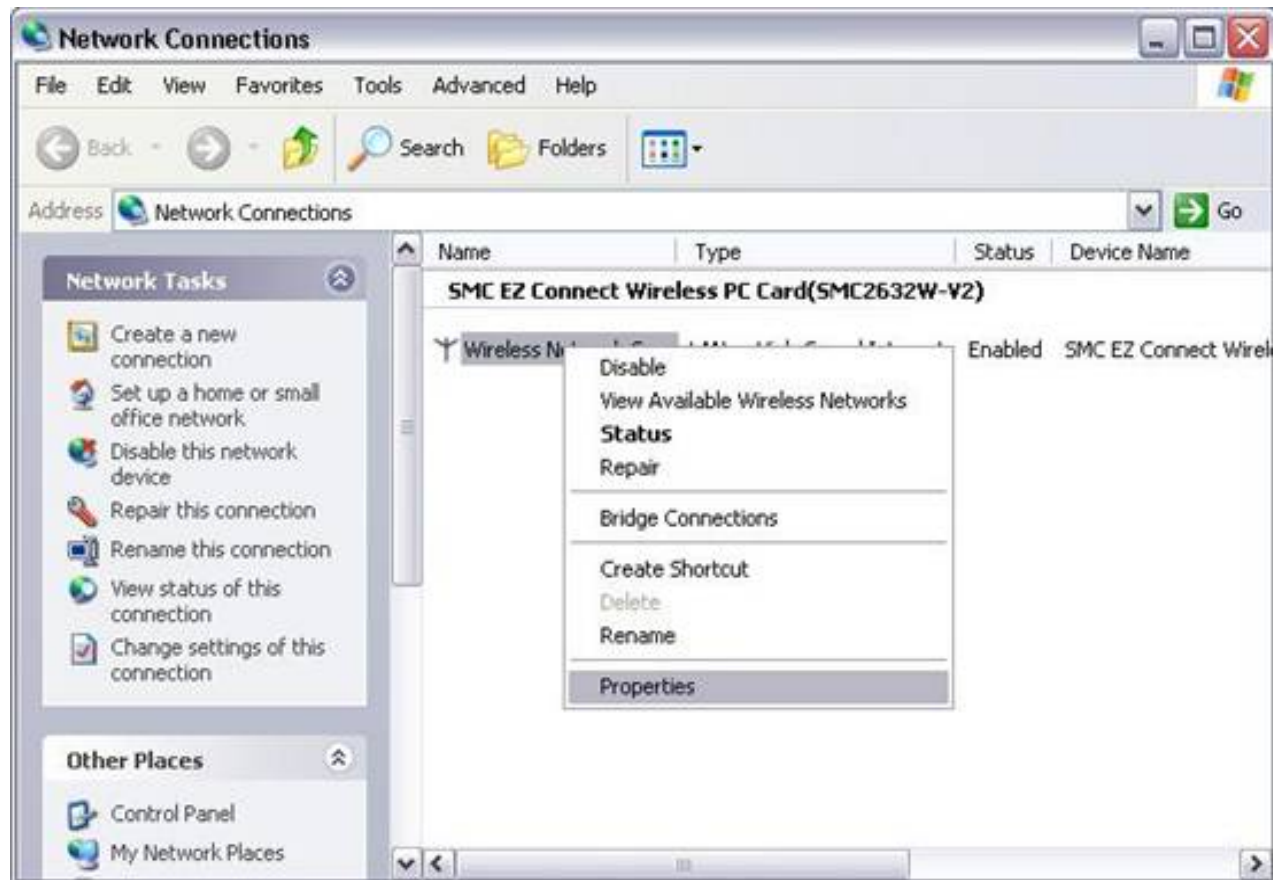


Figure 1.3

Step 4: Click the “Internet Protocol TCP/IP” option and make sure that the options for “Obtain IP address automatically” and “Obtain DNS servers automatically” are checked.

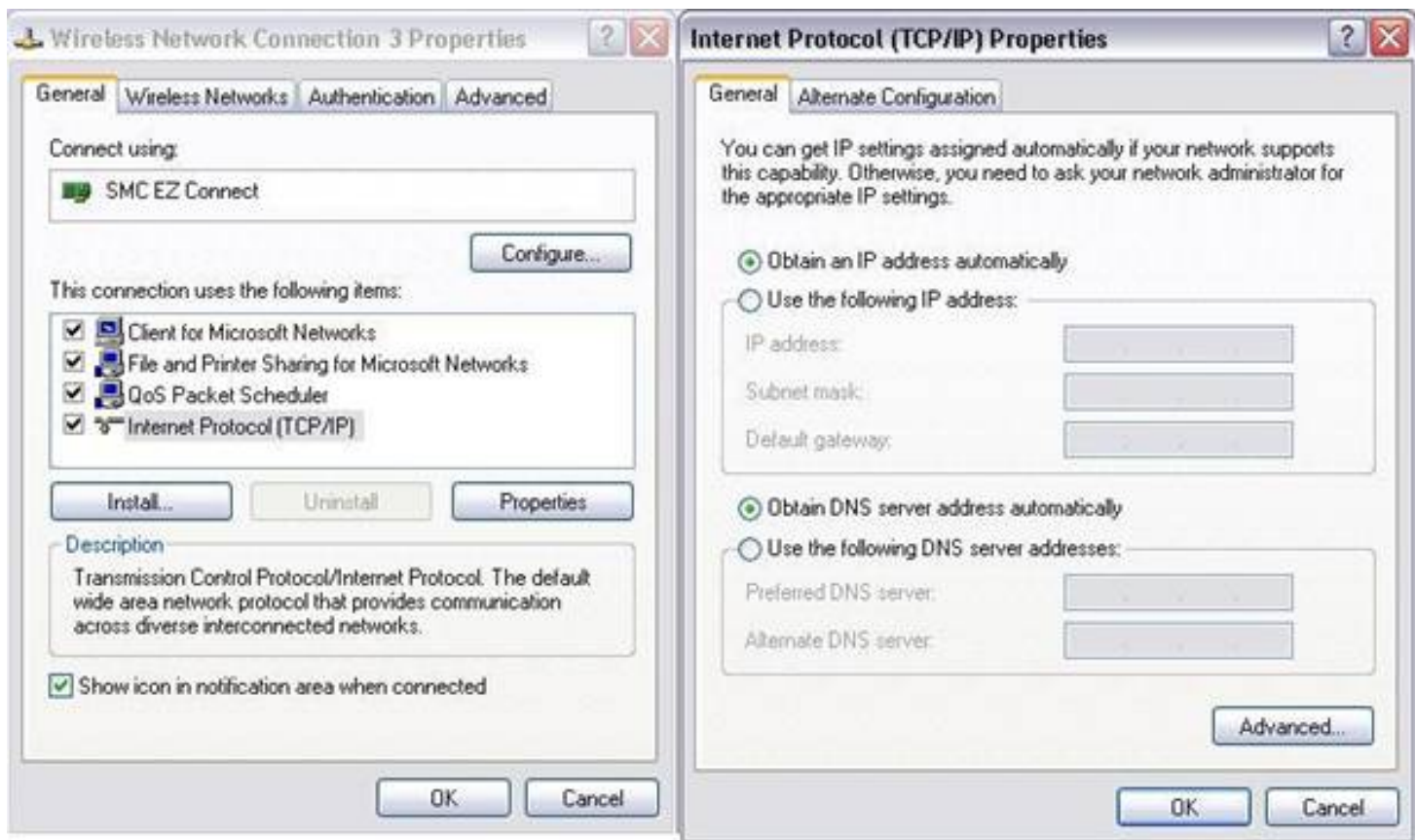


Figure 1.4

Step 5: Click on “OK” to the Internet Protocol Properties to close that window. Click “OK” again to close the Network Connections window.

Configure TCP/IP: Static IP on Windows XP

Step 1: Right-click the "Network Places" icon on your desktop and click "Properties".



Figure 1.0

Step 2: Right-click your "Local Area Connection" and click "Properties".

Step 3: Click "Internet Protocol TCP/IP" and click "Properties". Select the "Use the following IP Address" option and insert an IP address that is not in the range of the DHCP LAN address. For example, you might want to insert 192.168.2.50 for the IP address if the DHCP LAN address pool is 192.168.2.100 to 192.168.2.199. The gateway and preferred DNS server will be 192.168.2.1.



Figure 1.1

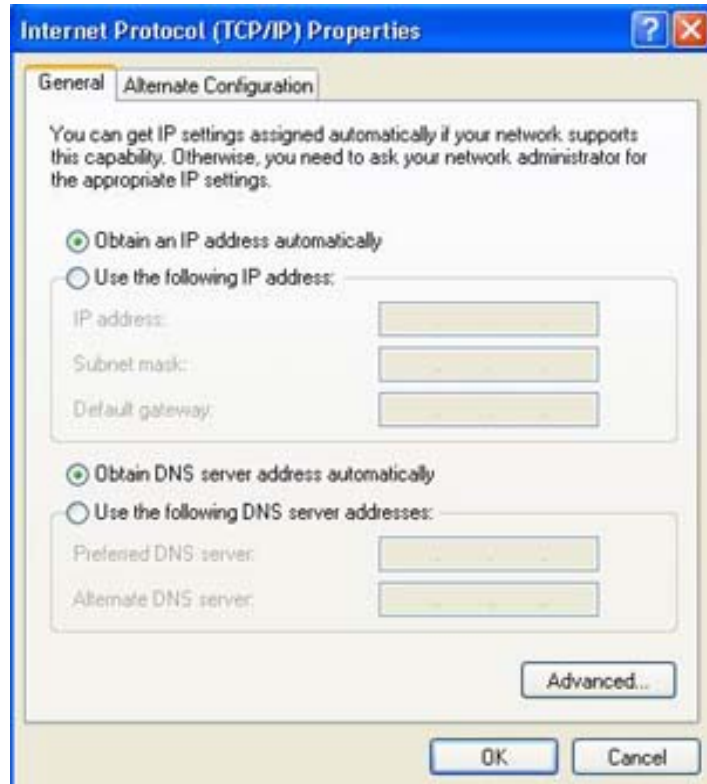


Figure 1.2

Step 4: Click on the "Use the following IP address" option.

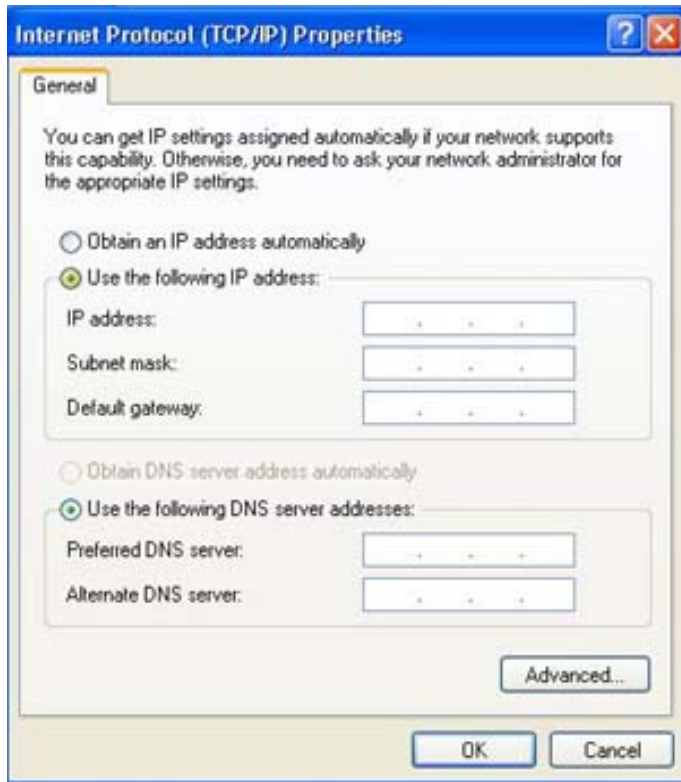


Figure 1.3

Step 5: Input a static IP.

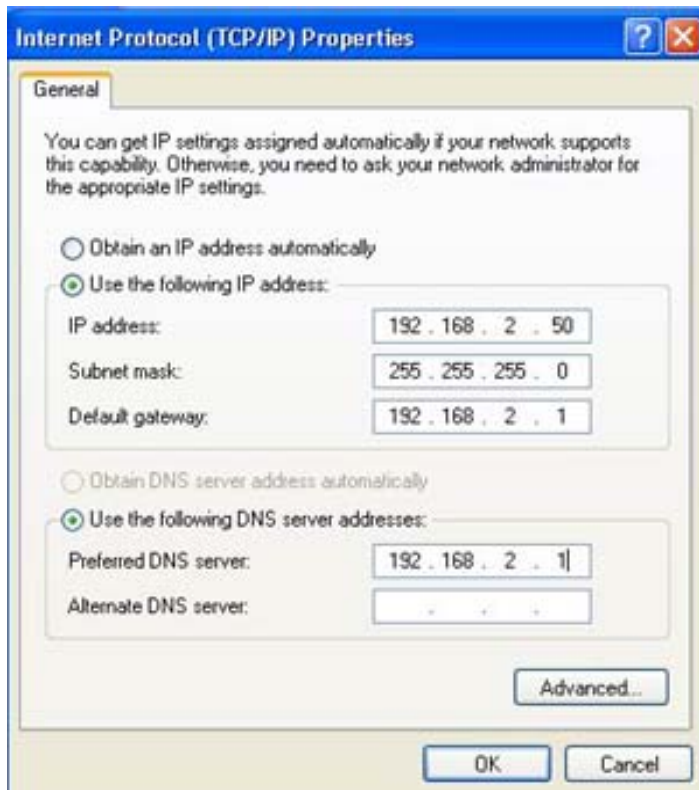


Figure 1.4

Step 6: Click "OK" and click "Close" to continue and save the changes.

SMC Networks EZ 3-Click Installation Wizard

Compatible with Windows 9x/Me/NT/2K/XP

Step 1: Insert the SMC2404WBR CD into your CD-ROM Drive.

Step 2: The EZ 3-Click Installation Wizard will auto-run. Choose the “Router Setup” option to begin configuring the router for Internet access.



Figure 1.0

Cable Connection

Step 3: Choose your specific WAN type. The Barricade Turbo Wireless Cable/DSL Broadband Router supports Cable/DSL. If you subscribe to a DSL connection, then normally you are using Point-to-Point Protocol over Ethernet (PPPoE) connection to get online. If you have a dynamic connection, then most likely you are using a Cable modem connection.



Figure 1.1

Step 4: If you selected the Cable option, the router will automatically begin to establish a connection with your ISP as shown in Figure 1.2. If you selected the DSL option, skip to *Step 5*. If you selected the Static IP option, please skip to *Step 6*.



Figure 1.2

DSL Connection

Step 5: Almost all DSL connections require a username and password. Please input this information in the specified boxes. If you do not have a username/password but still use a DSL connection, please leave these fields blank and click the "Next" button. Go to *Step 7* after clicking "Next".

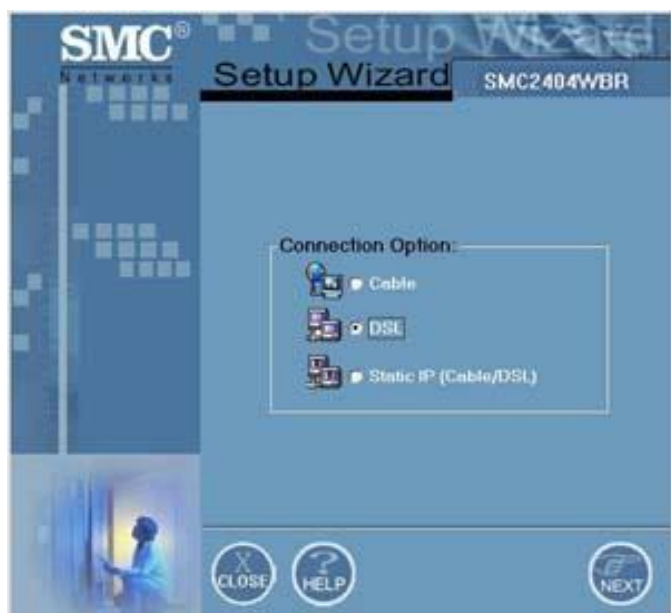


Figure 1.3

Static (Fixed) IP Connection

Step 6: If your ISP has given you a Static (Fixed) IP, then you should have the information concerning your IP Address, Subnet Mask, Gateway, and DNS Server addresses in your possession. Please input that data carefully and correctly in the appropriate fields. If you do not have this information or are uncertain about your connection, please contact your Internet Service Provider.



Figure 1.4



Figure 1.5

Step 7: The application will begin configuring the router after you have filled in the appropriate information. Click on "Next" to continue to the "Status" window, which will display what process is being performed.



Figure 1.6

Step 8: Once the router has been successfully configured, please click the "Finish" button and register your Wireless Barricade Turbo router. (Note: When registering your product, the Model Number of your product will be displayed in the lower left-hand corner of the screen for your convenience). You can get the Serial Number from the bottom of your Wireless Barricade Turbo. Thank you for choosing SMC Networks.



Figure 1.7



Figure 1.8

SMC Networks EZ 3-Click Installation Wizard

Cable Connection: Compatible with Windows 9x/Me/NT/2K/XP

Step 1: Insert the SMC2404WBR CD into your CD-ROM Drive.

Step 2: The EZ 3-Click Installation Wizard will auto-run. Choose the “Router Setup” option to begin configuring the router for Internet access.



Figure 1.0

Step 3: Choose the “Cable” option and press the “Next” button.

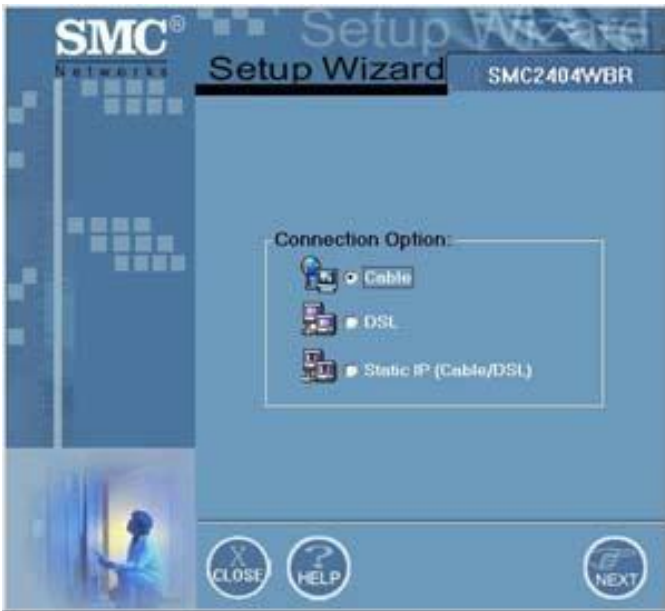


Figure 1.1

Step 4: The Setup Wizard will now configure the router to establish a connection with your ISP as shown below. If you receive any error messages regarding a failure to connect, please start over and try again or view the Help files for more troubleshooting steps.



Figure 1.2

Step 5: After the router has been successfully configured, you will receive a

“Congratulations” message in the Status window. At this point, your Wireless Barricade Turbo router is now online. Please click the “Finish” button.



Figure 1.3

Step 6: Once you click on the “Finish” button, you will be asked to register your product.



Figure 1.4

Step 7: Once you click “Yes”, you will be automatically directed to the online SMC Product Registration site so that you can register your new purchase. (Note: When registering your product Model Number of your product will be displayed in the lower left-hand corner of the screen for your convenience). You can obtain the Serial Number from the bottom of your Wireless Barricade Turbo unit.

Thank you for choosing SMC Networks.



Figure 1.5

SMC Networks EZ 3-Click Installation Wizard - Quick Install Guide

DSL Connection: Compatible with Windows 9x/Me/NT/2K/XP

Step 1: Insert the SMC2404WBR CD into your CD-ROM Drive.

Step 2: The Setup Wizard will auto-run. Choose the “Router Setup” option to begin configuring the router for Internet access.



Figure 1.0

Step 3: Choose the "DSL" option and then press the "Next" button.

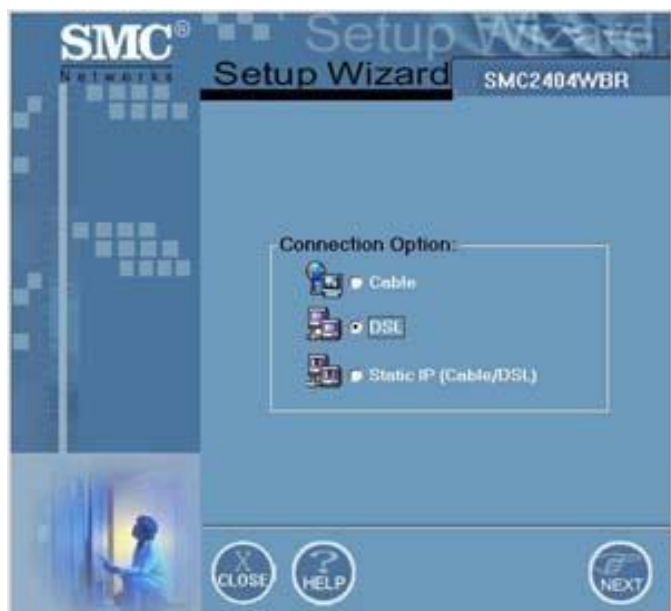


Figure 1.1

Step 4: Almost all DSL connections require a username and password. Please input this information. If you do not have a username/password but still use a DSL connection, please leave these fields blank and click the “Next” button.



Figure 1.2

Step 5: The Setup Wizard will now configure the router to establish a connection with your ISP as shown below. If you receive any error messages regarding a failure to connect, please start over and try again or view the Help files for more troubleshooting steps.



Figure 1.3

Step 6: After the router has been successfully configured, you will receive a “Congratulations” message in the Status window. At this point, your Wireless Barricade Turbo unit is now online. Please click the “Finish” button.



Figure 1.4

Step 7: Once you click on the “Finish” button, you will be asked to register your product.



Figure 1.5

Step 8: After clicking “Yes”, you will be automatically directed to the online SMC Product Registration site so that you can register your new purchase. (Note: When registering your product Model Number of your product will be displayed in the lower left-hand corner of the screen for your convenience). You can obtain the Serial Number from the bottom of your Wireless Barricade Turbo unit. Thank you for choosing SMC Networks.



Figure 1.6

SMC Networks 3-Click Installation Wizard - Quick Install Guide

Static (Fixed) IP Address Connection: Compatible with Windows 9x/Me/NT/2K/XP

Step 1: Insert the SMC2404WBR CD into your CD-ROM Drive.

Step 2: The Setup Wizard will auto-run. Choose the “Router Setup” option to begin configuring the router for Internet access.



Figure 1.0

Step 3: Choose the "Static IP" option and then click the “Next” button to continue.



Figure 1.1

Step 4: If your ISP has given you a Fixed or Static IP, then you should have the information concerning your IP Address, Subnet Mask, Gateway, and DNS addresses in your possession. Please input that data carefully and correctly in the appropriate fields. If you do not have this information or are uncertain about your connection, please contact your Internet Service Provider.



Figure 1.2

Step 5: The Setup Wizard will now configure the router to establish a connection with your ISP as shown below. If you receive any error messages regarding a

failure to connect, please start over and try again or view the Help files for more troubleshooting steps.



Figure 1.3

Step 6: After the Wireless Barricade Turbo has been successfully configured, you will receive a “Congratulations” message in the Status window. At this point, your router is now online. Please click the “Finish” button.



Figure 1.4

Step 7: Once you click on the finish button, you will be asked to register your

product.



Figure 1.5

Step 8: Once you click “Yes”, you will be automatically directed to the online SMC Product Registration site so that you can register your new purchase. (Note: When registering your product Model Number of your product will be displayed in the lower left-hand corner of the screen for your convenience). You can obtain the Serial Number from the bottom of your Wireless Barricade Turbo unit. Thank you for choosing SMC Networks.



Figure 1.6

Advanced Settings - Main Page

This section will discuss the advanced firewall features of the SMC2404WBR Broadband Router. This will also cover, in detail, how to configure Remote Management, SPI, Virtual Servers, Access Control and other features.



The screenshot shows the SMC Networks Advanced Setup interface. The top navigation bar includes the SMC Networks logo, the title "Advanced Setup", and links for "Home" and "Logout". A left sidebar menu lists various configuration categories: System, WAN, LAN, Wireless, NAT, Firewall (selected), Tools, and Status. The main content area is titled "Security Settings (Firewall)" and contains a descriptive paragraph about the Barricade firewall protection. Below the text, there are two radio buttons for "Enable or disable Firewall features": "Enable" (unselected) and "Disable" (selected). An "APPLY" button is located in the bottom right corner of the main content area.

SMC[®] Networks Advanced Setup Home Logout

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall**
- Tools
- Status

Security Settings (Firewall)

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

Enable or disable Firewall features : Enable Disable

APPLY

Advanced Settings - Wireless

This section will allow you to configure your SMC2404WBR for use with WEP (Wired Equivalent Privacy) security.



Figure 1.0

- To configure the Wireless Barricade Turbo 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 ID (SSID), and encryption options. On the main page, you can also disable the wireless function altogether.
- You need to open up your web browser and go to <http://192.168.2.1>, log into the router and go into the Advanced Setup. Click on the "Wireless" link on the left in order to configure the wireless settings. Please make sure that the Wireless functions are enabled before proceeding. You should specify a common radio channel and service domain (i.e., Service Set ID) to be used by the Wireless Barricade Turbo and all of your wireless clients. Be sure you configure all of your clients to the same values. By default, the Wireless Channel is set to "6" and the SSID is "default". The WEP is also disabled.

Channel and SSID

This page allows you to define SSID, Transmission Rate, Basic Rate and Channel ID for wireless connection. In the wireless environment, this gateway can be acting as an wireless access point. These parameters are used for the mobile stations to connect to this access point.

SSID	<input type="text"/>
Transmission Rate	22Mbps(Fully Automatic) ▾
Basic Rate	1.2Mbps ▾
Channel	6 ▾
Preamble	Long Preamble ▾



Figure 1.1

- Once you have established a wireless connection to the router, you can configure WEP encryption if you are transmitting sensitive data via the wireless network.
- The standard 64bit/128bit/256bit encryption requires you to use the same set of encryption/decryption keys for the Wireless Barricade Turbo and all of your wireless clients.
- You must have a 10-digit key for 64bit WEP, a 26-digit key for 128bit WEP and a 58-digit key for 256bit WEP.
- To manually configure the keys, enter 5 hexadecimal pairs for your chosen 64-bit key, enter 13 pairs for the 128bit key or enter 29 pairs for the 256bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F) Also note that the fields are filled in by default. You need to delete these characters/asterisks before entering your WEP key (For example: To configure WEP using Key 1, first delete the character entries you see for Key 1, then enter your desired hex pairs. Do not delete any asterisks from the other Keys)



Figure 1.2

- Note that you are given the option of choosing between four keys. The keys are displayed as Key 1, Key 2, Key 3, and Key 4. Normally, Key 1 is recommended. However, you can also enter keys under Key 2, 3, and/or 4. Once the same key is configured for Key 2, 3, or 4 of your wireless card, the wireless connection will be established.



Figure 1.3

- Also note that the WEP protects data transmitted between wireless nodes, but it does not secure any transmissions over your wired network or over the Internet.

Advanced Settings - Virtual Server

The Virtual Server portion is designed to allow traffic from the WAN side that is destined for a particular port to be specifically directed to the desired machine/server on the LAN side of the router. In other words, depending on the requested service (TCP/UDP port number), the Wireless Barricade Turbo redirects the external service request to the appropriate server (located at another internal IP address).



	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"/>

Figure 1.0

Standard Ports	
FTP	21
SSH	22
Telnet	23
SMTP	25
DNS	53 (UDP)
HTTP	80
POP3	110
IDENT	113
NNTP	119
PPTP	1723
RDP/Terminal Services	3389

The "Private IP" is the IP address of the computer that you are using:

§ To find out what IP address your computer has:

- Click on Start, select Run, and type "command"
- At the DOS prompt, type "ipconfig"
- This will bring up what IP scheme your computer is on
- For example

1. IP: 192.168.2.55

2. Subnet: 255.255.255.0

3. Default Gateway: 192.168.2.1

§ Now input the IP address in the "Private IP" portion

§ "Private Port" is the port that sends data, commonly known as the outbound port.

§ "Type" refers to have type of data this port will use. Please select the "Type" based on your software requirements

§ "Public Port" is the port that receives data or inbound traffic from the WAN

§ Click on "Enter" to save the changes.

Troubleshooting: Virtual Server

Example: Web Server

The web server should be set to "Private Port" 80 and "Public Port" 80:

- The web server can be accessed internally using the LAN IP, and externally using the WAN IP.
- Check the IP address on your configuration software. Make sure the configuration software is not set to the WAN IP. The server is now on a private network, so it must be configured with its correct LAN IP. When clients wish to access your web server, they will need to type the WAN IP address in their browser.
- a) If you own a web domain and are hosting the server on a machine behind the router, users can access

your web server using its domain name (for example: www.smc.com)

b) You must have the domain name translate to the WAN IP of the router

c) When plugged directly into the router, you must use the internal private IP of the server in order to access its web resources

- If you still cannot access your web server through the router after opening port 80, change the "Public Port" option to 50 instead. Then have your clients try to connect to the server using the `http://WAN_IP:50`
 - Basically the client would enter your WAN IP as usual, however, since the public port is now 50, they must also enter a colon, and then type in 50.
- If you still cannot access your web server after changing to a non-standard port, connect your machine directly into the modem and then see if your server works.
- If you cannot access the web server through a direct connection from the modem to the computer:
 - Check with your ISP regarding info on port 80. They are most likely blocking all traffic through this port

a) This is due to some viruses that use port 80.

b) You can set up the Virtual Server in the router to forward your web server to a different public port (i.e. – 50). This way, your WAN users can access the web domain by typing in `http://www.smc.com:50` (note: some domain hosting sites will automatically route the domain to port 50 for you – check with their Help Desk for more info)

Advanced Settings - Special Applications

Special Applications is a feature that allows your entire LAN or all the computers on your network to use the range of ports specified. The Trigger Port is the outbound port. It is the port through which your program begins communication. The Public Ports are the inbound ports that are open while your application is running.

Step 1: Input the outbound data port and then select the type of data that port uses.

Step 2: The Public Port are the incoming ports that must remain open while your program is in use.

Step 3: Input the inbound data port and then select the type of data that port uses.

Step 4: Click on the “Enable” check box and then click “Apply” to save the changes.

Step 5: Once all the settings have taken effect, click “Log Out”.

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"/>

Figure 1.0

Games:

Make sure that you have the necessary ports to play your games.

- These ports refer to:
 - Trigger port (Outbound data port): You can only enter one trigger in each column.
 - Public port (Inbound data port): You can enter one single port or a large range if necessary.
 - For example:
 - Trigger port: 200
 - Public port: 300, 400-500, 650

Messengers & Voice/Video Conferencing:

Make sure that you have the necessary ports to use your software.

- These ports refer to:
 - Trigger port (Outbound data port): Can be a single port or multiple ports.
 - Public port (Inbound data port): Can be a single port or a range or ports.
 - For example:
 - Trigger port: 100, Trigger port 2: 2000, Trigger port 3: 5556
 - Public port: 340, 4040-5000, 650,756

Advanced Settings - Access Control

Access Control is an extremely useful function provided so that Network Administrators can effectively manage or segment the networks. The features included here allow you to specify different privileges for your client PCs.

Access Control allows users to define the outgoing traffic permitted or not permitted for the WAN interface. The default is to permit all the outgoing traffic. The rules defined under access control can limit the access of different types of traffic. The Wireless Barricade Turbo can also limit the access of hosts within the Local Area Network (LAN). The MAC Filtering Table allows the router to define up to 32 hosts which are not allowed to access to the WAN port.

By default, you will see the following in Access Control:

The screenshot displays the 'Access Control' configuration interface. At the top, there is a section for 'Enable Filtering Function' with radio buttons for 'Yes' and 'No', where 'No' is selected. Below this is a section for 'Normal Filtering Table (up to 10 computers)'. It features a table with columns: 'Client PC Description', 'Client PC IP Address', 'Client Service', and 'Schedule Rule'. The table is currently empty, and a red error message 'No Valid Filtering Rule !!!' is displayed below the table header. Underneath the normal filtering table is a link labeled 'Add PC'. The bottom section is for 'MAC Filtering Table (up to 32 computers)'. It contains a table with two main columns: 'Rule Number' and 'Client PC MAC Address'. The 'Rule Number' column has rows numbered 1 through 4. The 'Client PC MAC Address' column is divided into eight sub-columns, each containing a text input field for a hexadecimal digit, with colons between the sub-columns to represent the MAC address format.

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

Rule Number	Client PC MAC Address
1	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Figure 1.0

Click on the "Add PC" link in order to define the appropriate settings for Client PC services.

Advanced Setup Home Logout

- Client PC Description:
- Client PC IP Address: 192.168.0. ~ 0
- Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8080, 8081	<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"/>

Figure 1.1

You can set a "Client PC Description". This should help you identify which PC or group of PCs that specific filtering rule applies to. The "Client PC Description" will be listed on the main Access Control Page in the "Normal Filtering Table". You can also specify the "Client PC Address". This allows you to segment a range of PCs and limit the services they have access to. The "Client PC Service" lists the plethora of protocols/services that the Wireless Barricade Turbo can effectively and completely block access to. (Note: This is solely port based)

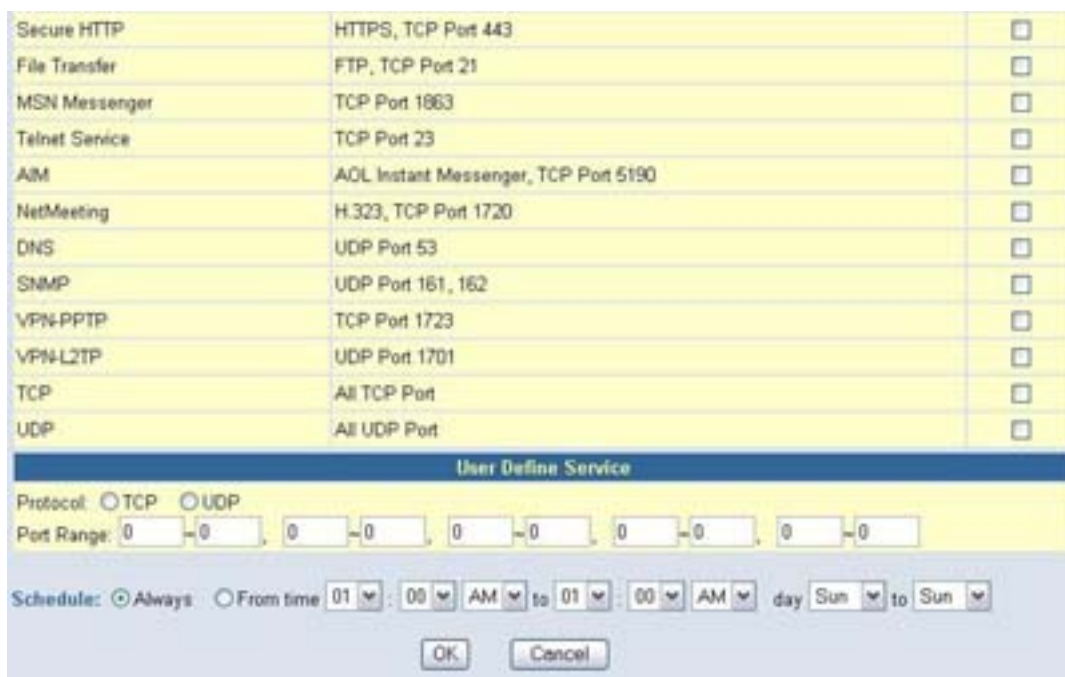


Figure 1.2

The above image shows that you have an option to manually configure the port ranges and the type of ports you which to block as well. This is called the "User Define Service". The user can select either the TCP or UDP protocol. Then you must enter the exact port ranges you which to filter. In this section, you are also given the option to set up the particular "Schedule" of when you want this filter to take effect.

Advanced Settings - URL Blocking

The Wireless Barricade Turbo allows users to block access to certain Internet sites by entering either a full URL address or just a keyword of the Internet site. User can enter the full URL address or some keywords of the Web site, The router will examine all the HTTP packets to block the access to those particular sites. This feature can be used to protect children from accessing certain violent or sexual content.



Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1	<input type="text"/>	Site 16	<input type="text"/>
Site 2	<input type="text"/>	Site 17	<input type="text"/>
Site 3	<input type="text"/>	Site 18	<input type="text"/>
Site 4	<input type="text"/>	Site 19	<input type="text"/>
Site 5	<input type="text"/>	Site 20	<input type="text"/>
Site 6	<input type="text"/>	Site 21	<input type="text"/>
Site 7	<input type="text"/>	Site 22	<input type="text"/>
Site 8	<input type="text"/>	Site 23	<input type="text"/>
Site 9	<input type="text"/>	Site 24	<input type="text"/>
Site 10	<input type="text"/>	Site 25	<input type="text"/>

Figure 1.0

To specify a particular PC or group of PCs, go back to the "Access Control" page, edit the appropriate Filtering rule and select the box for "WWW with URL Blocking".

Advanced Settings - Intrusion Detection



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
 - Discard Ping From WAN :
- When hackers attempt to enter your network, we can alert you by e-mail
 - Your E-mail Address :
 - SMTP Server Address :

Figure 1.0

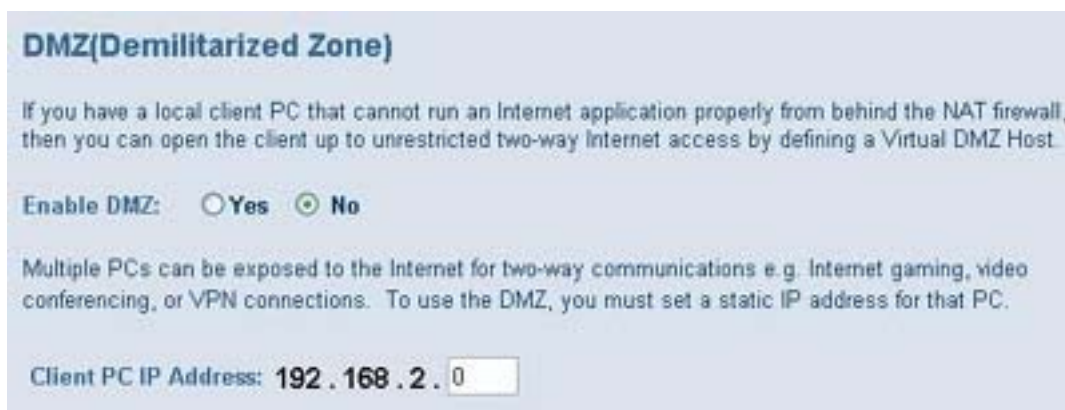
The Intrusion Detection feature of the Barricade limits the access of the incoming traffic from the WAN side. The Stateful Packet Inspection (SPI) functionality is enabled by default. You can also configure the router to discard pings from the WAN side.

When hackers attempt to enter your network, the Barricade can alert you via e-mail. You simply need to enter your email address and the SMTP mail server address. The Wireless Barricade Turbo inspects packets at the application layer and maintains TCP and UDP session information, including timeouts and number of active sessions, thus providing the ability to detect and prevent certain types of network attacks such as DoS attacks.

Network attacks that deny access to a network device are called denial-of-service (DoS) attacks. Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resource. By using the appropriate inspected information and timeout/threshold criteria, the Wireless Barricade Turbo prevents these types of attacks.

Advanced Settings - DMZ

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 the screen shown below. You simply need to enter the last octet of your IP address. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort



DMZ(Demilitarized Zone)

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

Enable DMZ: Yes No

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

Client PC IP Address: 192 . 168 . 2 .

Figure 1.0

Advanced Settings - Miscellaneous

Administrator Idle Time-Out: Allows you to set the specified time of inactivity which will command the router to automatically log out the administrator.

The screenshot shows the 'Advanced Setup' interface. At the top, there is a navigation bar with 'Home' and 'Logout' links. The main heading is 'Password Settings'. Below the heading, there is a paragraph of instructions: 'Set a password to restrict management access to the Barricade Plus. If you want to manage the Barricade Plus from a remote location (outside of the local network), you must also specify the IP address of the remote PC. You can do this in the Firewall - Access Control menu.' There are four form fields: 'Current Password', 'New Password', 'Re-Enter Password for Verification', and 'Idle Time Out'. The 'Idle Time Out' field is set to '10' and has the unit 'Min' next to it. Below the 'Idle Time Out' field, there is a note: '(Idle Time =0 : NO Time Out)'. The 'Current Password' field is currently empty.

Figure 1.0

Remote Management

Remote management allows you to log into your router from a remote location. By default, it is set to 0.0.0.0 which would allow any computer on the WAN side to log into the router

If specified to 24.45.34.12 for example, only a machine with that specific public IP will be able to remotely administer the router

To remotely administrate the router: 1) Open a web browser and 2) Type `http://WAN_IP:8080` in the address bar

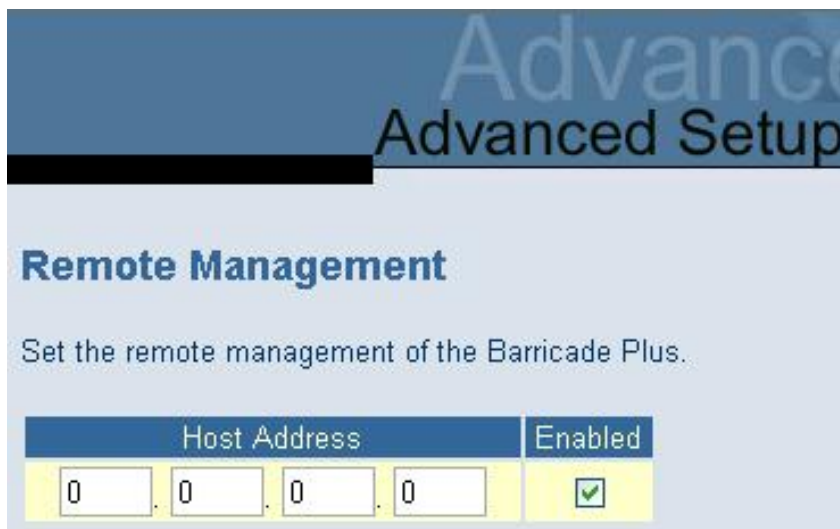


Figure 1.1

Configuration Tools: Allows you to backup/restore all your settings. Also gives you the option of restoring the router to factory defaults.

Simply select the "Backup" radio button and click "More Configuration". Click "Save" and choose the location where you want the file to be saved.

To restore your settings, select the "Restore" radio button and click "More Configuration". Then click "Browse", find the location where you previously saved the backup file and then click "Apply".

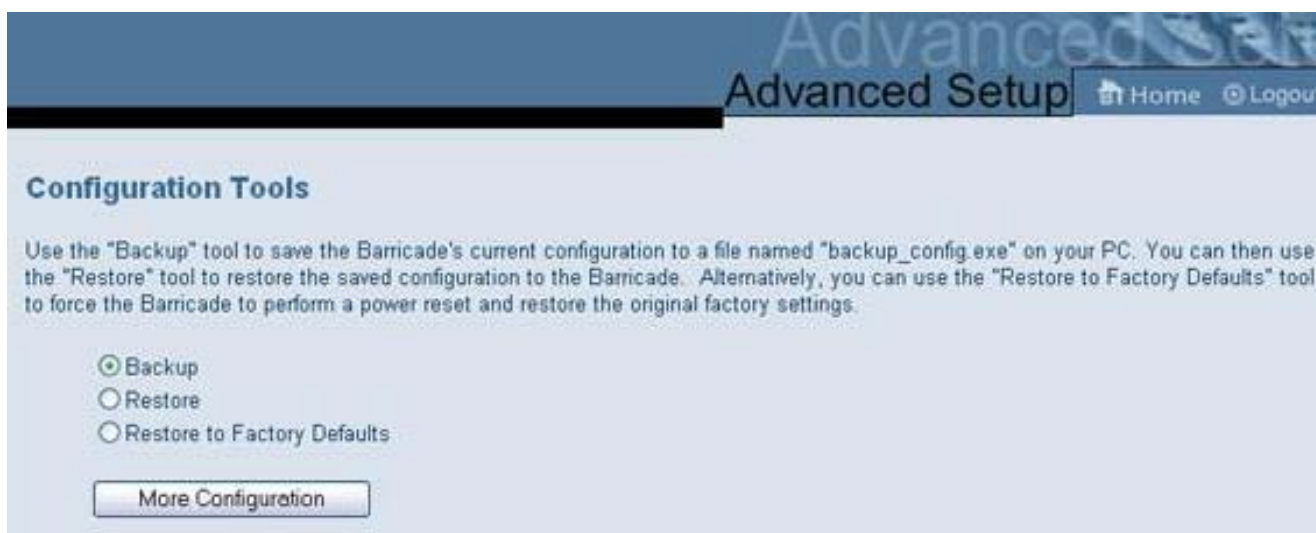


Figure 1.2

■ ***Troubleshooting: Remote Management***

Q) I set 0.0.0.0 as the Remote Mgmt. IP and still cannot access the router remotely.

A)

1) Check for firmware updates from <http://www.smc.com>. Once updated, reset and reconfigure your router.

2) Check your permissions with your network administrator. Make sure that you have access to port 8080.

Q) I set the IP address to a specific WAN IP and still cannot access the router.

A)

1) Go into the browser and type in http://WAN_IP:8080.

2) Check for firmware updates from <http://www.smc.com>. Once updated, reset and reconfigure your router.

Note: Check your permissions with your network administrator. Make sure that you have access to port 8080.

Troubleshooting Section: SMC2404WBR



This section will provide some common troubleshooting guides for your Wireless Barricade Turbo

SMC2404WBR Wireless Cable/DSL Broadband Router – Types of Connections

[Cable](#)

[DSL](#)

[Static \(Fixed IP\)](#)

Frequently Asked Questions

[Disable Dial-up and Proxy](#)

[Ethernet Adapter \(Network Interface Card\)](#)

[Software Conflicts](#)

[VPN Connections](#)

[General Information](#)

Types of WAN Connections

Ø A common WAN type is DHCP or Dynamic Host Configuration Protocol (commonly known as Dynamic IP addressing). This is for Internet Service Providers (ISP) that provide you with an IP address dynamically. For example, if you do not need a username and password to get online, then you most likely have a provider that is using DHCP.

Ø There are also providers that supply Static IP addresses. This means that your ISP has given you a list of numbers to manually configure your network connections. By selecting a Static IP Address setup, you have indicated that you will manually enter your IP address information. For example, you should a list of numbers similar to the following format:

§ IP: 24.34.67.129

§ Subnet Mask: 255.255.254.0

§ Default Gateway: 24.34.67.1

§ DNS:

○ Primary: 24.34.68.126

○ Secondary: 24.34.68.127

Ø Another equally common WAN type is Point-to-Point Protocol over Ethernet or simply PPPoE. This is for DSL connections that have provided you with a username and password in order for you to use the internet.

Cable Modem Troubleshooting

Ø Most Cable services are very simple to configure. You simply need to clone the MAC address of the network card that was registered by your ISP. To do so, you **MUST** run the SMC Connection Wizard software from the machine that is usually plugged directly into the modem. You can also manually log into the router to clone the MAC address. The directions are shown below.

Ø You may need to obtain your exact HOST NAME from the ISP. Many @home service **NO LONGER** use host names, however, this varies from ISP to ISP. You can contact your provider for more info or you can follow the directions below:

Windows 9x/ME

- 1) Go to the Control Panel
- 2) Double-click on Network
- 3) Go to the Identification tab and write down the computer name (it will most likely be in a cc43567-a format)

Windows 2K/XP

- 1) Go to the Control Panel
- 2) Double-click on System
- 3) Go to the Network tab and write down the computer name

Ø Now that you have the host name, you will be able to configure the router to connect to your ISP. Simply log into the unit by going into <http://192.168.2.1>, click on “Advanced Setup”, and click on "WAN". Then go to the “Dynamic IP” section and type in the host name exactly as you wrote it down earlier. Then click the “Apply” button. Wait about 10 seconds and then click on the “Status” link on

the top of the page. On the left “Internet” column, it should say Cable/DSL Connected at this point. If so, then you are online. If it still says Disconnected, then go back to the "Dynamic IP" section and click on the “CloneMAC Address” button. Then press “Apply” again and go back to “Status”.

Ø If you still cannot get a connection, recycle the power on all networked devices (including the router, modem and PCs)

If you continue to have problems, download the latest firmware available for download from our site: <http://www.smc.com/>

DSL Modem Troubleshooting

Ø Most DSL services provide DHCP to their customers, however, they require a username and password in order to log into the service. This is called PPP over Ethernet. You need to verify exactly what your login and password is for your service.

Ø Then log into the router at <http://192.168.2.1>, go to the “Advanced Setup” section, click on "WAN", and then select "PPPoE". You will then see fields for your login and your password. Enter this information exactly as provided by the ISP. In most cases, you should leave the Service Name blank. Then press the “Apply” button. The router should automatically establish a connection to the WAN. Go to the “Status” section, and under the “Internet” column, it should say Cable/DSL Connected. If so, then you are online and can now open your web browser. If it still says Disconnected, then turn off the router and the DSL modem for about 5 minutes. Then turn them back on, log into the router again, and it should be connected.

- Earthlink customers may need to enter their full email address for the “User Name” or “Account”. See examples below:

a) ELN/username@earthlink.net

b) username@earthlink.net

c) you may also need to enter “Earthlink DSL” as the Service Name

- Below is a list of services that may require the full email address for the “User Name” (much like Earthlink DSL).

a) Mindspring (username@mindspring.com)

b) Ameritech (username@ameritech.net)

c) MTS Sympatico Business
(username@res.mts.net)

d) Bell Canada (username@on.aibn.com or
username@qc.aibn.com)

e) Pacific Bell (username@pacbell.net)

f) SBC (username@sbcglobal.net)

If you continue to have problems, download the latest firmware available for download from our site: <http://www.smc.com/>. The instructions will be included in the download file.

Static IP Address Troubleshooting

- Ø This should be the simplest of all the different types of WAN configurations. You need to be sure that you have ALL 5 numbers from your ISP:
 - § IP Address
 - § Subnet Mask
 - § Default Gateway
 - § Primary DNS
 - § Secondary DNS (in some special cases, the ISP may not have provided a secondary DNS number)
- Ø Log into the router's web interface at <http://192.168.2.1> and then go to the “Advanced Setup” section. Click on “Static IP” and input the data that your ISP has given you. Then go ahead and click the “Apply” button in the bottom right-hand corner. It will then ask you to enter the DNS numbers. Click “Apply” again when finished. The router should instantly establish a connection to the WAN. To verify that you are connected, go to the “Status” section and under the INTERNET heading you should see Cable/DSL: Connected.
- Ø If the router shows that it is Disconnected, recycle the power on all networked devices (including the router, modem and PCs). Then follow the steps above to log into the router, check the configuration and view the Connection Status. At that point, it should be online.
- Ø If you continue to have any technical difficulties, please download the latest revision of firmware available for free download from <http://www.smc.com>. Once that is complete, go ahead and reset the router to defaults and then reconfigure it for internet access. Then you should be good to go.
- Ø You can also contact Technical Services through the online support form.

Frequently Asked Questions - Main Page



This section will show common troubleshooting guides that may be very helpful when configuring your router. You will also find the General FAQ section extremely useful as it includes several networking definitions, MAC OS info and Linux help files.

Disabling Dial-up and Proxy

1. Usually you can determine if you are running firewall software by looking in the systems tray. This is located in your lower right-hand side of your screen. Most common firewall software applications are Zone Alarm, Black Ice Defender, Norton, and McAfee. If you want to disable these, you can usually right-click these icons and look for a menu that gives you an option to EXIT, SHUT DOWN or CLOSE.
2. If you have a Dial-up and/or proxy server connection, you can disable this by launching your Internet Explorer browser. Click on the "Stop" icon (marked by a circle with a check mark). Then, click on "Tools" and select "Internet Options". You will see several tabs at the top of this window. Click on the "Connections" tab. Now you should have various radio buttons to choose from. Select "Never dial a connection". To disable your proxy server, click on the "LAN Settings" button. This will open a window called Local Area Network Settings properties. Make sure that absolutely nothing is checked.

Network Interface Cards - What adapter are you using?

The following section is very helpful in the event that you cannot connect to the router interface. This will show you how to change the actual speed of your adapter and properly identify its Make/Model. You will also want to have this information handy if you need to contact Technical Services for any reason.

Windows 9x/Me

§ Click “Start”, and then go to “Settings” and click on “Control Panel”. Double-click the “Network” Icon and then you will see a list of adapters. Usually the network interface card will include 10/100 or LAN in its actual name.

§ If you have a problem connecting to the router interface, there may be a problem with the auto negotiation features of your adapter. In this case you would need to hard-set the speed of the adapter. To do this, double-click on its name in “Network” and go to the Advanced tab. Look through each setting and change the “media type” or “link speed” to 10Mb Half Duplex/10BaseT. Then press OK to save the changes.

§ To continue installing the router, [click here](#).

Windows NT

§ Right-click the “Network” icon on your desktop and go to the “Adapters” tab. Then you may see a list of adapters. Usually the network interface card will include 10/100 or LAN in its actual name.

§ If you have a problem connecting to the router interface, there may be a problem with the auto negotiation features of your adapter. In this case, you would need to hard-set the speed of the adapter. To do this, double-click on its name under this “Adapters” tab and change the speed to 10Mb Half Duplex/10BaseT. Then save the changes. The system may need to be restarted afterwards.

§ To continue installing the router, click [here](#).

Windows 2000

§ Click “Start”, click “Settings” and click on “Control Panel”. Then go ahead and double-click on “Network and Dial-up Connections”. You should see a list of Local Area Connections. If there are too many adapters and it is confusing to identify your LAN connection, please click on “View” on the top menu bar, click “Arrange Icons” and select “By Device Name”.

§ You should now be able to identify the specific adapters. Scroll to the right using the scroll on the bottom of the window. It will show the appropriate LAN connection for the corresponding adapter.

§ Right-click on the “Local Area Connection” and click “Properties”. On the top of this window, you should see text that reads “Connect using:”. The brand/model of your adapter will be displayed in the window below that text. If you have a problem connecting to the router interface, there may be a problem with the auto negotiation features of your adapter. In this case, you would need to hard-set the speed of the adapter. Click the “Configure” button and go to the “Advanced” tab. Look through each setting and change the “media type” or “link speed” to 10Mb Half Duplex/10BaseT. Then press OK to save the changes.

Windows XP

§ Click “Start”, click “My Computer”, and then click “My Network Places” on the left. Then click “View Network Connections” on the left. You should see a list of Local Area Connections. If there are too many adapters and it is confusing to identify your LAN connection, please click on “View” on the top menu bar, click “Arrange Icons” and select “By Device Name”.

§ You should now be able to identify the specific adapters. It will show the appropriate LAN connection for the corresponding adapter.

§ Right-click on the “Local Area Connection” and click “Properties”. On the top of this window, you should see text that reads “Connect using:”. The brand/model of your adapter will be displayed in the window below that text. If you have a problem connecting to the router interface, there may be a problem with the auto negotiation features of your adapter. In this case, you would need to

hard-set the speed of the adapter. Click the “Configure” button and go to the “Advanced” tab. Look through each setting and change the “media type” or “link speed” to 10Mb Half Duplex/10BaseT. Then press OK to save the changes.

Third Party Software

Routing Software:

You may have installed programs that allow you to route information from one network to another. You may need to uninstall/disable this software in order to successfully access the router. This would include popular proxy applications such as:

- § Internet Connection Sharing
- § Sygate Home Network
- § WinGate
- § WinProxy

Firewall Software:

You may have installed programs or firewall software that protects your PC for intruders. You may need to uninstall/disable this software in order to successfully access the router. This would include popular proxy applications such as:

- § Zone Alarm
- § Norton Internet Security
- § Norton SystemWorks
- § McAfee Firewall

Making VPN Connections

Ø *Overview*

§ IPsec stands for IP Security. It provides authentication and encryption over the Internet. It functions at Layer 3 and thus secures **everything** on the network. It has become a standard protocol used for virtual private networks (VPNs).

§ PPTP stands for Point-to-Point Tunneling Protocol. It basically allows you to establish a connection to a corporate network and you can share files and other data as if your machine were actually on that local network.

§ L2TP stands for Layer 2 Tunneling Protocol. It is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks.

§ VPN is an acronym for Virtual Private Network. This is a private network that can exist in a public infrastructure. It maintains security and privacy through the use of tunneling protocols and IP Security.

Ø *General*

§ In general, most VPN applications will automatically function properly through the router. In some cases, you may need to specifically open ports in the router through the Virtual Server section.

§ If you are using IP Security, you need to open port 500.

§ If you are using PPTP, you need to open port 1723.

§ If you are using L2TP, port 1701 must be opened.

§ Please review the “Advanced Settings – Virtual Server” section of this Help documentation for more info on configuring this section of the router.

Ø *CheckPoint VPN*

§ Update firmware to latest version, reset to defaults.

§ Try forwarding ports 256, 564, and 500, in the Virtual Server screen of the Barricade.

§ There also may be a "Use Through NAT Transparency Mode", "Use through Firewall", or similar setting in the client software; if so, select it.

§ Open port 500 in the "Virtual Server" screen of the Barricade section and try again.

§ Set your computer up as the DMZ host under the "Misc Item" section in the Barricade.

§ Try hard setting the MTU level to 576 and try again. This can be done either in the client software, the registry, or by a third party program.

§ If you have tried all suggestions above and you are still unable to use your VPN through the Barricade, then you will need to refer to the VPN software developer for additional assistance.

Ø *SecureRemote VPN*

§ This application commonly uses IP Security so you will need to open port 500 as stated before.

§ UDP Encapsulation Mode enables IKE/IPSec Secure Remote users to traverse Network Address Translation devices, firewalls and other devices that fail to handle IPSec packets. It also enables more than one Secure Remote user to work with IPSec behind a port-mapping NAT device, also known as dynamic NAT, (e.g., FireWall-1 Hide NAT mode) with the same VPN-1/SecuRemote/SecureClient gateway.

§ This is achieved by encapsulating IPSec packets inside UDP datagrams. This option is negotiated in IKE. VPN-1/SecuRemote/SecureClient supports this feature only in IPSec ESP mode (AH is not supported).

- § Two modes of UDP Encapsulation are available:
- Automatic mode in which UDP encapsulation is performed only when the Secure Remote client is behind a dynamic Network Address Translation device configured for Hide mode. In other cases, IPsec packets are transmitted in the standard manner. The server determines how to transmit IPsec packets according to value of the source port in IKE packets.
 - Forced mode in which the client can work only in UDP Encapsulation Mode. Communication is enabled only if the gateway supports UDP encapsulation and always uses UDP Encapsulation Mode. Forced mode should be used if the client is behind devices which drop or damage IPsec packets but do not modify IKE packets.

Ø *AT&T Client VPN*

§ AT&T Global Networks, (formerly IBM Global Networks), has used IPsec Header Authentication, and thus would not work through a NAT device.

§ The new version of the AT&T Client VPN software (which they call the "dialer" with Bluemoon Tunneling) now supports IPsec Data Authentication without IPsec Header Authentication, and it now works through routers.

§ However, in order to make this work, you need to put the following two undocumented statements in the "custom.ini" file which is located in the same directory as the rest of the VPN client software (typically c:\program files\AT&T Global Network\).

§ The version of the AT&T client software must be 4.25.2 or higher (which was released on Sept 6, 2000).

§ In custom.ini put:

- [BlueMoon]
- AllowNatThroughFireWall=True

SMC2404WBR: 11/22 Mbps Auto-Sensing Wireless Cable/DSL Broadband Router F.A.Q.

TERMINOLOGY

Q. What is a LAN?

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

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

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

Q. What is MDI / MDI-X?

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

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

Q. What is NAT?

A. **Network Address Translation** - An IETF standard that allows an organization to present itself to the Internet with one address. NAT converts the address of each LAN node into one IP address for the Internet and vice versa. It also serves as a firewall by keeping individual IP addresses hidden from the outside world. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Q. What is a MAC Address?

A. The unique serial number burned into Ethernet and Token Ring adapters that identify that network card from all others.

Q. What is PPP over Ethernet?

A. **Point-to-Point Protocol Over Ethernet** - A method for running the

PPP protocol, commonly used for dial-up Internet connections, over Ethernet. Used by DSL and some cable modem providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet. A discovery process in PPPoE determines the Ethernet MAC address of the remote device in order to establish a session.

Q. What is DHCP?

A. **Dynamic Host Configuration Protocol** - Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network. It eliminates having to manually assign permanent IP addresses. DHCP software typically runs in servers and is also found in network devices such as ISDN routers and modem routers that allow multiple users access to the Internet. Newer DHCP servers dynamically update the DNS servers after making assignments.

Q. What are TCP and UDP ports?

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

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

Q. What are the definitions for the firewall terms in the Help File?

A. **SYN Flood Attack** - An assault on a network that prevents a TCP/IP server from servicing other users. It is accomplished by not sending the final acknowledgment to the server's SYN-ACK response (SYNchronize-ACKnowledge) in the handshaking sequence, which causes the server to keep signaling until it eventually times out. The source address from the client is, of course, counterfeit. SYN flood attacks can either overload the server or cause it to crash.

Smurf Attack - A type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

Denial Of Service Attack - An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack interrupts network service for some period. A distributed denial of service (DDOS) attack uses multiple computers throughout the network that it has previously infected. All of these "zombies" work together to send out bogus messages, thereby increasing the amount of phony traffic.

Ping of Death - A ping request that crashes the target computer. It is caused by an invalid packet size value in the packet header. There are patches for most operating systems to prevent it.

IP Spoofing - A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted port. To engage in IP

spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted port and then modify the packet headers so that it appears that the packets are coming from that port.

Troubleshooting

Q. I have trouble logging into the router.

A. Disable/Uninstall ALL software firewalls. Then make sure that there are NO proxy configurations in the browser. In Internet Explorer, you go to Tools, click on Internet Options, click on the Connections tab, click on LAN settings and make sure that nothing is checked. In Netscape, go to Edit, click Preferences, go to Advanced, and make sure that Direct Connection to Internet is checked. Be sure to upgrade the firmware on the unit.

Q. How do you reset the Barricade to factory defaults?

A. Power off the router for about 30 seconds and then turn it on. Depress the RESET button for 5 seconds and release it. The RESET button is on the left of the front panel. The power light will flash rapidly, all 8 port lights will turn on shortly, and then the router will return to its normal state.

Q. How do I update the firmware?

A.

1. Turn on the router and plug it into your network adapter using port 1, 2, 3, or 4 on the router.
2. Connect to the web user interface by typing the Barricade's IP Address (ex: 192.168.2.1) in your browser. Leave the password field blank and login (or enter your password if you created one)
3. Go to the Advanced section. Click on the "Tools" link, and then click the "Firmware Upgrade" option.
4. Set the "Update Target" to **Firmware**. Click the "Browse" button and point

it to the location of the firmware file. Click the "Apply" button and follow the prompts. You will notice the lights on the Barricade will react in a certain sequence. Wait patiently while the Barricade performs its reboot sequence.

5. Your 2404WBR has now been successfully upgraded. Please log into the Barricade's management and configure the router according to your type of broadband connection.

Q. How do I configure the Barricade using a MacIntosh?

A. Please follow the steps as they are outlined below:

1. Click on the <Apple> key, choose Control Panels, and select TCP/IP
2. Select "Connect via Ethernet Built In or Ethernet Slot"
3. Set the next option to "Configure using <DHCP>"
4. Hit the close box in the top left corner you will be asked to save. Hit <Save>
5. *Optional:* Select Edit, User Mode, and Advanced. Click on the "Options...." Button to verify that TCP/IP is active.

Q. Can I assign static IP addresses to machines behind the router? If so, how?

A. Yes. Note that each machine **MUST** have a different IP address and DNS host name. You can also enter your ISP's DNS numbers instead of the router's IP address if you wish to do so. See below:

Windows 9x/ME

- 1) Go to your control panel and double-click on Network.
- 2) Double-click where you see TCP/IP (ethernet card).
- 3) Click specify an IP address and type in 192.168.2.55
- 4) Where it says subnet mask, type in 255.255.255.0
- 5) Click on the gateway tab and type in 192.168.2.1. Click add
- 6) Click on the DNS tab and enable it. Set the host name to 123 and the DNS Search Order to 192.168.2.1. Then click OK twice.
- 7) Restart the computer when it requests you too.

Windows 2k/XP

- 1) Go to your control panel and double-click on Network and Dialup

Connections.

- 2) Double-click on Local Area Network and click Properties. Double-click where you see Internet Protocol TCP/IP.
- 3) Click use the following IP address and type in 192.168.2.55
- 4) Where it says subnet mask, type in 255.255.255.0
- 5) For the gateway, type in 192.168.2.1.
- 6) Set the preferred DNS to 192.168.2.1. Leave alternate blank. Then click OK twice.

Mac OS

- 1) Go into your TCP/IP Control Panel
- 2) Set an IP of 192.168.2.55
- 3) Set a subnet mask of 255.255.255.0
- 4) Set a router address of 192.168.2.1
- 5) Set the primary DNS to 192.168.2.1 (leave the alternate/secondary blank)
- 6) Close and save the information

Q. What is DMZ? And how many DMZ computers does the Barricade support?

A. Demilitarized Zone (DMZ) is a feature of the firewall. It allows a particular computer to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. DMZ allows a machine to be exposed for that purpose. The Barricade supports one DMZ host computer at a time per public IP address that you have at your disposal.

Q. What is “Discard Ping From WAN Side”?

A. This provided added firewall security. Enabling this feature stops the router from responding to pings from Internet users.

PING: Packet INternet Groper - An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Q. How do I enable the Remote Admin feature?

A. You need to enter the IP address of the WAN location from where you plan to remotely administer the router. If you do not know the IP beforehand, then you can set the remote management value to 0.0.0.0 and this will command the router to allow ANY machine access to the router (of course the user must know the password in order to log in and change any settings). To actually access the router web console, you need to type in the router's WAN IP (shown on the Status page) and type :8080 afterwards. (i.e. - http://24.24.24.24:8080)

This does not allow you to access machines behind the router. In order to accomplish that feat, you would have to install server software on that computer (i.e. – ftp, web, or pc anywhere server)

Q. How can I get a Multi Homed server to be accessible from the LAN side of the Barricade?

Let's say you have 2 or more websites running off of one server and people from the internet side of the Barricade can get to the websites fine by typing in the Domain name. You will not be able to reach the website from the LAN side by doing the same. Even typing the IP address on the LAN side will bring up some default Microsoft page given by the program used to create the websites. The problem was the internal routing of the DNS.

This situation is also known as a (Multi Homed) setup, which is basically multiple domain names hosted by one server.

A. Create a "Hosts" file in the default windows directory and point the IP address to the domain name.

The entries look like this:

192.168.2.XXX www.computerresources.com

192.168.2.XXX www.computerIO.com

192.168.2.XXX www.computerwhatever.com

(Where the "XXX" refers to the IP Address of the server doing the Hosting and the space in-between the # and the name is made by hitting the "tab" key.)

Q. How does the Barricade determine the time?

A. The Barricade is obtaining the correct time from the internet using SNTP protocol. So the gateway can get the time from NTP server in the internet.

Simple Network Time Protocol (SNTP)

The Simple Network Time Protocol (SNTP) is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC-1305 is not needed or justified. It can operate in both unicast modes (point-to-point) and broadcast modes (point-to-multipoint). It can also operate in IP multicast mode where this service is available. SNTP involves no change to the current or previous NTP specification versions or known implementations, but rather a clarification of certain design features of NTP which allow operation in a simple, stateless remote-procedure call (RPC) mode with accuracy and reliability expectations similar to the UDP/TIME protocol described in RFC-868.

Troubleshooting: ISP Specific

CABLE MODEM SERVICES

Q. @Home Services (Comcast@Home, At&t@Home, etc.)

A. You need to obtain your exact HOST NAME from the ISP. Many @home service NO LONGER use host names, however, this varies from ISP to ISP. You can contact your provider for more info or you can follow the directions below:

Windows 9x/Me

- 1) Go to the Control Panel
- 2) Double-click on Network
- 3) Go to the Identification tab and write down the computer name (it will most likely be in a cc43567-a format)

Windows 2K/XP

- 1) Go to the Control Panel
- 2) Double-click on System
- 3) Go to the Network tab and write down the computer name

Now that you have the host name, you will be able to configure the router to connect to your ISP. Simply log into the unit by going into <http://192.168.2.1> and click on the Setup Wizard. Then select the Cable Modem radio button and write in the host name exactly as you wrote it down earlier. Then click the Finish button. The router should connect to the Internet within seconds. If not, go to the Status page. On the left "Internet" column, it may say Cable/DSL Disconnected at this point. If so, then go ahead and recycle the power on the modem and router and set up the router for "Cable Modem" again.

If you continue to have problems, download the latest firmware available for download from our site: <http://www.smc.com/>

Q. Adelphia / Videotron / Cox Communications / Telus.NET

A In most cases, this setup will only require simply cloning the MAC address of the network card. You need to log in to the router at <http://192.168.2.1> and go to the Advanced Setup section. Then go to the WAN section and click on the "Dynamic IP" button, then press "CloneMAC Address" and press APPLY. Wait about 10 seconds and then click on the "Status" link. On the left "Internet" column, it should state Cable/DSL Connected at this point. If so, then you are online. If it still says Disconnected, then turn off the router and the cable modem for about 5

minutes. Then turn them back on, log into the router again, and see if it says connected. If not, then you may require a host name. Follow the procedures shown for @Home customers to determine exactly what your host name is. Then enter this name in the "Dynamic IP" section and that should get you connected.

If you continue to have problems, download the latest firmware available for download from our site: <http://www.smc.com/>

Q. Other Cable Services

A. In most cases, this setup will only require simply cloning the MAC address of the network card. You need to log in to the router at <http://192.168.2.1> and go to the Advanced Setup section. Then go to the WAN section and click on the "Dynamic IP" button, then press "CloneMAC Address" and press APPLY. Wait about 10 seconds and then click on the "Status" link. On the left "Internet" column, it should state Cable/DSL Connected at this point. If so, then you are online. If it still says Disconnected, then turn off the router and the cable modem for about 5 minutes. Then turn them back on, log into the router again, and it should be connected.

If you continue to have problems, download the latest firmware available for download from our site: <http://www.smc.com/>

Troubleshooting: ISP Specific

DSL MODEM SERVICES

Q. General DSL Services

A. Most DSL services provide DHCP to their customers, however, they require a username and password in order to log into the service. This is

called PPP over Ethernet. You need to verify exactly what your login and password is for your service. Then log into the router at <http://192.168.2.1>, go to the "Advanced Setup" section and click on "WAN". Then click on "PPPoE". You will then see fields for your login and your password. Enter this information exactly as provided by the ISP. In most cases, you should leave the Service Name blank. Then press the "Apply" button. The router should automatically establish a connection to the WAN. Go to the "Status" section, and under the "Internet" column, it should say Cable/DSL Connected. If so, then you are online. If it still says Disconnected, then turn off the router and the DSL modem for about 5 minutes. Then turn them back on, log into the router again, and it should be connected.

Tips

- 1) Earthlink customers may need to enter their full email address for the "User Name". See examples below:
 - a. ELN/username@earthlink.net
 - b. username@earthlink.net
 - c. you may also need to enter "Earthlink DSL" as the Service Name
- 2) Below is a list of services that may require the full email address for the "User Name" (much like Earthlink DSL).
 - a. Mindspring (username@mindspring.com)
 - b. Ameritech (username@ameritech.net)
 - c. MTS Sympatico Business (username@res.mts.net)
 - d. Bell Canada (username@on.aibn.com or username@qc.aibn.com)
 - e. Pacific Bell (username@pacbell.net)
 - f. SBC (username@sbcglobal.net)

If you continue to have problems, download the latest firmware available for

Troubleshooting: Third Party Applications

Q. Why can't I access my ISP's resources, such as their mail and news servers?

A. If the servers have simple names like 'mail' or 'news', then you will need to replace those server names with the IP addresses. You can find these server names in the account properties of the email client software. They should be labeled POP3 and SMTP servers. Call your ISP for more details on how to change the POP3 and SMTP server addresses to exact IP addresses or domain names.

Q. How do I get PC Anywhere to work with the Barricade?

A: The default setting is enough to connect to a PC Anywhere **host** on the WAN side; it is not necessary to configure the router in this scenario.

To setup a PC Anywhere host on the LAN side, you have to setup Virtual Server for ports 5631, 5632 and 22. For example:

<u>ID</u>	<u>Service IP</u>	<u>Private Port</u>	<u>Public Port</u>
1	192.168.2.7*	5631 TCP	5631 TCP
2	192.168.2.7*	22 UDP	22 UDP
3	192.168.2.7*	5632 UDP	5632 UDP

* This is the LAN IP address of your machine that you are using the PC Anywhere application on.

If you want to setup more than one PC Anywhere host on your LAN, then you would need to configure your PC Anywhere host to listen to different port numbers, (i.e.: 5641/5642). You can find out how to change these ports in the program's Help wizard are on Symantec's web site.

Q. How do I set up the router to work with Netmeeting?

A. MS Netmeeting is a router-unfriendly application simply because of that fact that it uses dynamic ports - meaning that every time the application is opened, it is using different ports to operate. Hence, this application does not work well behind any NAT firewall. Some customers have been able to get this application to work by opening up all the ports for certain triggers. This is definitely not recommended by SMC, but we can provide you with the information these customers have given us. Beyond this, there is nothing else that can be done. If this info does not solve your problem, please contact Microsoft.

Triggers = 389, 522, 1503, 1024, 1720, 1731
Incoming ports (the same for all triggers) = 1-64535

All the ports are TCP. You can also try putting your machine in the DMZ (through Misc. Items) and make sure that you have upgraded the firmware on the router.

Q. I cannot DCC send or access some other functions of IRC.

A. Here is the information that we have on IRC.

IRC DCC / IRC DCC.

The IRC port is usually 6667, but is sometimes 7000
OUT TCP 6667

or

OUT TCP 7000

IN TCP 113

IRC Chat

OUT TCP 100

IN TCP 101

IRC Fserve

OUT TCP 110

IN TCP 111

IRC IDENT

IN UDP 113

IRC Send

OUT TCP 120

IN TCP 121

IRC Get

OUT TCP 130

IN TCP 131

You need to open the appropriate ports in the router's firewall and you will be able to operate IRC as you usually do. You can put this information in Virtual Server and/or Special Applications. Try setting the above ports (i.e. - 113, 6667, 7000, 120, 130, etc) as Triggers and then set the incoming ports to 6667,7000,100-131. Also, go into Virtual Server and put in 113, 6667, 7000, etc. as Service Ports along with your IP Address (the public ports equal the private ports). Lastly, if you still have problems, try setting the public ports in Special Applications to 1-64535 (note: this opens a WIDE range of ports).

Q. How do I configure the router to work with MSN Messenger?

A. Here is all the info we have on MSN Messenger:

MSN Messenger

NOTE: Shut off any personal firewall programs such as BlackIce, ZoneAlarm, etc.

Ports 6891-6900 enable File send,

Port 6901 is for voice communications

Allows Voice, PC to Phone, Messages, and Full File transfer capabilities.

IN TCP 6891 - 6900

IN TCP 1863

IN UDP 1863

IN UDP 5190

IN UDP 6901

IN TCP 6901

Try setting 6891,6900, and 6901 as triggers. Then set the public ports to 1863,5190-6901. If that does not work, set the incoming ports to 1-64535 (note: this opens a WIDE range of ports) and add in 5190 and 1863 as

triggers. You can also try putting your machine in the DMZ (go into Misc. Items). Make sure that you have upgraded the firmware as well.

Q. How do I configure ICQ to work through the firewall?

A. Here is all the info we have on ICQ:

ICQ

In ICQ under "Preferences & security", "Preferences" and Connections, click on "I am behind a firewall or proxy" then click on "Firewall Settings". Then select "I don't have a SOCKS Proxy server on my firewall" or "I am using another Proxy server". Click Next. Click "Use the following TCP listen ports for incoming event" and set the TCP ports for 20000 to 20019 for the first user, 20020 to 20039 for the second user, 20040 to 20059 for the third user, etc.

OUT UDP 4000

IN TCP 20000 20019 for one user

OR

IN TCP 20000 20039 for two users

OR

IN TCP 20000 20059 for three users, etc.

Try setting 4000, 20000, 20019, and 20039 as triggers. Then set the public ports to 4000, 20000-20039. If you still have problems, set the public ports to 1-64535 (note: this opens a WIDE range of ports). You can also try putting your machine in the DMZ (go into Misc. Items) and make sure that you have the latest firmware.

Q. How do I configure ICU to work with the router?

A. Here is all the info we have on ICU:

ICU Client

OUT TCP 2019

IN TCP 2000 2038

IN TCP 2050 2051

IN TCP 2069

IN TCP 2085

IN TCP 3010 3030

OUT TCP 2000 2038

OUT TCP 2050 2051

OUT TCP 2069

OUT TCP 2085

OUT TCP 3010 3030

Try setting 2000, 2050, 2069, 2085, 3010, and 2019 as triggers. Then set the public ports to 2000-3030. If you still experience problems, set the public ports to 1-64535 (note: this opens a WIDE range of ports). You can also try putting your machine in the DMZ (go into Misc. Items) and make sure that you have the latest firmware.

Q. How do I get an MSN Game to work properly through the firewall?

A. Here is all the info we have on the Gaming Zone:

MSN Game Zone

IN TCP 6667

IN TCP 28800 - 29000

for DX play also open these ports:

IN TCP 47624

IN TCP 2300 - 2400

IN UDP 2300 - 2400

Try setting 6667, 28800, 29000, 47624, 2300, and 2400 as triggers. Then set the public ports to 2300-2400,28800-29000,6667,47624. If you still experience problems, set the public ports to 1-64535 (note: this opens a WIDE range of ports). You can also try putting your machine in the DMZ (go into Misc. Items) and make sure that you have the latest firmware.

Support Info:

<http://support.microsoft.com/support/kb/articles/q159/0/31.asp>

DX support page

<http://support.microsoft.com/support/kb/articles/Q240/4/29.ASP>

<http://support.microsoft.com/support/kb/articles/q236/4/30.asp>

Q. How do I set up an ftp server behind the router?

A. You need to set up the router to forward your ftp ports to your server machine. Simply log into the router and click on Virtual Server. Then put in the ftp port that you are running your server on (standard port is 21). Also, enter in a service port that is one number below your ftp port (i.e. - if you put in 21, you will also need to put 20). This is the data port. Then where it says 192.168.2.XXX, type in the last octet of the SERVER machine's IP address. Then set the public and private ports to TCP. Your colleagues can then connect to your server by using the PUBLIC IP that your ISP has given you. In the current version of firmware, the virtual server loop-back does not

work. So you will not be able to test the server yourself by putting in the WAN IP.

<u>ID</u>	<u>Service IP</u>	<u>Private Port</u>	<u>Public Port</u>
1	192.168.2.7*	20 TCP	20 TCP
2	192.168.2.7*	21 TCP	21 TCP

* This is the LAN IP address of your machine that you are using the FTP application on.

Q. If I set the FTP server to any port besides 21, clients cannot connect to my server.

A. This is because the clients that are connecting are ALSO behind some sort of router. In this situation, you MUST run your FTP server on port 21.

Q. How do I configure the router to work with CuSeeMe?

A. Unfortunately, CuSeeMe has officially stated that their program does not work through NAT routers. See the link below:

<http://support.cuseeme.com/cu3win/faq/cufaq097.htm>

Q. How do I configure the router to work with Paltalk?

A. Here is all the info we have on Paltalk:

Pal Talk

Each computer using Pal Talk must use a different OUT port number, starting at 5001 and incrementing by 1.

OUT TCP 5001

IN UDP 2090 2091 [voice]

IN TCP 2090 2091

IN TCP 2095 [file transfer]

IN TCP 5200 5203 [answering service (future)]

IN TCP 8080 [video]

IN UDP 8090 - 8290 [group voice]

Try setting 5001, 2090, 2095, 5200, 8080, and 8090 as triggers. Then set the public ports to 8080-8290,5000-5203,2090-2095. If you still experience problems, set the public ports to 1-64535 (note: this opens a WIDE range of

ports). You can also try putting your machine in the DMZ (go into Misc. Items) and make sure that you have the latest firmware.

Support Info:

<http://www.paltalk.com/paltalk/support/network/index.htm>

Q. How do I set up windows file sharing on my LAN?

A. Note that this is a Windows configuration issue and is not supported by SMC Networks. The site shown below will walk you through the setup step by step:

<http://www.wown.com>

Q. How do I set up the router to work with BattleNet/Diablo games?

A. Here is all the info we have on BattleNet:

BattleNet/Diablo

Trigger	Public ports
---------	--------------

4000	4000,6112-6119
6112	4000,6112-6119
6113	4000,6112-6119
6114	4000,6112-6119
6115	4000,6112-6119
6116	4000,6112-6119
6117	4000,6112-6119
6118	4000,6112-6119
6119	4000,6112-6119

Set up the Special Applications section as shown above (all ports are TCP). If you still experience problems, set the public ports to 1-64535 (note: this opens a WIDE range of ports). You can also try putting your machine in the DMZ (go into Misc. Items) and make sure that you have the latest firmware.

Glossary

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

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

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

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

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

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

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DHCP - Dynamic Host Configuration Protocol. This protocol automatically configures the TCP/IP settings of every computer on your home network.

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

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

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

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

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

Fixed IP – (see Static IP)

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

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

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

ISP - Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

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

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

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

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

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

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

NAT – (Network Address Translation) This process allows all of the computers on your home network to use one IP address. The NAT capability of the Barricade, allows you to access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP. Network Address Translation can be used to give multiple users access to the Internet with a single user account, or to map the local address for an IP server (such as Web or FTP) to a public address. This secures your network from direct attack by hackers, and provides more flexible management by

allowing you to change internal IP addresses without affecting outside access to your network. NAT must be enabled to provide multi-user access to the Internet or to use the Virtual Server function.

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

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

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

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

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

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

TCP/IP - Transmission Control Protocol/Internet Protocol. This is the standard protocol for data transmission over the Internet.

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

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

LIMITED WARRANTY

SMC's Limited Warranty Statement

Limited Warranty Statement: SMC Networks Europe ("SMC") warrants its products to be free from defects in workmanship and materials, under normal use and service, for the applicable warranty term. All SMC products carry a standard 2 year limited warranty from the date of purchase from SMC or its Authorized Reseller. SMC may, at its own discretion, repair or replace any product not operating as warranted with a similar or functionally equivalent product, during the applicable warranty term. SMC will endeavour to repair or replace any product returned under warranty within 30 days of receipt of the product. As new technologies emerge, older technologies become obsolete and SMC will, at its discretion, replace an older product in its product line with one that incorporates these newer technologies

The standard limited warranty can be upgraded to a 5 year Limited Lifetime * warranty by registering new products within 30 days of purchase from SMC or its Authorized Reseller. Registration can be accomplished via the enclosed product registration card or online via the SMC web site. Failure to register will not affect the standard limited warranty. The Limited Lifetime warranty covers a product during the Life of that Product, which is defined as a period of 5 years from the date of purchase of the product from SMC or its authorized reseller.

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

Customers must contact SMC for a Return Material Authorization number prior to returning any product to SMC. Proof of purchase may be required. Any product returned to SMC without a valid Return Material Authorization (RMA) number clearly marked on the outside of the package will be returned to customer at customer's expense. Customers are responsible for all shipping charges from their facility to SMC. SMC is responsible for return shipping charges from SMC to customer.

LIMITED WARRANTY

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

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

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

* Under the limited lifetime warranty, internal and external power supplies, fans, and cables are covered by a standard one-year warranty from date of purchase.

LIMITED WARRANTY

Full Installation Manual

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

Firmware and Drivers

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

Contact SMC

Contact details for your relevant countries are available on www.smc-europe.com and www.smc.com.

Statement of Conditions

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

Limitation of Liability

In no event, whether based in contract or tort (including negligence), shall SMC be liable for incidental, consequential, indirect, special or punitive damages of any kind, or for loss of revenue, loss of business or other financial loss arising out of or in connection with the sale, installation, maintenance, use, performance, failure or interruption of its products, even if SMC or its authorized reseller has been advised of the possibility of such damages.

Copyright

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

Trademarks

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