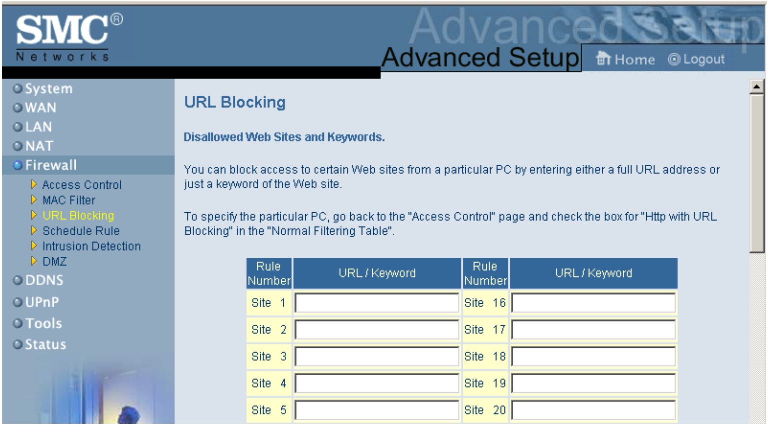
The MAC Filtering feature of the Wireless Barricade allows you to control access to your network to up to 32 clients based on the MAC (Media Access Control) Address of the client machine. This ID is unique to each network adapter. If the MAC address is listed in the table, that client machine will have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

URL Blocking

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

To complete this configuration, you will need to create or modify an access rule in “Access Control” on page 51. To modify an existing rule, click the Edit option next to the rule you want to modify. To create a new rule, click on the Add PC option.

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



URL Blocking

Disallowed Web Sites and Keywords.

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

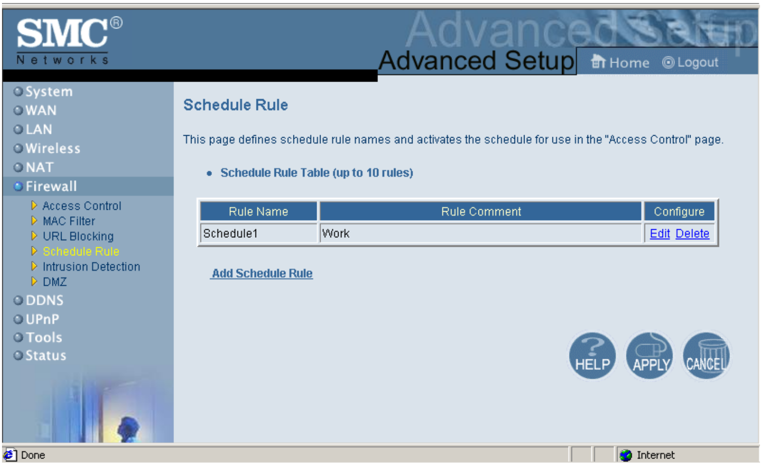
To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	

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

Schedule Rule

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



Schedule Rule

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

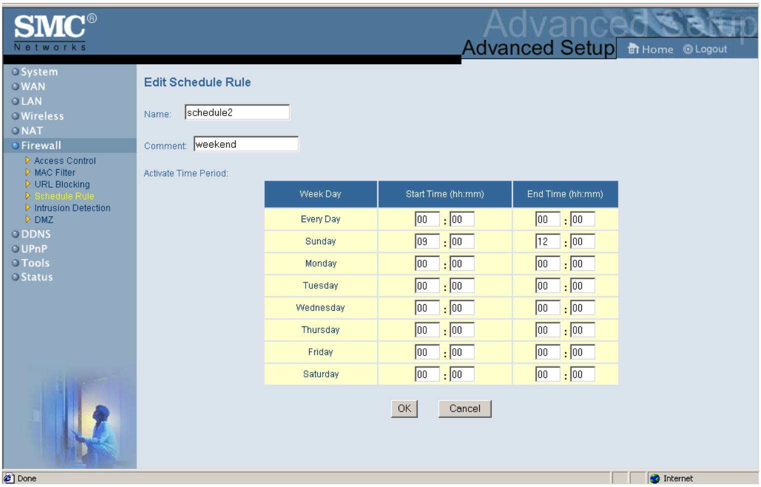
- Schedule Rule Table (up to 10 rules)

Rule Name	Rule Comment	Configure
Schedule1	Work	Edit Delete

Add Schedule Rule

Enables Schedule-based Internet access control.

1. Click Add Schedule Rule.
2. Define the settings for the schedule rule (as shown on the following screen).



Edit Schedule Rule

Name: schedule2

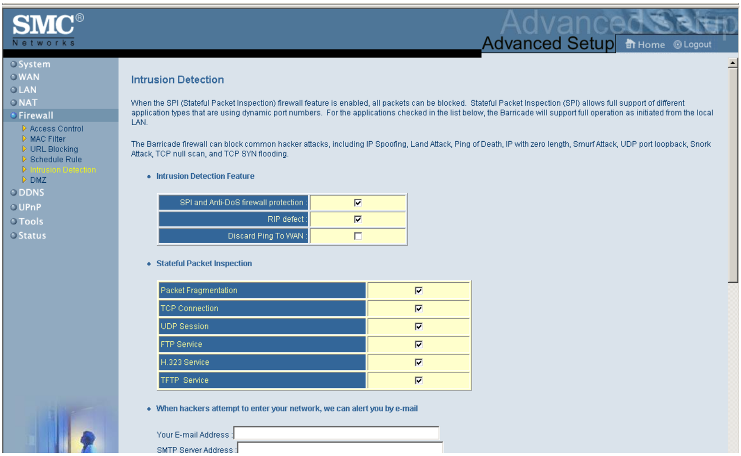
Comment: weekend

Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	00 : 00	00 : 00
Sunday	09 : 00	12 : 00
Monday	00 : 00	00 : 00
Tuesday	00 : 00	00 : 00
Wednesday	00 : 00	00 : 00
Thursday	00 : 00	00 : 00
Friday	00 : 00	00 : 00
Saturday	00 : 00	00 : 00

3. Click OK and then click the APPLY button to save your 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

SPI and Anti-DoS firewall protection :	☑
RIP defect :	☑
Discard Ping To WAN :	☐

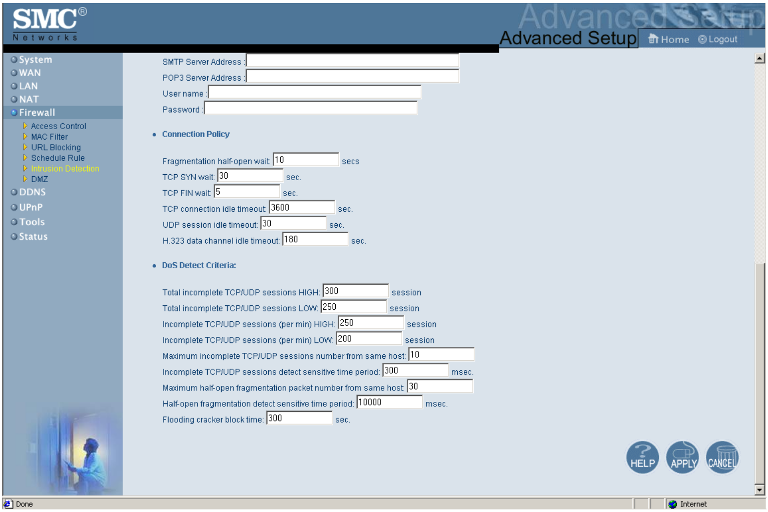
- Stateful Packet Inspection

Packet Fragmentation	☑
TCP Connection	☑
UDP Session	☑
FTP Service	☑
H.323 Service	☑
TFTP Service	☑

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

Your E-mail Address :

SMTP Server Address :



SMTP Server Address :
POP3 Server Address :
User name :
Password :

- Connection Policy

Fragmentation half-open wait: 10 secs
TCP SYN wait: 30 sec.
TCP FIN wait: 5 sec.
TCP connection idle timeout: 3600 sec.
UDP session idle timeout: 30 sec.
H.323 data channel idle timeout: 180 sec.

- DoS Detect Criteria:

Total incomplete TCP/UDP sessions HIGH: 300 session
Total incomplete TCP/UDP sessions LOW: 250 session
Incomplete TCP/UDP sessions (per min) HIGH: 250 session
Incomplete TCP/UDP sessions (per min) LOW: 200 session
Maximum incomplete TCP/UDP sessions number from same host: 10
Incomplete TCP/UDP sessions detect sensitive time period: 300 msec.
Maximum half-open fragmentation packet number from same host: 30
Half-open fragmentation detect sensitive time period: 10000 msec.
Flooding cracker block time: 300 sec.

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

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

- **Discard Ping from WAN (Default: Disabled)** – Prevents a PING on the Gateway’s WAN port from being routed to the network.

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

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

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

- **When hackers attempt to enter your network, we can alert you by e-mail** – Enter your E-mail address. Specify your SMTP and POP3 servers, user name, and password.

- **Connection Policy** – Enter the appropriate values for TCP/UDP sessions as described in the following table.

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

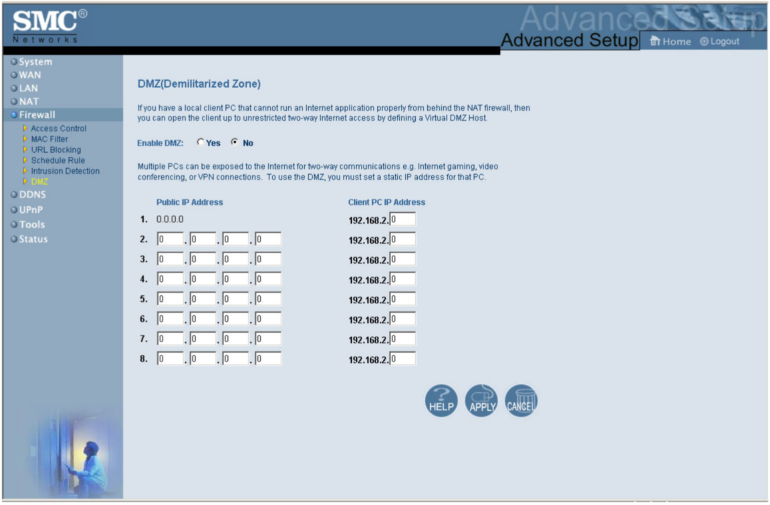
DoS Criteria and Port Scan Criteria

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

Parameter	Defaults	Description
Total incomplete TCP/UDP sessions HIGH	300 sessions	Defines the rate of newly unestablished sessions that will cause the software to *start* deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of newly unestablished sessions that will cause the software to *stop* deleting half-open sessions.
Incomplete TCP/UDP sessions (per min.) HIGH	250 sessions	Maximum number of allowed incomplete TCP/UDP sessions per minute.
Incomplete TCP/UDP sessions (per min.) LOW	200 sessions	Minimum number of allowed incomplete TCP/UDP sessions per minute. Set this to “0” if no minimum setting is required.
Maximum incomplete TCP/UDP sessions number from same host	10 sessions	Maximum number of incomplete TCP/UDP sessions from the same host.
Incomplete TCP/UDP sessions detect sensitive time period	300 msec	Length of time before an incomplete TCP/UDP session is detected as incomplete.
Maximum half-open fragmentation packet number from same host	30	Maximum number of half-open fragmentation packets from the same host.
Half-open fragmentation detect sensitive time period	1sec	Length of time before a half-open fragmentation session is detected as half-open.

Parameter	Defaults	Description
Flooding cracker block time	300 sec	Length of time from detecting a flood attack to blocking of the attack.

DMZ



DMZ(Demilitarized Zone)

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

Enable DMZ: ○ Yes ● No

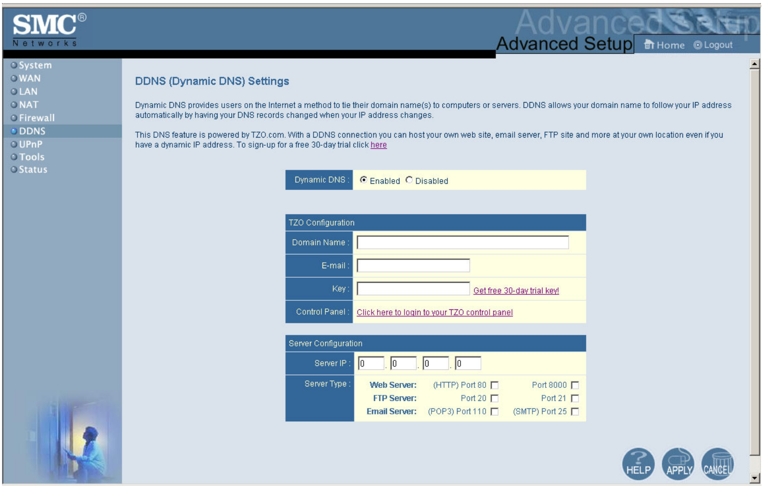
Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

	Public IP Address	Client PC IP Address
1.	0.0.0.0	192.168.2.0
2.	0 . 0 . 0 . 0	192.168.2.0
3.	0 . 0 . 0 . 0	192.168.2.0
4.	0 . 0 . 0 . 0	192.168.2.0
5.	0 . 0 . 0 . 0	192.168.2.0
6.	0 . 0 . 0 . 0	192.168.2.0
7.	0 . 0 . 0 . 0	192.168.2.0
8.	0 . 0 . 0 . 0	192.168.2.0

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

DDNS (Dynamic DNS) Settings

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



DDNS (Dynamic DNS) Settings

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

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

Dynamic DNS : ● Enabled ○ Disabled

TZO Configuration

Domain Name :

E-mail :

Key : Get free 30-day trial key!

Control Panel : Click here to login to your TZO control panel

Server Configuration

Server IP : 0 . 0 . 0 . 0

Server Type :

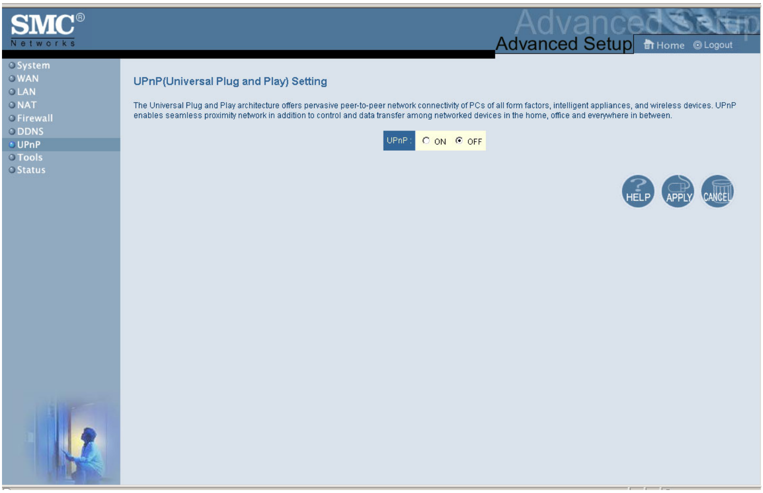
Web Server:	(HTTP) Port 80 □	Port 8000 □
FTP Server:	Port 20 □	Port 21 □
Email Server:	(POP3) Port 110 □	(SMTP) Port 25 □

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

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

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

UPnP (Universal Plug and Play) Setting



UPnP(Universal Plug and Play) Setting

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the home, office and everywhere in between.

UPnP : ○ ON ● OFF

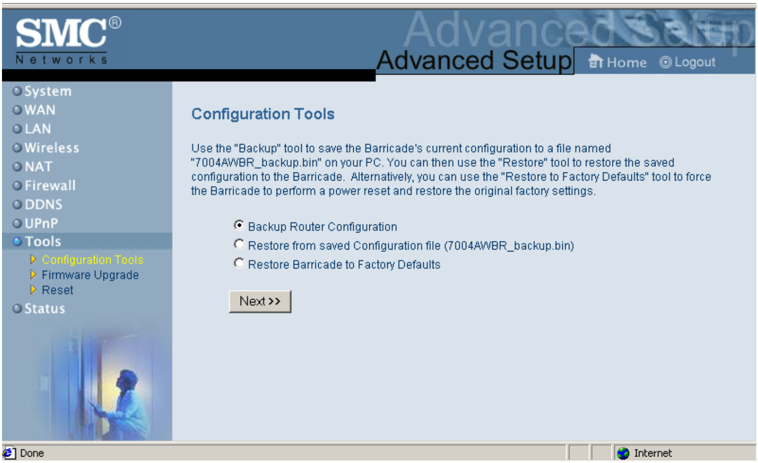
Enable UPnP by checking ON in the screen above. UPnP allows the device to automatically:

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

Tools

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

Tools - Configuration Tools



Configuration Tools

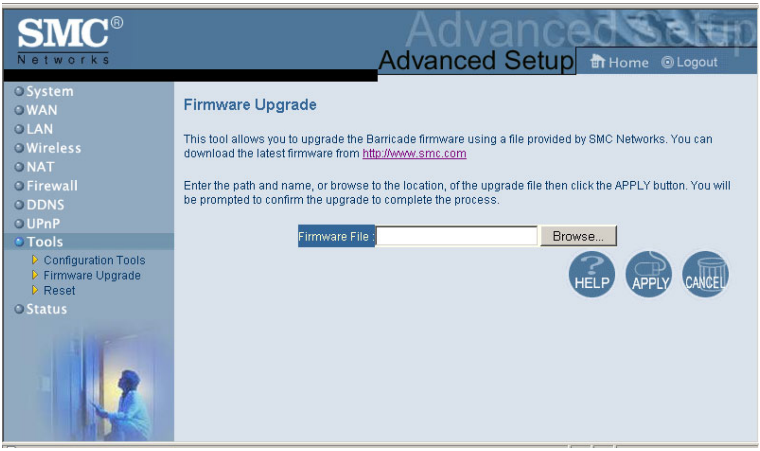
Use the "Backup" tool to save the Barricade's current configuration to a file named "7004AWBR_backup.bin" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Barricade. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Barricade to perform a power reset and restore the original factory settings.

● Backup Router Configuration
○ Restore from saved Configuration file (7004AWBR_backup.bin)
○ Restore Barricade to Factory Defaults

Next >>

- Backup – saves the Wireless Barricade’s configuration to a file.
- Restore – restores settings from a saved backup configuration file.
- Restore to factory defaults – restores the Wireless Barricade settings back to the factory default original.

Tools - Firmware Upgrade



Firmware Upgrade

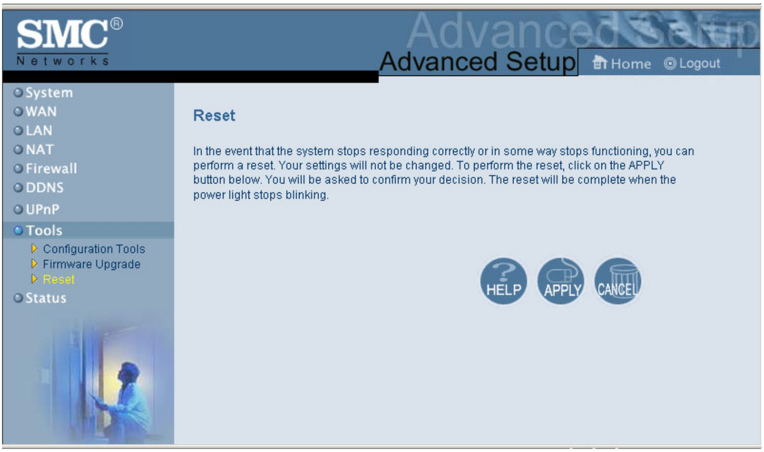
This tool allows you to upgrade the Barricade firmware using a file provided by SMC Networks. You can download the latest firmware from http://www.smc.com

Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.

Firmware File :

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

Tools - Reset



Reset

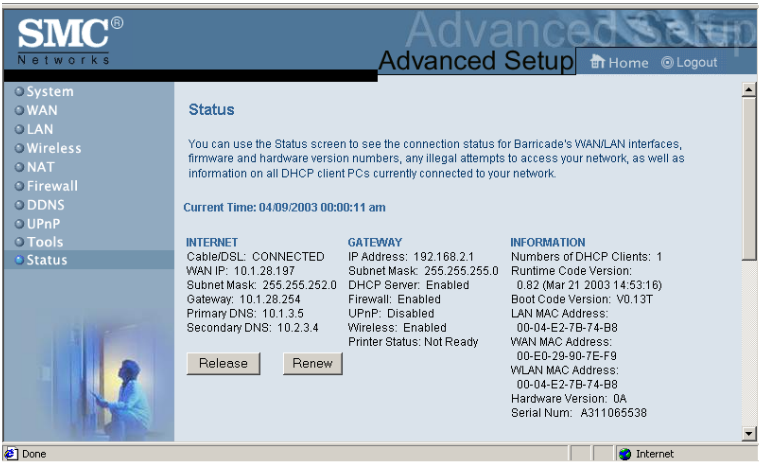
In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.

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

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

Status

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



Status

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

Current Time: 04/09/2003 00:00:11 am

INTERNET
Cable/DSL: CONNECTED
WAN IP: 10.1.28.197
Subnet Mask: 255.255.252.0
Gateway: 10.1.28.254
Primary DNS: 10.1.3.5
Secondary DNS: 10.2.3.4

GATEWAY
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
Firewall: Enabled
UPnP: Disabled
Wireless: Enabled
Printer Status: Not Ready

INFORMATION
Numbers of DHCP Clients: 1
Runtime Code Version:
0.82 (Mar 21 2003 14:53:16)
Boot Code Version: V0.13T
LAN MAC Address:
00-04-E2-7B-74-B8
WAN MAC Address:
00-E0-29-90-7E-F9
WLAN MAC Address:
00-04-E2-7B-74-B8
Hardware Version: 0A
Serial Num: A311065538

The following items are included on this screen:

Section	Description
INTERNET	Displays WAN connection type and status.
GATEWAY	Displays system IP settings, as well as DHCP and Firewall status.
INFORMATION	Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, as well as the hardware version and serial number.
Security Log	Displays illegal attempts to access your network.
Save	Click on this button to save the security log file.
Clear	Click on this button to delete the access log.
Refresh	Click on this button to refresh the screen.
DHCP Client Log	Displays information on all DHCP clients on your network.

Configuring the Print Server

If you want to use the print server built into the Wireless Barricade, then you must first install the Port Monitor program as described in the following section for Windows 95/98/Me/NT/2000.

To configure the Wireless Barricade Print Server for Windows 95/98/Me/NT/2000, or Unix, see “Configure the Print Server” on page 70.

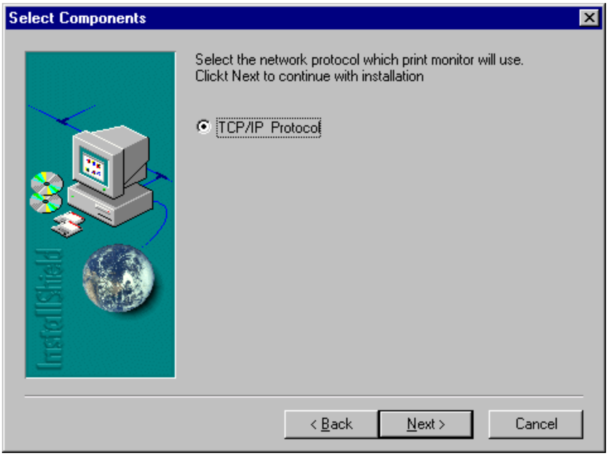
Install the SMC Printer Port Monitor

Skip this section if you are using Unix.

For Windows 95/98/Me/NT/2000 clients, you need to install the port monitor program as described in this section.

1. Insert the installation CD-ROM into your CD-ROM drive. Under the Print Server directory, run the setup.exe program. The SMC Port Monitor installation program advises you to close all other Windows programs currently running on your computer. Click Next to continue.

2. The next screen indicates that the print client uses TCP/IP network protocol to monitor print requests. Click Next.

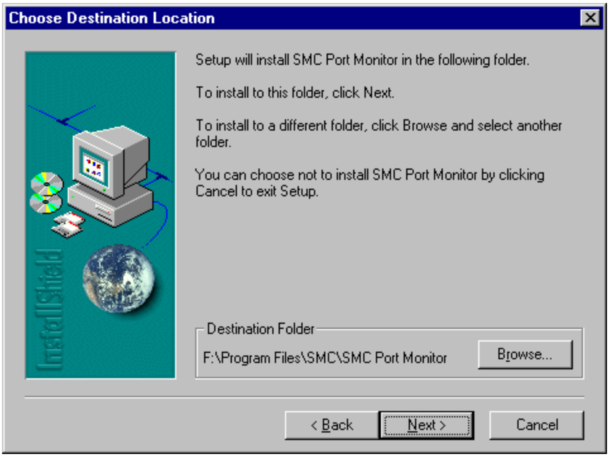


Select Components

Select the network protocol which print monitor will use.
Clickt Next to continue with installation

● TCP/IP Protocol

3. Select the destination folder and click on the Next button. The setup program will then begin to install the programs into the destination folder.



Choose Destination Location

Setup will install SMC Port Monitor in the following folder.

To install to this folder, click Next.

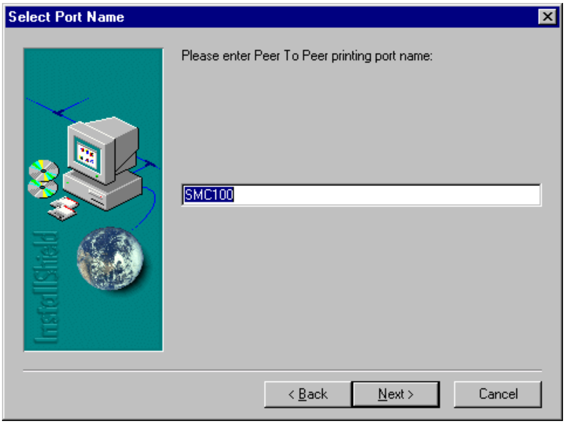
To install to a different folder, click Browse and select another folder.

You can choose not to install SMC Port Monitor by clicking Cancel to exit Setup.

Destination Folder
F:\Program Files\SMC\SMC Port Monitor

4. Select the Program Folder that will contain the program icon for uninstalling the port monitor, and then click Next.

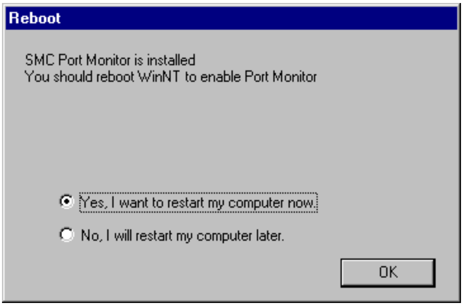
5. Enter the printer port name that will be used to identify the port monitor in your system, and press Next.



Please enter Peer To Peer printing port name:

SMC100

6. When the setup program finishes installing the port monitor, check the radio button to restart your computer and then click OK.



SMC Port Monitor is installed
You should reboot WinNT to enable Port Monitor

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

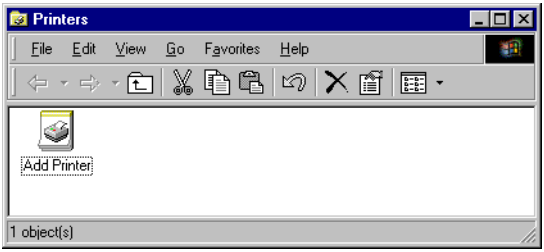
7. After rebooting your computer, add the Wireless Barricade print server to your system as described in the following section.

Configure the Print Server

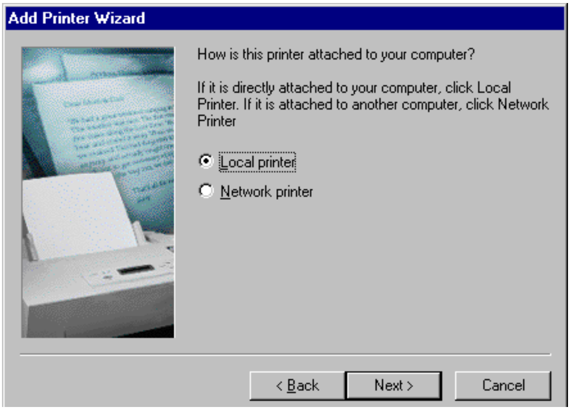
The Wireless Barricade's print server supports Microsoft Windows 95/98/Me/NT/2000, and Unix. If you are using Windows 95/98/Me/NT/2000, first install the port monitor as described in the previous section before adding the Wireless Barricade's print server to your operating system.

Configure the Network Printer in Windows 95/98/Me/2000

1. On a Windows 95/98/Me/2000 platform, open the Printers window in the My Computer menu, and double-click the Add Printer icon.



2. Follow the prompts to add a Local printer to your system. Specify the printer type attached to the Wireless Barricade.



Add Printer Wizard

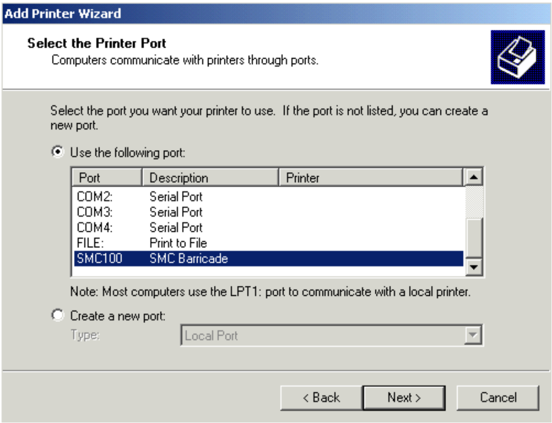
How is this printer attached to your computer?

If it is directly attached to your computer, click Local Printer. If it is attached to another computer, click Network Printer

● Local printer

○ Network printer

3. Select the monitored port (the default port name is SMC100) and then click the Create a new port button.



Add Printer Wizard

Select the Printer Port
Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

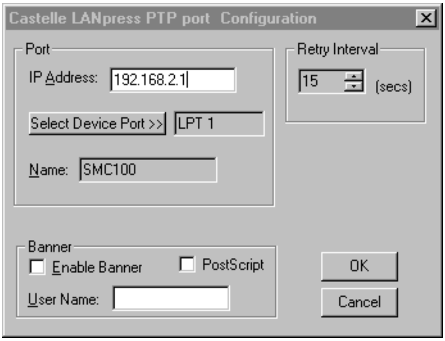
● Use the following port:

Port	Description	Printer
COM2:	Serial Port	
COM3:	Serial Port	
COM4:	Serial Port	
FILE:	Print to File	
SMC100	SMC Barricade	

Note: Most computers use the LPT1: port to communicate with a local printer.

○ Create a new port:
Type: Local Port

4. Enter the IP address of the Wireless Barricade and click OK, and then click Next in the Add Printer Wizard dialog box.



Castelle LANpress PTP port Configuration

Port

IP Address: 192.168.2.1

Select Device Port >> LPT 1

Name: SMC100

Retry Interval

15 (secs)

Banner

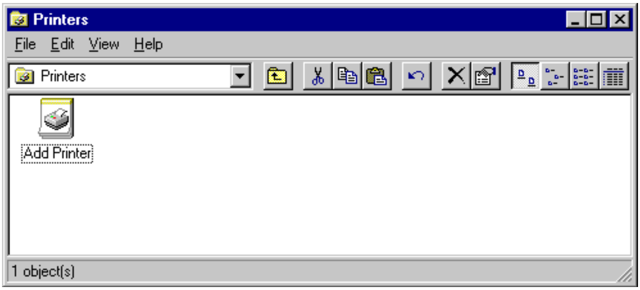
□ Enable Banner □ PostScript

User Name:

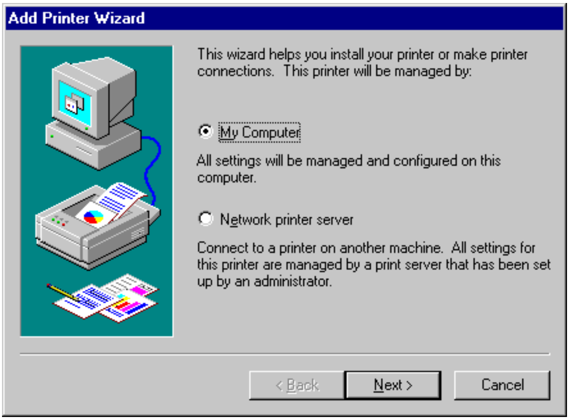
5. Continue following the prompts to finish installing the Wireless Barricade print server. The printer type you specified will now be added to your Printers menu.

Configure the Network Printer in Windows NT

1. On a Windows NT platform, open the Printers window in the My Computer menu, and double-click the Add Printer icon.



2. Follow the prompts to add a local printer to your system.



This wizard helps you install your printer or make printer connections. This printer will be managed by:

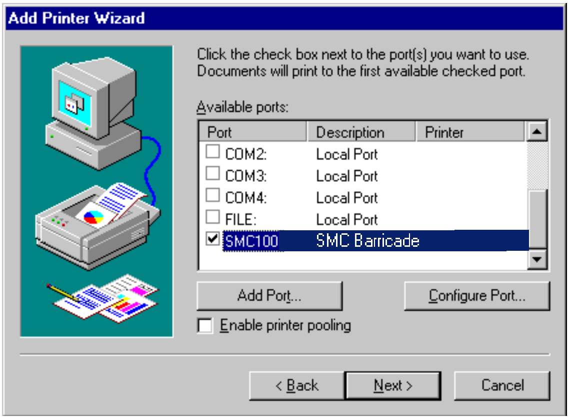
● My Computer

All settings will be managed and configured on this computer.

○ Network printer server

Connect to a printer on another machine. All settings for this printer are managed by a print server that has been set up by an administrator.

3. Select the monitored port. The default port name is SMC100. Then click the Configure Port button.



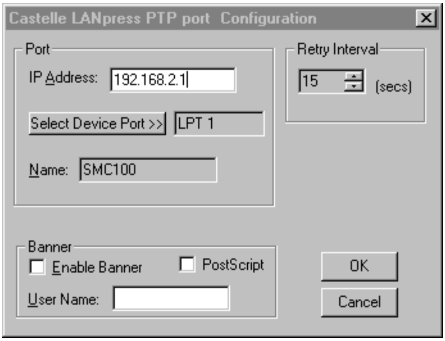
Click the check box next to the port(s) you want to use. Documents will print to the first available checked port.

Available ports:

Port	Description	Printer
□ COM2:	Local Port	
□ COM3:	Local Port	
□ COM4:	Local Port	
□ FILE:	Local Port	
☑ SMC100	SMC Barricade	

□ Enable printer pooling

4. Enter the IP address of the Wireless Barricade and click OK, and then click Next in the Add Printer Wizard dialog box.



Castelle LANpress PTP port Configuration

IP Address: 192.168.2.1

LPT 1

Name: SMC100

15 (secs)

☐ Enable Banner ☐ PostScript

User Name:

5. Specify the printer type attached to the Wireless Barricade.

6. Continue following the prompts to finish installing the Wireless Barricade print server. The printer type you specified will now be added to your Printers menu.

Configure the Network Printer in Unix Systems

Follow the traditional configuration procedure on Unix platforms to set up the Wireless Barricade print server. The printer name is lpt1.

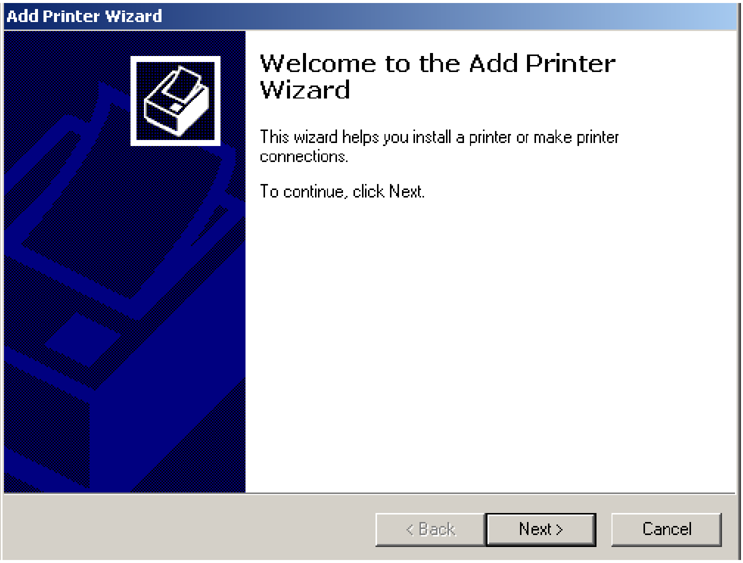
Configure LPR port on Windows 2000/XP

The Wireless Barricade Printer function can also be used with the LPR port on Windows XP and Windows 2000 machines. Below is an outline on how to configure the LPR port on a Windows 2000 machine; however the same steps will apply for a Windows XP.

1. Open the Control Panel.

2. Click on the Printers and Faxes or Printers icon.

3. Click on the Add Printer icon to launch the Add Printer Wizard.



Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

To continue, click Next.

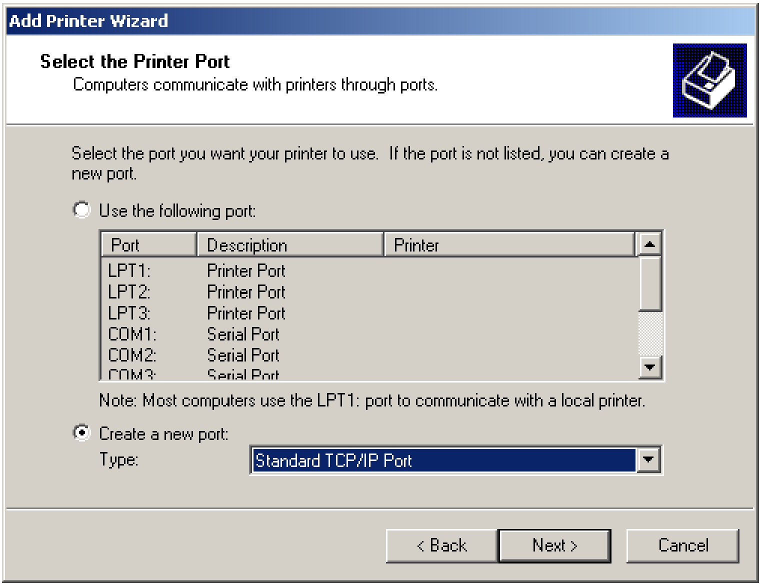
4. Click Next button to begin the printer installation process.

5. On the next dialog box, choose the Local Printer option and verify the “Automatically detect and install my Plug and Play printer” option is unchecked.

Note: On Windows XP check the “Local printer attached to this computer.”

6. Click the Next button to create a new printer port.

7. Select the Create a New Port option and then select the Standard TCP/IP Port option in the drop down menu.



Add Printer Wizard

Select the Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port:

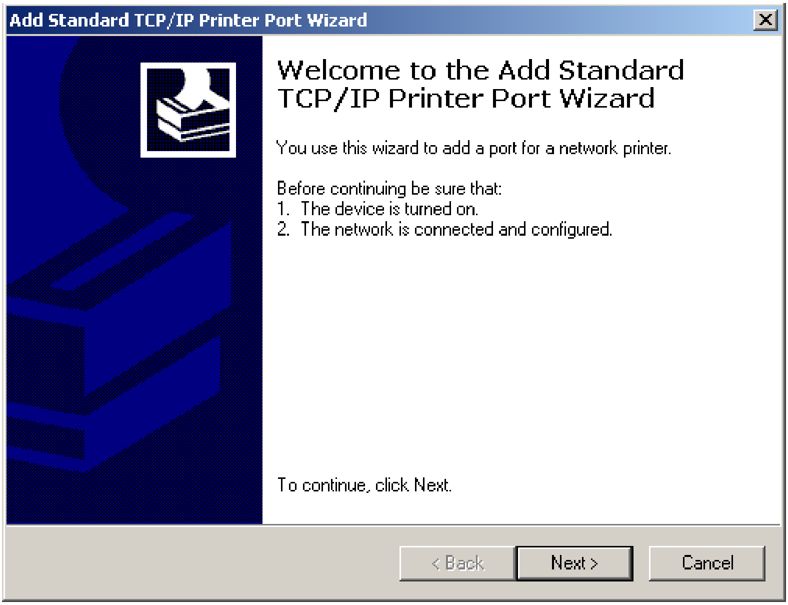
Port	Description	Printer
LPT1:	Printer Port	
LPT2:	Printer Port	
LPT3:	Printer Port	
COM1:	Serial Port	
COM2:	Serial Port	
COM3:	Serial Port	

Note: Most computers use the LPT1: port to communicate with a local printer.

● Create a new port:

Type: Standard TCP/IP Port

8. When you click the Next button the “Add Standard TCP/IP Printer Port Wizard” will launch.



Add Standard TCP/IP Printer Port Wizard

Welcome to the Add Standard TCP/IP Printer Port Wizard

You use this wizard to add a port for a network printer.

Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

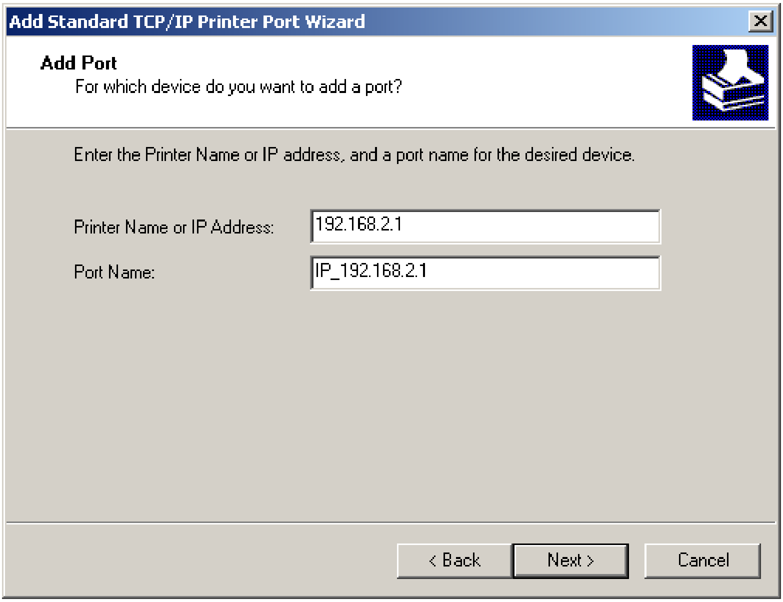
To continue, click Next.

9. To start this new installation wizard click the Next button.

10. Provide the appropriate IP and Port name information for your new Printer port. If you are using default settings on the router you can use the following information:

Printer Name or IP Address: 192.168.2.1 Port Name: IP_192.168.2.

Note: This is the IP that you use to administer your router with (for example: 192.168.2.1). If you have changed this IP address then please use the new one that you have assigned to your router.



Add Standard TCP/IP Printer Port Wizard

Add Port

For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

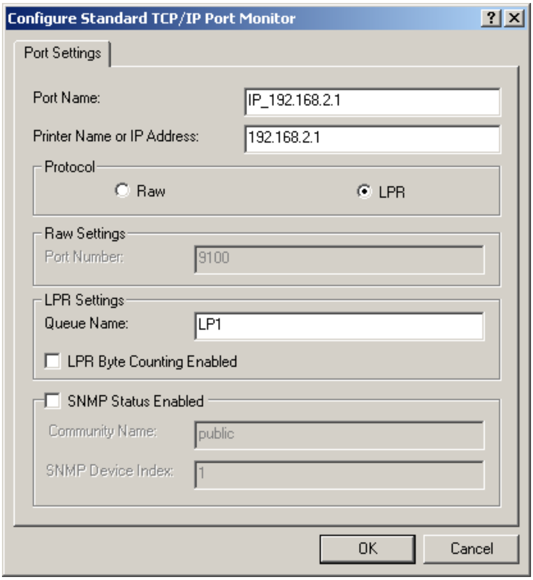
Printer Name or IP Address: 192.168.2.1

Port Name: IP_192.168.2.1

11. Click the Next button to continue

12. On the next dialog box, under the Device type choose the Custom option

13. Then click the Settings… button to input the Specific Wireless Barricade Printer port information.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.2.1

Printer Name or IP Address: 192.168.2.1

Protocol: ○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: LP1

□ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

14. In the Configure Standard TCP/IP Port Monitor dialog box you will need to configure some additional settings. Please confirm these settings below:

- Port Name: IP_192.168.2.1*
- Printer Name or IP Address: 192.168.2.1*

  * This should be the same information that was configured in Step 7.
- In the Protocol section click on the LPR option
- The Raw Settings section should be grayed out
- The LPR Settings section should have the Queue Name set to one of 2 options depending on the version of Wireless Barricade you are using.

- The Queue Name is LPT1.
- Verify the LPR Byte Counting Enabled and SNMP Status Enabled options are unchecked.

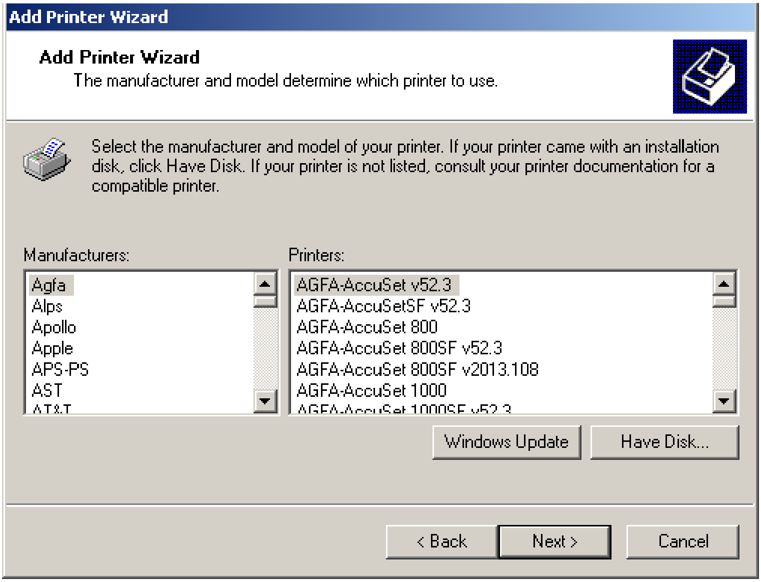
15. Once you have verified all of these settings, click the OK button to save these settings and close the “Configure Standard TCP/IP Port Monitor” window.

16. Click Next to continue and view a summary of the configuration that you have just completed.

17. Click the Finish button to complete the configuration process of the TCP/IP port

18. The Add Printer Wizard will now guide you through the Printer Driver installation for the LPR port you just installed.

19. In the dialog box listed below, choose the manufacturer of the printer that you have, and then choose your model of printer. If your printer is not listed here, then please refer to your printer documentation to get your printer installed.



Add Printer Wizard

Add Printer Wizard

The manufacturer and model determine which printer to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for a compatible printer.

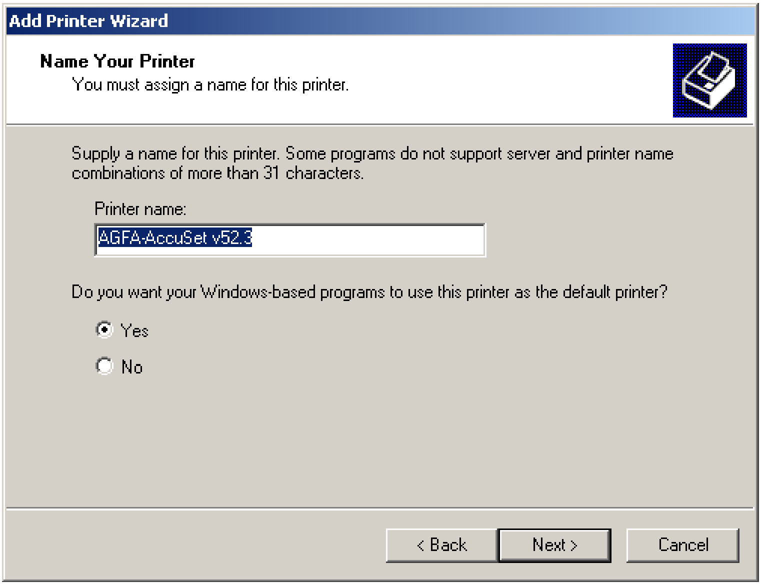
Manufacturers:

Agfa
Alps
Apollo
Apple
APS-PS
AST
AT&T

Printers:

AGFA-AccuSet v52.3
AGFA-AccuSetSF v52.3
AGFA-AccuSet 800
AGFA-AccuSet 800SF v52.3
AGFA-AccuSet 800SF v2013.108
AGFA-AccuSet 1000
AGFA-AccuSet 1000SF v52.3

20. Once you have your printer listed and selected in this dialog box click the Next button.



Add Printer Wizard

Name Your Printer
You must assign a name for this printer.

Supply a name for this printer. Some programs do not support server and printer name combinations of more than 31 characters.

Printer name: AGFA-AccuSet v52.3

Do you want your Windows-based programs to use this printer as the default printer?

● Yes

○ No

21. Name your printer. In this dialog box you will give your installed printer a name; this will be the name this printer is referred to in your Printer folder.

22. Once you have named your printer, click Next to continue.

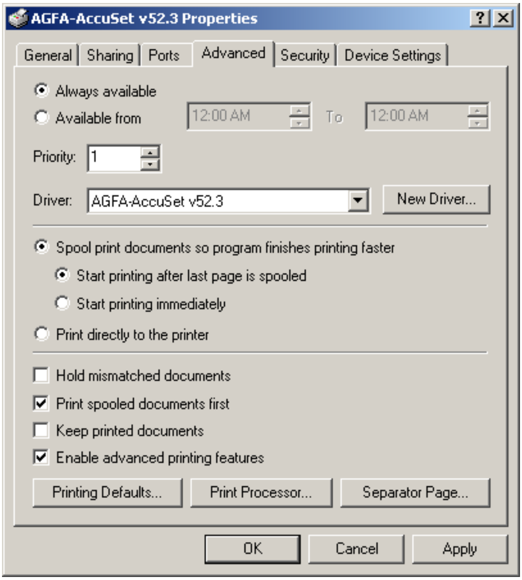
23. Choose the Do not share this printer option and click the Next button.

24. Choose No to the Print Test Page option, and click the Next button.

25. On the next screen, you should now see a dialog box with a summary of all the printer information that you have just configured. To complete the installation, click the Finish button.

Once you have completed the printer installation, you will need to configure some properties on your printer. To do so, please follow the steps listed below:

1. If you closed out the Printers window, please re-open it from the control panel.
2. Locate the printer that you just installed and right-mouse click on it and choose Properties.
3. Click on the Advanced tab and verify the following settings:



AGFA-AccuSet v52.3 Properties

● Always available

○ Available from 12:00 AM To 12:00 AM

Priority: 1

Driver: AGFA-AccuSet v52.3

● Spool print documents so program finishes printing faster

● Start printing after last page is spooled

○ Start printing immediately

○ Print directly to the printer

□ Hold mismatched documents

☑ Print spooled documents first

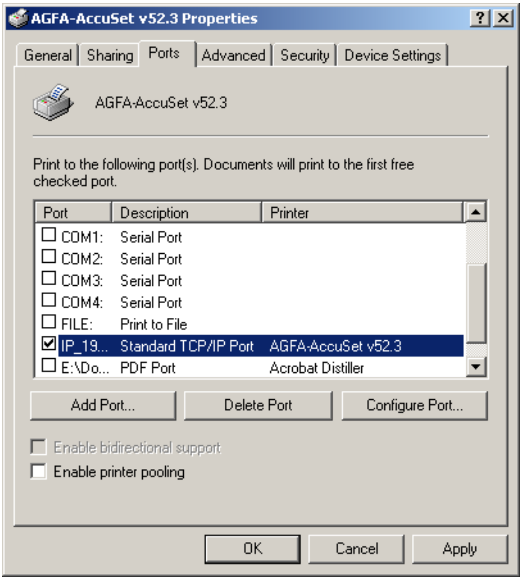
□ Keep printed documents

☑ Enable advanced printing features

- Both the “Spool print documents so program finishes printing faster” and the “Start printing after last page is spooled” options are selected.
- Both the “Print spooled documents first” and “Enable advanced printing features” options are checked.

- All of the other options should be disabled or unchecked.

4. Click on the Ports tab and verify that you have the TCP/IP port that you just created selected and the Enable bidirectional support and Enable printer pooling options are unchecked.



AGFA-AccuSet v52.3

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☐ COM1:	Serial Port	
☐ COM2:	Serial Port	
☐ COM3:	Serial Port	
☐ COM4:	Serial Port	
☐ FILE:	Print to File	
☑ IP_19...	Standard TCP/IP Port	AGFA-AccuSet v52.3
☐ E:\Do...	PDF Port	Acrobat Distiller

☐ Enable bidirectional support

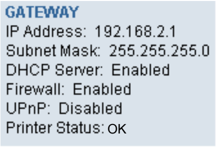
☐ Enable printer pooling

5. Click the Apply button to save the settings.

6. Next click on the General tab and click on the Print Test Page button. This will verify that you have successfully setup your LPR printing port, and now you can print through the SMC Wireless Barricade.

Confirm printer connection

On the status page of the web-based login, you can confirm the printer connection to the Wireless Barricade.



GATEWAY
IP Address: 192.168.2.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled
Firewall: Enabled
UPnP: Disabled
Printer Status: OK

TROUBLESHOOTING

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

The information outlined in this section describes common problems you may encounter and possible solutions to them. The Wireless Barricade can be easily monitored through panel indicators to identify problems. If you cannot resolve any connection problems after checking the indicators, then refer to the other sections in the following table.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Power LED is Off	● External power supply has failed or is disconnected. ● Check connections between the Wireless Barricade, the external power supply, and the wall outlet. ● If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. ● If the unit powers off after running for a while, check for loose power connections, power losses or surges at the power outlet. ● If you cannot isolate the problem, then the external power supply may be defective. In this case, contact SMC Technical Support for assistance.

Troubleshooting Chart	
Symptom	**Action**
LED Indicators	
Link LED is Off	● Verify that the Wireless Barricade and attached device are powered on. ● Be sure the cable is plugged into both the Wireless Barricade and the corresponding device. ● Verify that the proper cable type is used and its length does not exceed specified limits. ● Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. ● Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.

Troubleshooting Chart	
Symptom	**Action**
Network Connection Problems	
Cannot Ping the Wireless Barricade from the attached LAN, or the Wireless Barricade cannot Ping any device on the attached LAN	• Verify that IP addresses are properly configured. For most applications, you should use the Wireless Barricade's DHCP function to dynamically assign IP addresses to any host on the attached LAN. However, if you manually configure any IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Wireless Barricade and attached LAN devices. • Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.
Mobile users cannot access the Wireless Barricade	• Make sure that the Wireless Barricade and all mobile users are configured to use the same radio channel, wireless domain (SSID), and encryption keys. • Ensure that all mobile users are within range of the Wireless Barricade as specified in Appendix C.

Troubleshooting Chart	
Symptom	**Action**
Management Problems	
Cannot connect using the Web browser	● Be sure you have configured the Wireless Barricade with a valid IP address, subnet mask, and default gateway. ● Check that you have a valid network connection to the Wireless Barricade and that the port you are using has not been disabled. ● Check network cabling between the management station and the Wireless Barricade.
Forgot or lost the password	● Press the “Reset” button for at least five seconds on the rear panel to restore the factory defaults.
Printer Server	
The printer cannot print or prints garbage	● Make sure the parallel cable between the Wireless Barricade and printer is connected and is in good condition

SPECIFICATIONS

Below is an outline of the Technical Specifications for the Barricade 2.4GHz 11 Mbps Wireless Cable/DSL Broadband Router (SMC7004AWBR)

Standards
IEEE 802.3 10BASE-T Ethernet
IEEE 802.3u 100BASE-TX Fast Ethernet
IEEE 802.11b

LAN Interface
3 - RJ-45 10/100 Mbps Auto MDI/MDI-X ports

WAN Interface
1- RJ-45 10/100 Mbps Auto MDI/MDI-X port
Serial, 1 RS-232 DB-9 connector

WLAN Interface
Standard: IEEE 802.11b, Direct Sequence Spread Spectrum (DSSS)
Transmission Rate: 11 Mbps, automatic fallback to 5.5, 2 or 1 Mbps
Maximum Channels: US/Canada: 11, Europe (ETSI): 13
Range: Up to 304 m (1000 ft)
Frequency: (US/Canada/Europe) 2.400-2.4835 GHz, Japan: 2.471-2.497 GHz
Sensitivity: 1, 2, 5.5 Mbps: -80 dBm; 11 Mbps: -76 dBm typical
Modulation: CCK, BPSK, QPSK
Encryption: 64-bit/128-bit WEP
Maximum Clients: 128

Printer Interface
Parallel
1 DB-25 printer port

Management
Web management

Advanced Features
Dynamic IP Address Configuration – DHCP, DNS
Firewall – Client privileges, hacker prevention and logging
Virtual Private Network – PPTP, L2TP, IPSec pass-through
Backup Internet Connection –
Dial-on-demand via secondary WAN port
Printer server

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

Temperature
Operating: 0 to 40 °C (32 to 104 °F)
Storage: -20 to 70 °C (-4 to 158 °F)

Dimensions
21.91 x 13.34 x 2.54 cm (8.63 x 5.25 x 1 in.)

Weight
0.68 kg (1.5 lbs)

Input Power
9 V DC (1.0 A)

Maximum Current
0.40 A RMS max.@110 V, 0.87 A RMS max.@240 V

Power Consumption
10 Watts max. @ 100-240 VAC

Heat Dissipation
34.1 BTU/hr max. @ 100-240 VAC

Internet Standards
ARP (RFC 826), IP (RFC 791), ICMP (RFC 792), UDP (RFC 768), TCP (RFC 793), Telnet (RFC 854-859), MD5 (RFC 1321),

BOOTP Extension (RFC 1497), PPP LCP Extension (RFC 1570), PPPoE (RFC 2516), NAT (RFC 1631), PPP (RFC 1661), HTML (RFC 1866), HTTP (RFC 1945), CHAP (RFC 1944), DHCP (RFC 2131), PPTP (RFC 2637)

Temperature
Operating (0 to 40 °C), 32 to 104 °F
Storage (- 40 to 70 °C), - 40 to 158 °F

Humidity
5% to 95% (noncondensing)

Compliances
CE Mark
Emissions
  FCC Class B
  Industry Canada Class B
  EN55022 (CISPR 22) Class B
  C-Tick - AS/NZS 3548 (1995) Class B
  ETS 300 328
  MPT RCR STD-33
Immunity
  EN 61000-3-2/3
  EN 61000-4-2/3/4/5/6/8/11
Safety
  UL 1950
  EN60950 (TÜV)
  CSA 22.2 No. 950

FOR TECHNICAL SUPPORT, CALL:

From U.S.A. and Canada (24 hours a day, 7 days a week)
(800) SMC-4-YOU; (949) 679-8000; Fax: (949) 679-1481
From Europe (8:00 AM - 5:30 PM UK Time)
44 (0) 118 974 8700; Fax: 44 (0) 118 974 8701

INTERNET

E-mail addresses:
techsupport@smc.com
european.techsupport@smc-europe.com
support@smc-asia.com
Driver updates:
http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
World Wide Web:
http://www.smc.com
http://www.smc-europe.com
http://www.smc-asia.com

FOR LITERATURE OR ADVERTISING RESPONSE, CALL:

U.S.A. and Canada:	(800) SMC-4-YOU;	Fax (949) 679-1481
Spain:	34-93-477-4935;	Fax 34-93-477-3774
UK:	44 (0) 1932 866553;	Fax 44 (0) 118 974 8701
France:	33 (0) 41 38 32 32;	Fax 33 (0) 41 38 01 58
Italy:	39 (0) 335 5708602;	Fax 39 02 739 14 17
Benelux:	31 33 455 72 88;	Fax 31 33 455 73 30
Central Europe:	49 (0) 89 92861-0;	Fax 49 (0) 89 92861-230
Nordic:	46 (0) 868 70700;	Fax 46 (0) 887 62 62
Eastern Europe:	34 -93-477-4920;	Fax 34 93 477 3774
Sub Saharian Africa:	27 0126610232;	Fax 27-11 314 9133
North West Africa:	216 71236616;	Fax 216 71751415
CIS:	7 (095) 789 35 73;	Fax 7 (095) 789 35 73
PRC (Beijing):	86-10-8251-1550;	Fax 86-10-8251-1551
PRC (Shanghai):	86-21-6485-9922;	Fax 86-21-6495-7924
Taiwan:	886-2-8797-8006;	Fax 886-2-8797-6288
Asia Pacific:	(65) 6 238 6556;	Fax (65) 6 238 6466
Korea:	82-2-553-0860;	Fax 82-2-553-7202
Japan:	81-3-5645-5715;	Fax 81-3-5645-5716
Australia:	61-2-8875-7887;	Fax 61-2-8875-7777
India:	91 22 5696 2790;	Fax 91 22 5696 2794

SMC®
Networks

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

SMC7004AWBR
Part Number: 01-111234-001
Revision Number E042003-R01 F 1.0