

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. The left sidebar contains a navigation menu with the following items: System, WAN (selected), Dynamic IP, PPPoE (highlighted), 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 sub-heading: "If your Internet Service Provider requires the use of PPPoE, enter the information below." The form fields are: User Name (text input), Password (text input), Please retype your password (text input), Service Name (text input), MTU (1492) (text input with a tooltip "(1440<=MTU Value<=1492)"), Maximum Idle Time (0-60) (text input with a tooltip "(minutes)"), and an Auto-reconnect checkbox (unchecked). At the bottom right of the form are three buttons: HELP, APPLY, and CANCEL.

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

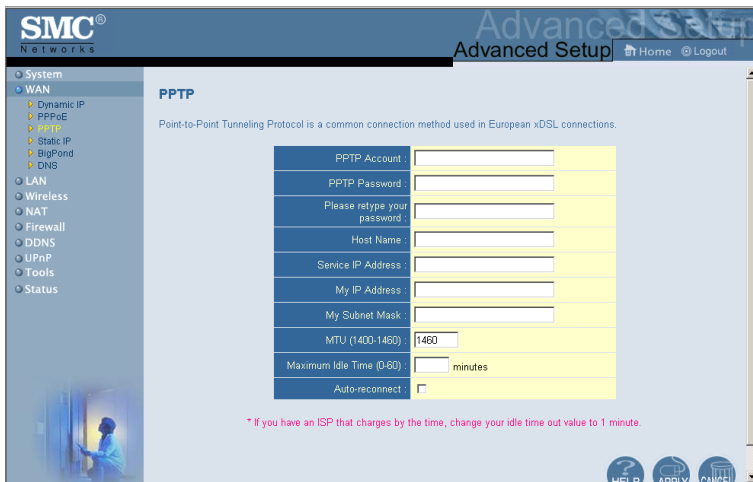
The MTU (Maximum Transmission Unit) governs the maximum size of the data packets. Leave this on the default value (1454) unless you have a particular reason to change it.

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

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)



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



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.

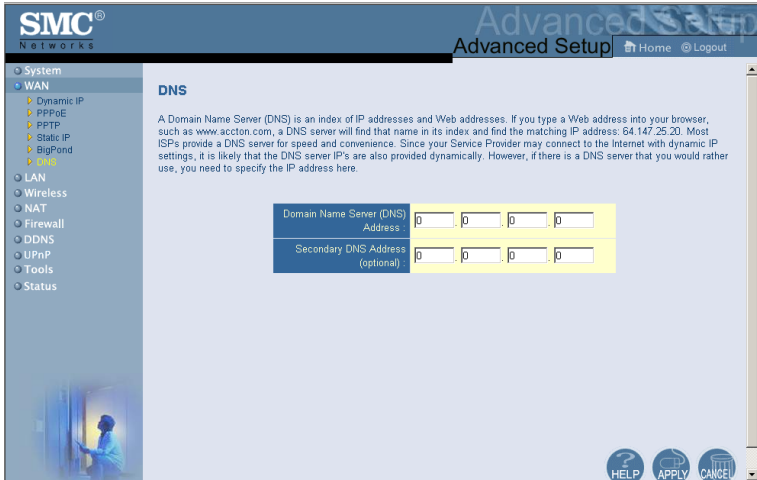
Configuring the Wireless Barricade g Router

BigPond



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



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 'LAN Settings' page in the SMC Networks Advanced Setup interface. The page is titled 'LAN Settings' and includes a navigation menu on the left with options like System, WAN, LAN, Wireless, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is divided into three sections: 'LAN IP', 'Lease Time', and 'IP Address Pool'. Each section contains input fields for configuration. The 'LAN IP' section has fields for IP Address (192.168.2), IP Subnet Mask (255.255.255.0), and DHCP Server (Enabled). The 'Lease Time' section has a dropdown menu set to 'Forever'. The 'IP Address Pool' section has fields for Start IP (192.168.2), End IP (192.168.2), and Domain Name (optional).

- 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. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, Wireless (selected), Channel and SSID (selected), Encryption, NAT, Firewall, DDNS, UPnP, Tools, and Status. The main content area is titled "Channel and SSID" and includes a descriptive paragraph: "This page allows you to define SSID, Transmission Rate, Basic Rate and Channel ID for wireless connection. In the wireless environment, this Blamcade g can also act as a wireless access point. These parameters are used for the mobile stations to connect to this access point." Below the text is a configuration table:

SSID:	default
Transmission Rate:	Fully Automatic
Basic Rate:	All (1, 2, 5.5, 11Mbps)
Channel:	Auto
Broadcast SSID:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

At the bottom right of the interface are three buttons: HELP, APPLY, and CANCEL.

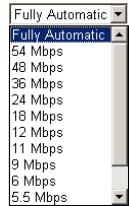
You must specify a common radio channel and SSID (Service Set ID) to be used by the Router and all of your wireless clients. Be sure you configure all of your clients to the same values.

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

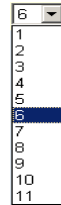
Transmission Rate: Set the rate of data transmitted from the Router. The lower the data rate, the longer the transmission distance. (Default: Fully Automatic.)



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



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

- System
- WAN
- LAN
- Wireless
 - NAT
 - Address Mapping
 - Virtual Server
 - Special Application
- Firewall
 - DDNS
 - UPnP
 - Tools
 - Status

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

The screenshot shows the SMC Networks Advanced Setup interface. On the left is a navigation menu with options: System, WAN, LAN, Wireless, NAT (selected), Address Mapping, Special Application, Firewall, DDNS, UPnP, Tools, and Status. The main area is titled 'Virtual Server' and contains a descriptive paragraph: '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).' Below this text is a table with 11 rows and 5 columns: Index, Private IP, Service Port, Type, and Enabled. The table is currently empty, with all fields in the rows being blank or showing default values like 'TCP' in the Type column.

	Private IP	Service Port	Type	Enabled
1.	192.168.2.1		TCP	<input type="checkbox"/>
2.	192.168.2.1		TCP	<input type="checkbox"/>
3.	192.168.2.1		TCP	<input type="checkbox"/>
4.	192.168.2.1		TCP	<input type="checkbox"/>
5.	192.168.2.1		TCP	<input type="checkbox"/>
6.	192.168.2.1		TCP	<input type="checkbox"/>
7.	192.168.2.1		TCP	<input type="checkbox"/>
8.	192.168.2.1		TCP	<input type="checkbox"/>
9.	192.168.2.1		TCP	<input type="checkbox"/>
10.	192.168.2.1		TCP	<input type="checkbox"/>
11.	192.168.2.1		TCP	<input type="checkbox"/>

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.	8112	TCP	8112	TCP	<input checked="" type="checkbox"/>
2.	28800	TCP	2300-2400,47624	TCP	<input checked="" type="checkbox"/>
3.		TCP		UDP	<input type="checkbox"/>
4.		TCP		BOTH	<input type="checkbox"/>
5.		TCP		TCP	<input type="checkbox"/>
6.		TCP		TCP	<input type="checkbox"/>
7.		TCP		TCP	<input type="checkbox"/>
8.		TCP		TCP	<input type="checkbox"/>
9.		TCP		TCP	<input type="checkbox"/>
10.		TCP		TCP	<input type="checkbox"/>

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

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
- select one --
- Battle.net
- Dialpad
- ICU 11
- MSN Gaming Zone
- PC-to-Phone
- Quick Time 4

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

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).

The screenshot shows the 'Access Control Add PC' configuration page in the SMC Networks Advanced Setup interface. The page includes a navigation menu on the left, a main configuration area with input fields for Client PC Description and Client PC IP Address, a table of Client PC Services, and a 'User Define Service' section at the bottom.

Client PC Description: Normal

Client PC IP Address: 192.168.2.101 ~ 125

Client PC Services:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3126, 8000, 8080, 8001	<input checked="" type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input checked="" 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 checked="" type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	ADL Instant Messenger, TCP Port 5190	<input checked="" type="checkbox"/>
NetMeeting	H.323, TCP Port 1720	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

User Define Service

Protocol: TCP UDP

Port Range: [0-0] [0-0] [0-0] [0-0] [0-0]

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

Buttons: OK, Cancel

MAC Filtering Table

SMC Networks Advanced Setup Home Logout

- System
- WAN
- LAN
- Wireless
- NAT
- Firewall
 - Access Control
 - Port Forwarding
 - URL Blocking
 - Schedule Rules
 - 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.

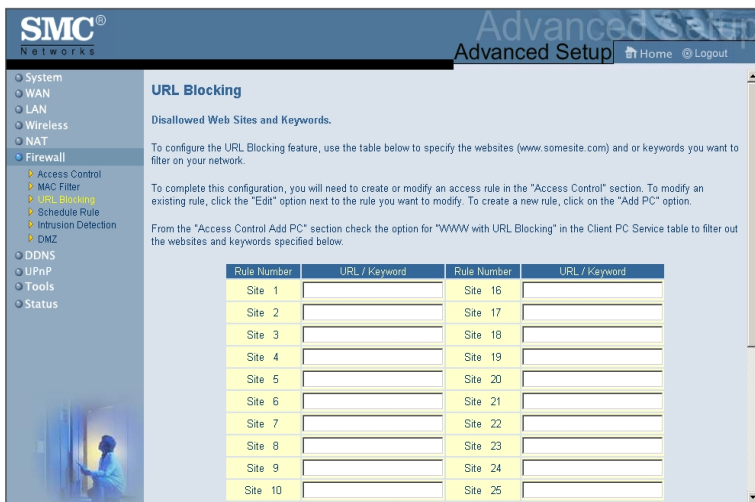
Configuring the Wireless Barricade g Router

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.



The screenshot shows the SMC Networks Advanced Setup interface. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall (selected), Access Control, MAC Filter, URL Blocking (selected), Schedule Rule, Intrusion Detection, DMZ, DDNS, UPnP, Tools, and Status. The main content area is titled "URL Blocking" and includes the following text:

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	<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"/>

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. The left sidebar contains a navigation menu with categories: System, WAN, LAN, Wireless, NAT, Firewall (expanded), DDNS, UPnP, Tools, and Status. The Firewall section includes sub-items: Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, and DMZ. The main content area is titled "Schedule Rule" and contains the text: "This page defines schedule rule names and activates the schedule for use in the 'Access Control' page." Below this text is a "Schedule Rule Table (up to 10 rules)" with the following table:

Rule Name	Rule Comment	Configure
Normal	office hours	Edit Delete

Below the table is a button labeled "Add Schedule Rule" which is circled in pink. At the bottom right of the main content area are three circular buttons: HELP, APPLY, and CANCEL. A small image of a person at a computer is visible in the bottom left corner of the interface.

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.

The screenshot shows the SMC Advanced Setup web interface. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, NAT, Firewall (selected), Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, DMZ, DDNS, UPnP, Tools, and Status. The main content area is titled 'Edit Schedule Rule' and includes a description: '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 8AM to 3PM during the week. Simply configure 9:00 AM as "Start Time" and 9:00 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.'

Configuration fields:

- 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