

register a new MAC address for your account. Register the default MAC address of the Router.

Point-to-Point Over Ethernet (PPPoE)

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN (selected), Dynamic IP, PPPoE, Static IP, BigPond, DNS, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'PPPoE' and contains the following text: 'Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again.' Below this text is a note: 'If your Internet Service Provider requires the use of PPPoE, enter the information below.' The configuration fields are: User Name (text box), Password (text box), Please retype your password (text box), Service Name (text box), MTU (1492, with a note '(1440 <= MTU Value <= 1492)'), Maximum Idle Time (0, with a note '(minutes)'), and an Auto-reconnect checkbox. At the bottom right are buttons for HELP, APPLY, and CANCEL.

Enter the PPPoE User Name and Password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers.

The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1454) unless you have a particular reason to change it.

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

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

Configuring the Wireless Barricade g Router

Point-to-Point Tunneling Protocol (PPTP)

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation tree with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing options like Dynamic IP, PPPoE, PPTP, Static IP, BigPond, and DNS. The PPTP option is selected. The main content area is titled 'PPTP' and contains a description: 'Point-to-Point Tunneling Protocol is a common connection method used in European xDSL connections.' Below this is a form with the following fields: PPTP Account, PPTP Password, a field to retype the password, Host Name, Service IP Address, My IP Address, My Subnet Mask, MTU (1400-1460) with a value of 1460 entered, Maximum Idle Time (0-60) minutes, and an Auto-reconnect checkbox. A red note at the bottom states: '* If you have an ISP that charges by the time, change your idle time out value to 1 minute.' At the bottom right are buttons for HELP, APPLY, and CANCEL.

PPTP Account	
PPTP Password	
Please retype your password	
Host Name	
Service IP Address	
My IP Address	
My Subnet Mask	
MTU (1400-1460)	1460
Maximum Idle Time (0-60)	minutes
Auto-reconnect	☐

* If you have an ISP that charges by the time, change your idle time out value to 1 minute.

Point-to-Point Tunneling Protocol (PPTP) can be used to join different physical networks using the Internet as an intermediary. Using the above screen allows client PCs to establish a normal PPTP session and provides hassle-free configuration of the PPTP client on each client PC.

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

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

Static IP Address

The screenshot shows the SMC Networks Advanced Setup web interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under the WAN category, options include Dynamic IP, PPPoE, PPTP, Static IP (which is selected), BigPond, and DNS. The main content area is titled 'Static IP' and contains the following text: 'If your Service Provider has assigned a fixed IP address; enter the assigned IP address, subnet mask and the gateway address provided.' Below this is a question: 'Has your Service Provider given you an IP address and Gateway address?'. There are three input fields, each with a dropdown arrow: 'IP address assigned by your Service Provider', 'Subnet Mask', and 'Service Provider Gateway Address'. At the bottom right of the interface are three circular buttons labeled 'HELP', 'APPLY', and 'CANCEL'.

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

You may need a fixed address if you want to provide Internet services, such as a web server or FTP server.

Configuring the Wireless Barricade g Router

BigPond

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. Under the WAN category, sub-items include Dynamic IP, PPPoE, PPTP, Static IP, BigPond (highlighted in yellow), and DNS. The main content area is titled 'BigPond' and contains the text: 'In this section you can configure the built-in client for the BigPond Internet service available in Australia.' Below this text is a configuration table with four rows, each with a label and a text input field. The rows are: 'User Name', 'Password', 'Please retype your password', and 'Authentication Service Name'. The bottom of the page features three circular buttons: 'HELP' (with a question mark icon), 'APPLY' (with a floppy disk icon), and 'CANCEL' (with an 'X' icon).

BigPond	
User Name	
Password	
Please retype your password	
Authentication Service Name	

BigPond is a service provider in Australia that uses a heartbeat system to maintain the Internet connection. Configure the built-in client with your user name, password and service name to get online. Leave the Authentication Service Name as “login-server” for a universal configuration.

DNS

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The WAN category is expanded, showing options like Dynamic IP, PPPoE, PPTP, Static IP, and BigPond. The main content area is titled 'DNS' and contains a descriptive paragraph about DNS servers. Below the text are two input fields for IP addresses, each split into four segments. The first field is labeled 'Domain Name Server (DNS) Address' and the second is 'Secondary DNS Address (optional)'. At the bottom right are three buttons: HELP, APPLY, and CANCEL.

SMC® Networks Advanced Setup Home Logout

DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.accton.com, a DNS server will find that name in its index and find the matching IP address: 64.147.25.20. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.

Domain Name Server (DNS) Address				
Secondary DNS Address (optional)				

HELP APPLY CANCEL

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

Configuring the Wireless Barricade g Router

LAN

The screenshot shows the 'Advanced Setup' page for an SMC Networks router. The left sidebar contains a navigation menu with options: System, WAN, LAN (selected), Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled 'LAN Settings' and includes a sub-header 'LAN IP'. Below this, there are fields for 'IP Address' (192.168.2.), 'IP Subnet Mask' (255.255.255.0), and 'DHCP Server' (Enabled). A 'Lease Time' dropdown is set to 'Forever'. The 'IP Address Pool' section includes fields for 'Start IP' (192.168.2.), 'End IP' (192.168.2.), and 'Domain Name' (optional). The top right of the page has links for Home and Logout. The bottom right corner features icons for help, save, and print.

- LAN IP – Use the LAN menu to configure the LAN IP address for the Router and to enable the DHCP server for dynamic client address allocation.
- Set a period for the lease time if required. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
- IP Address Pool – A dynamic IP address range may be specified (192.168.2.2–254). IP addresses running from 192.168.2.100 to 192.168.2.199 are the default value. Once the IP addresses, e.g. 192.168.2.100–199, have been assigned, these IP addresses will be part of the dynamic IP address pool. IP addresses from 192.168.2.2 to 192.168.2.99, and 192.168.2.200 to 192.168.2.254 will be available as static IP addresses.

Remember not to include the address of the Router in the client address pool. Also remember to configure your client PCs for dynamic IP address allocation.

Wireless

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

Channel and SSID

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless (selected), NAT, Firewall, DDNS, UPnP, Tools, and Status. The 'Wireless' section is expanded, showing 'Channel and SSID' and 'Encryption'. The main content area is titled 'Channel and SSID' and contains a text box explaining that this page allows defining SSID, Transmission Rate, Basic Rate, and Channel ID for wireless connection. Below this are five configuration fields: SSID (text box with 'default'), Transmission Rate (dropdown menu with 'Fully Automatic'), Basic Rate (dropdown menu with 'All (1, 2, 5.5, 11Mbps)'), Channel (dropdown menu with 'Auto'), and Broadcast SSID (radio buttons for 'Enable' and 'Disable', with 'Enable' selected). At the bottom right are three buttons: HELP, APPLY, and CANCEL.

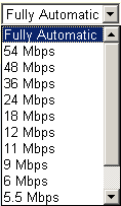
You must specify a common radio channel and SSID (Service Set ID) to be used by the Router and all of your wireless clients. Be sure you configure all of your clients to the same values.

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

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

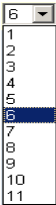
Configuring the Wireless Barricade g Router

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



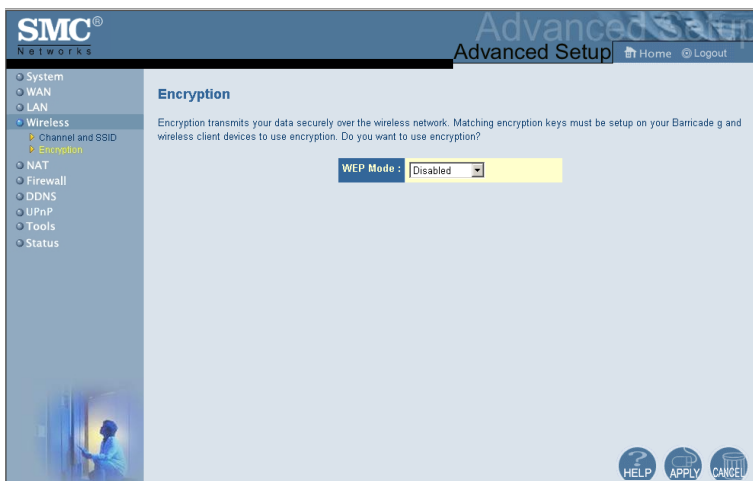
Channel: The radio channel through which the Router communicates with PCs in its BSS. (Default: 6)

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



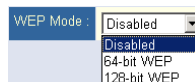
Broadcast SSID: Broadcasting the SSID on the wireless network for easy connection with client PCs. For security reason, disable SSID broadcast. (Default: Enable)

Encryption



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

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



You may manually enter the keys or automatically generate encryption keys. To manually configure the keys, enter five hexadecimal pairs for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.) For automatic 64-bit security, enter a passphrase and click Generate. Four keys will be generated (as shown below). Choose a key from the drop-down list or accept the default key. Automatic 128-bit security generates a single key.

Configuring the Wireless Barricade g Router

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

- Channel and SSID
- Encryption

NAT

Firewall

DDNS

UPnP

Tools

Status

Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Barricade g and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode: 64-bit WEP

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

Passphrase:

Key 1:

Default Key: 1

Key 2:

Key 3:

Key 4:

HELP

APPLY

CANCEL

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

- Channel and SSID
- Encryption

NAT

Firewall

DDNS

UPnP

Tools

Status

Encryption

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Barricade g and wireless client devices to use encryption. Do you want to use encryption?

WEP Mode: 128-bit WEP

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

Passphrase:

Key:

HELP

APPLY

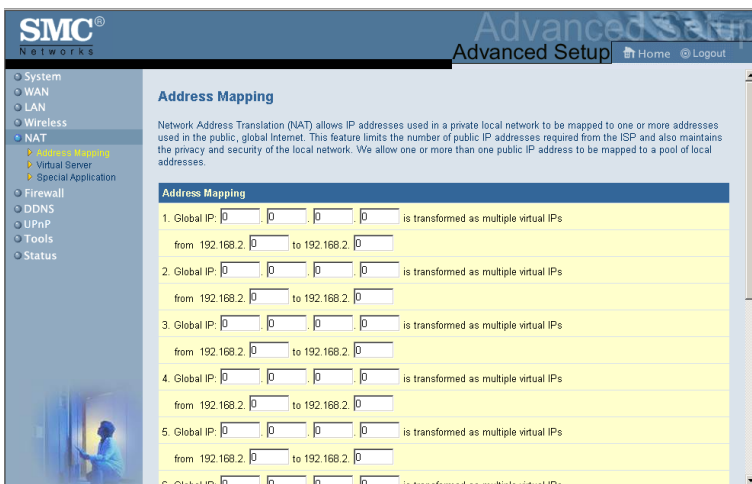
CANCEL

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

NAT - Network Address Translation

From this section you can configure the Address Mapping, Virtual Server, and Special Application features that provide control over the TCP/UDP port openings in the router's firewall. This section can be used to support several Internet based applications such as web, E-mail, FTP, and Telnet

Address Mapping



SMC® Networks Advanced Setup | Home | Logout

Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses.

Address Mapping	
1. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs from 192.168.2. [0] to 192.168.2. [0]
2. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs from 192.168.2. [0] to 192.168.2. [0]
3. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs from 192.168.2. [0] to 192.168.2. [0]
4. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs from 192.168.2. [0] to 192.168.2. [0]
5. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs from 192.168.2. [0] to 192.168.2. [0]
6. Global IP: [0] [0] [0] [0]	is transformed as multiple virtual IPs

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

Configuring the Wireless Barricade g Router

Virtual Server

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

- Address Mapping
- Special Application

Firewall

DDNS

UPnP

Tools

Status

Virtual Server

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

	Private IP	Service Port	Type	Enabled
1.	192.168.2.1		TCP	☐
2.	192.168.2.1		TCP	☐
3.	192.168.2.1		TCP	☐
4.	192.168.2.1		TCP	☐
5.	192.168.2.1		TCP	☐
6.	192.168.2.1		TCP	☐
7.	192.168.2.1		TCP	☐
8.	192.168.2.1		TCP	☐
9.	192.168.2.1		TCP	☐
10.	192.168.2.1		TCP	☐
11.	192.168.2.1		TCP	☐

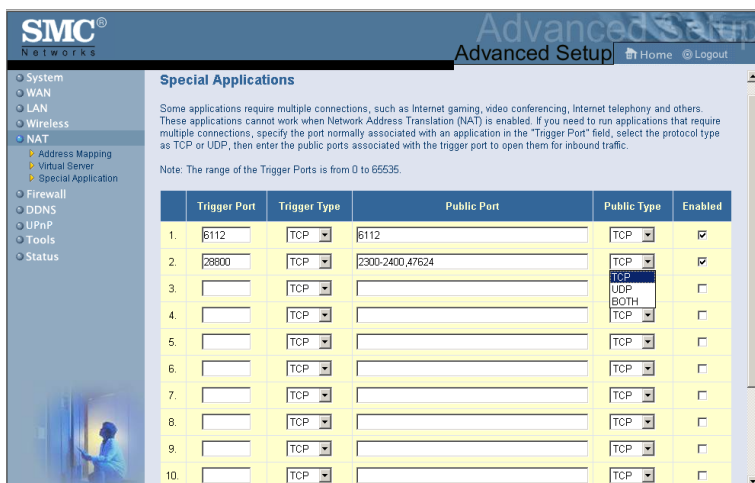
If you configure the Router as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number),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

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

The more common TCP service ports include:
HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110

Special Applications

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



Special Applications

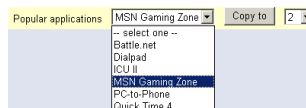
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated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

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

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	6112	TCP	6112	TCP	☒
2.	28800	TCP	2300-2400,47624	TCP	☒
3.		TCP		UDP	☐
4.		TCP		BOTH	☐
5.		TCP		TCP	☐
6.		TCP		TCP	☐
7.		TCP		TCP	☐
8.		TCP		TCP	☐
9.		TCP		TCP	☐
10.		TCP		TCP	☐

Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, then enter the ports that the application requires.

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



Popular applications

MSN Gaming Zone

Copy to 2

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

Configuring the Wireless Barricade g Router

Example:

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	6112	UDP	6112	UDP	Battle.net
2	28800	TCP	2300-2400, 47624	TCP	MSN Game Zone

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

Firewall

The Router firewall can provide access control of connected client PCs, block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network users.

Access Control

SMC® Networks Advanced Setup [Home](#) [Logout](#)

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

Access Control

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.

• Enable Filtering Function : ☐ Yes ☒ No

• Normal Filtering Table (up to 10 computers)

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
Normal	192.168.2.101 ~ 125	WWW, WWW with URL Blocking, FTP, AIM	Always Blocking	Edit Delete

[Add PC](#)

[HELP](#) [APPLY](#) [CANCEL](#)

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

Configuring the Wireless Barricade g Router

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

SMC®
Networks

Advanced Setup
Advanced Setup Home Logout

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

Access Control Add PC

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

Client PC Description: Normal

Client PC IP Address: 192.168.2.101 ~ 125

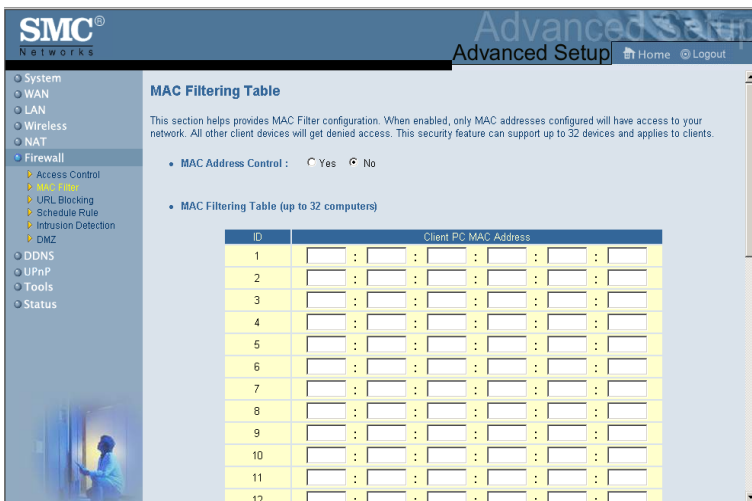
Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3126, 8000, 8080, 8001	☒
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	☒
E-mail Sending	SMTP, TCP Port 25	☐
News Forums	NNTP, TCP Port 119	☐
E-mail Receiving	POP3, TCP Port 110	☐
Secure HTTP	HTTPS, TCP Port 443	☐
File Transfer	FTP, TCP Port 21	☒
MSN Messenger	TCP Port 1863	☐
Telnet Service	TCP Port 23	☐
AIM	AOL Instant Messenger, TCP Port 5190	☒
NetMeeting	H.323, TCP Port 1720	☐
DNS	UDP Port 53	☐
SNMP	UDP Port 161, 162	☐
VPN-PPTP	TCP Port 1723	☐
VPN-L2TP	UDP Port 1701	☐
TCP	All TCP Port	☐
UDP	All UDP Port	☐

User Define Service
Protocol: ☐ TCP ☐ UDP
Port Range: 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0, 0 ~ 0
Scheduling Rule (Ref. Schedule Rule Page): Always Blocking

OK Cancel

MAC Filtering Table



SMC® Networks Advanced Setup [Home](#) [Logout](#)

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

MAC Filtering Table

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

- MAC Address Control : ☐ Yes ☒ No
- MAC Filtering Table (up to 32 computers)

ID	Client PC MAC Address					
1		:		:		:
2		:		:		:
3		:		:		:
4		:		:		:
5		:		:		:
6		:		:		:
7		:		:		:
8		:		:		:
9		:		:		:
10		:		:		:
11		:		:		:
12		:		:		:

The MAC Filtering feature of the Router allows you to control access to your network for 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.

Configuring the Wireless Barricade g Router

URL Blocking

To configure the URL Blocking feature, use the table below to specify the web sites (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 55. 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 web sites and keywords specified below.

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

MAC Filter

URL Blocking

Schedule Rule

Intrusion Detection

DMZ

DDNS

UPnP

Tools

Status

URL Blocking

Disallowed Web Sites and Keywords.

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 the "Access Control" section. 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.

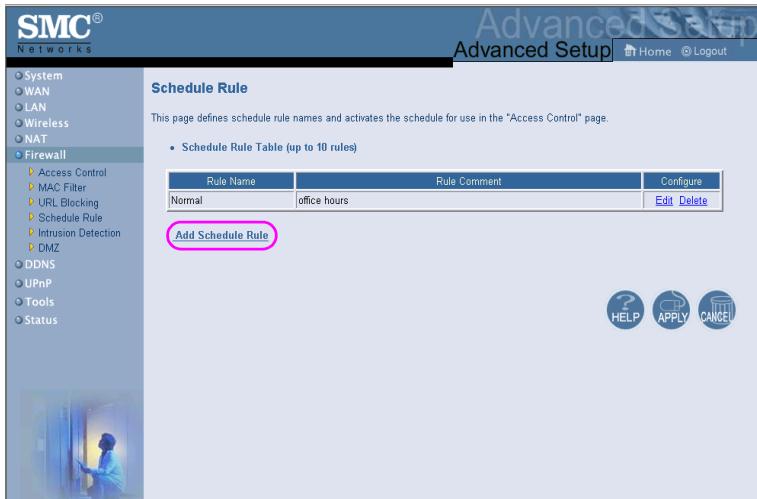
From the "Access Control Add PC" section check the option for "WWW with URL Blocking" in the Client PC Service table to filter out the websites and keywords specified below.

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

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.



The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall (selected), DDNS, UPnP, Tools, and Status. Under the Firewall category, sub-items include Access Control, MAC Filter, URL Blocking, Schedule Rule (highlighted), Intrusion Detection, and DMZ. The main content area is titled "Schedule Rule" and includes a description: "This page defines schedule rule names and activates the schedule for use in the 'Access Control' page." Below this is a section for the "Schedule Rule Table (up to 10 rules)". A table with three columns is shown: "Rule Name", "Rule Comment", and "Configure". The first row contains the text "Normal" under "Rule Name", "office hours" under "Rule Comment", and "Edit Delete" under "Configure". Below the table is a button labeled "Add Schedule Rule", which is circled in pink in the original image. At the bottom right of the main area are three circular buttons: "HELP", "APPLY", and "CANCEL".

SMC[®] Networks

Advanced Setup | Home | Logout

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
Normal	office hours	Edit Delete

Add Schedule Rule

HELP APPLY CANCEL

Configuring the Wireless Barricade g Router

Enables Schedule-based Internet access control.

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

SMC®
Networks

Advanced Setup

Home Logout

System

WAN

LAN

Wireless

NAT

Firewall

Access Control

MAC Filter

URL Blocking

Schedule Rule

Intrusion Detection

DMZ

DDNS

UPnP

Tools

Status

Edit Schedule Rule

Use this section to create your network schedule rules.

The times you set below are the times periods that you want the Access Control Rule to be active. For example, if you want to block Internet access (block WWW) from 9AM to 5PM during the week. Simply configure 9:00 AM as "Start Time" and 5:00 PM as "End Time" for each weekday - during that time period the user will be unable to access the internet.

Once the schedule rule is setup, you will need to configure or edit an Access Control rule, and select your Schedule Rule that you want to apply to that Access Control rule. You can set the schedule rule at the bottom of the Access Control Configuration page in the "Scheduling Rule" drop-down option.

Schedule Rule Name

Normal

Schedule Rule Comment/Desc

office hours (ex. 10:30AM - 7:45PM)

Current Router Time

2002/01/01 00:35:41 AM

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	: AM	: AM
Sunday	: AM	: AM
Monday	08 : 00 AM	18 : 00 AM
Tuesday	08 : 00 AM	18 : 00 AM
Wednesday	08 : 00 AM	18 : 00 AM
Thursday	08 : 00 AM	18 : 00 AM
Friday	08 : 00 AM	18 : 00 AM
Saturday	: AM	: AM