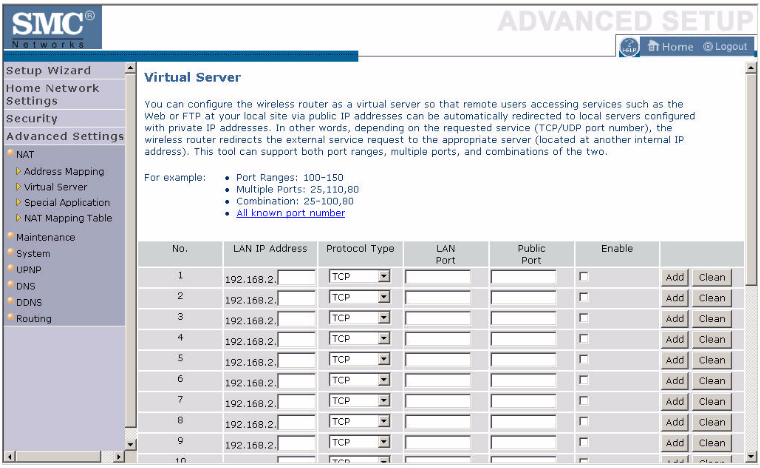
Virtual Server



Virtual Server

You can configure the wireless router 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 wireless router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges, multiple ports, and combinations of the two.

For example:
- Port Ranges: 100-150
- Multiple Ports: 25,110,80
- Combination: 25-100,80
- All known port number

No.	LAN IP Address	Protocol Type	LAN Port	Public Port	Enable	
1	192.168.2.	TCP			☐	Add Clean
2	192.168.2.	TCP			☐	Add Clean
3	192.168.2.	TCP			☐	Add Clean
4	192.168.2.	TCP			☐	Add Clean
5	192.168.2.	TCP			☐	Add Clean
6	192.168.2.	TCP			☐	Add Clean
7	192.168.2.	TCP			☐	Add Clean
8	192.168.2.	TCP			☐	Add Clean
9	192.168.2.	TCP			☐	Add Clean
10						

Using this feature, you can put PCs with public IPs and PCs with private IPs in the same LAN area.

If you configure the Barricade 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 Barricade redirects the external service request to the appropriate server (located at another internal IP address).

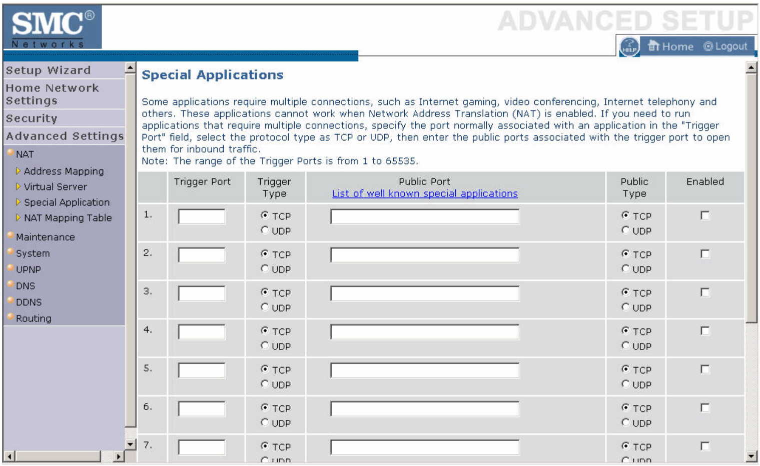
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they 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. Click **All known port number** for more information about public service ports.

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.

Click the **List of well known special applications** link for more information.



Special Applications

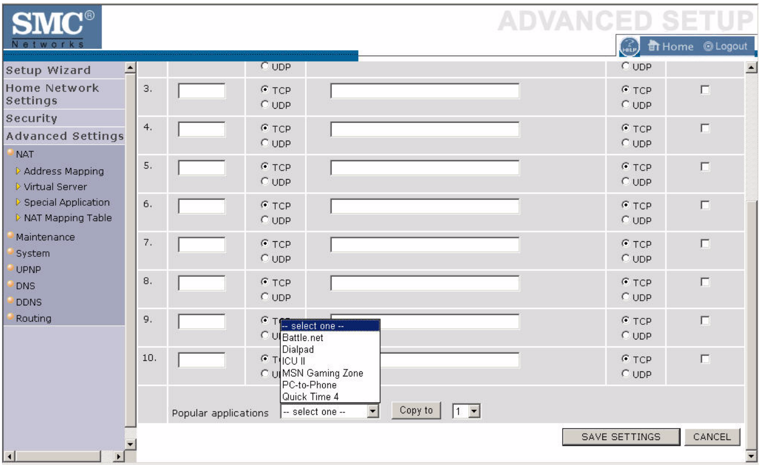
Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated 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 1 to 65535.

	Trigger Port	Trigger Type	Public Port List of well known special applications	Public Type	Enabled
1.		● TCP ○ UDP		● TCP ○ UDP	□
2.		● TCP ○ UDP		● TCP ○ UDP	□
3.		● TCP ○ UDP		● TCP ○ UDP	□
4.		● TCP ○ UDP		● TCP ○ UDP	□
5.		● TCP ○ UDP		● TCP ○ UDP	□
6.		● TCP ○ UDP		● TCP ○ UDP	□
7.		● TCP ○ UDP		● TCP ○ UDP	□

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

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.



		○ UDP		○ UDP	
3.		● TCP ○ UDP		● TCP ○ UDP	□
4.		● TCP ○ UDP		● TCP ○ UDP	□
5.		● TCP ○ UDP		● TCP ○ UDP	□
6.		● TCP ○ UDP		● TCP ○ UDP	□
7.		● TCP ○ UDP		● TCP ○ UDP	□
8.		● TCP ○ UDP		● TCP ○ UDP	□
9.		● TCP ○ UDP		● TCP ○ UDP	□
10.		● TCP ○ UDP		● TCP ○ UDP	□

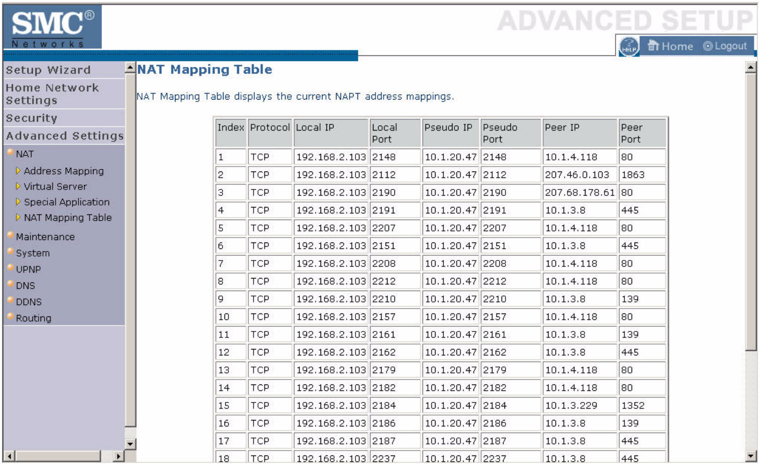
Popular applications -- select one -- Copy to 1

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

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

NAT Mapping Table

This page displays the current NAPT (Network Address Port Translation) address mappings.



NAT Mapping Table

NAT Mapping Table displays the current NAPT address mappings.

Index	Protocol	Local IP	Local Port	Pseudo IP	Pseudo Port	Peer IP	Peer Port
1	TCP	192.168.2.103	2148	10.1.20.47	2148	10.1.4.118	80
2	TCP	192.168.2.103	2112	10.1.20.47	2112	207.46.0.103	1863
3	TCP	192.168.2.103	2190	10.1.20.47	2190	207.68.178.61	80
4	TCP	192.168.2.103	2191	10.1.20.47	2191	10.1.3.8	445
5	TCP	192.168.2.103	2207	10.1.20.47	2207	10.1.4.118	80
6	TCP	192.168.2.103	2151	10.1.20.47	2151	10.1.3.8	445
7	TCP	192.168.2.103	2208	10.1.20.47	2208	10.1.4.118	80
8	TCP	192.168.2.103	2212	10.1.20.47	2212	10.1.4.118	80
9	TCP	192.168.2.103	2210	10.1.20.47	2210	10.1.3.8	139
10	TCP	192.168.2.103	2157	10.1.20.47	2157	10.1.4.118	80
11	TCP	192.168.2.103	2161	10.1.20.47	2161	10.1.3.8	139
12	TCP	192.168.2.103	2162	10.1.20.47	2162	10.1.3.8	445
13	TCP	192.168.2.103	2179	10.1.20.47	2179	10.1.4.118	80
14	TCP	192.168.2.103	2182	10.1.20.47	2182	10.1.4.118	80
15	TCP	192.168.2.103	2184	10.1.20.47	2184	10.1.3.229	1352
16	TCP	192.168.2.103	2186	10.1.20.47	2186	10.1.3.8	139
17	TCP	192.168.2.103	2187	10.1.20.47	2187	10.1.3.8	445
18	TCP	192.168.2.103	2237	10.1.20.47	2237	10.1.3.8	445

The NAT address mappings are listed 20 lines per page, click the control buttons to move forwards and backwards. As the NAT mapping is dynamic, a **Refresh** button is provided to refresh the NAT Mapping Table with the most updated values.

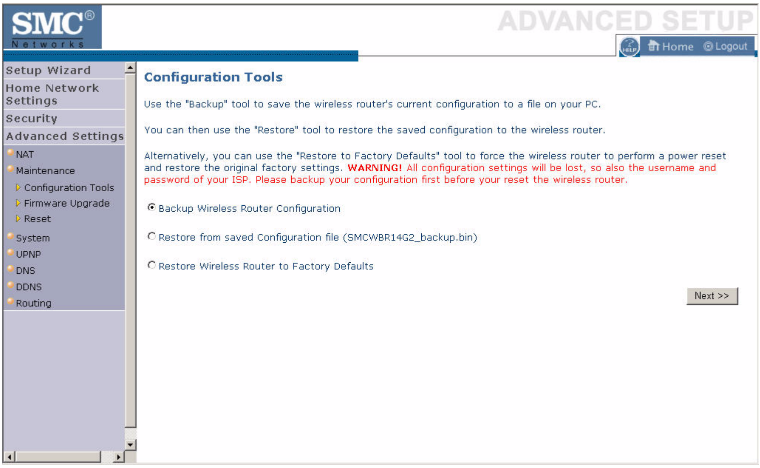
The content of the NAT Mapping Table is described as follows:

- Protocol - protocol of the flow.
- Local IP - local (LAN) host’s IP address for the flow.
- Local Port - local (LAN) host’s port number for the flow.
- Pseudo IP - translated IP address for the flow.
- Pseudo Port - translated port number for the flow.
- Peer IP - remote (WAN) host’s IP address for the flow.
- Peer Port - remote (WAN) host’s port number for the flow.

Maintenance

Use the Maintenance menu to back up the current settings, to restore previously saved settings, or to restore the factory default settings.

Configuration Tools



Configuration Tools

Use the "Backup" tool to save the wireless router's current configuration to a file on your PC.

You can then use the "Restore" tool to restore the saved configuration to the wireless router.

Alternatively, you can use the "Restore to Factory Defaults" tool to force the wireless router to perform a power reset and restore the original factory settings. **WARNING!** All configuration settings will be lost, so also the username and password of your ISP. Please backup your configuration first before your reset the wireless router.

● Backup Wireless Router Configuration

○ Restore from saved Configuration file (SMCWBR14G2_backup.bin)

○ Restore Wireless Router to Factory Defaults

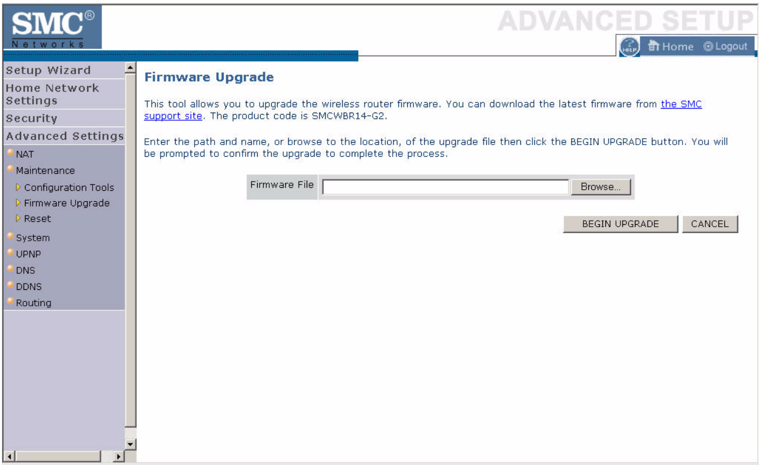
Check **Backup Wireless Router Configuration** and click **NEXT** to save your Barricade’s configuration to a file named config.bin on your PC.

You can then check the **Restore from saved Configuration file (SMCWBR14-G2_backup.bin)** radio button and click **NEXT** to restore the saved backup configuration file.

To restore the factory settings, check **Restore Wireless Router to Factory Defaults** and click **NEXT**. You will be asked to confirm your decision.

Firmware Upgrade

Use this screen to update the firmware to the latest version.



Firmware Upgrade

This tool allows you to upgrade the wireless router firmware. You can download the latest firmware from the SMC support site. The product code is SMCWBR14-G2.

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

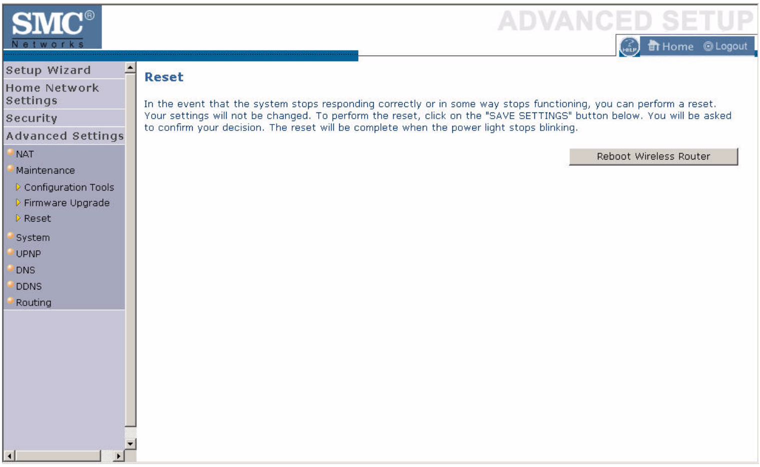
Firmware File [ ] Browse...

BEGIN UPGRADE | CANCEL

Go to www.smc.com to find the latest firmware. Download the firmware to your hard drive first. Click **Browse...** to locate the saved file. After locating the new firmware file, click **BEGIN UPGRADE**. Follow the instructions to complete the upgrade. After restarting, check the Status page to make sure the device is running the new code.

Reset

Perform a reset from this screen.



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 "SAVE SETTINGS" button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking.

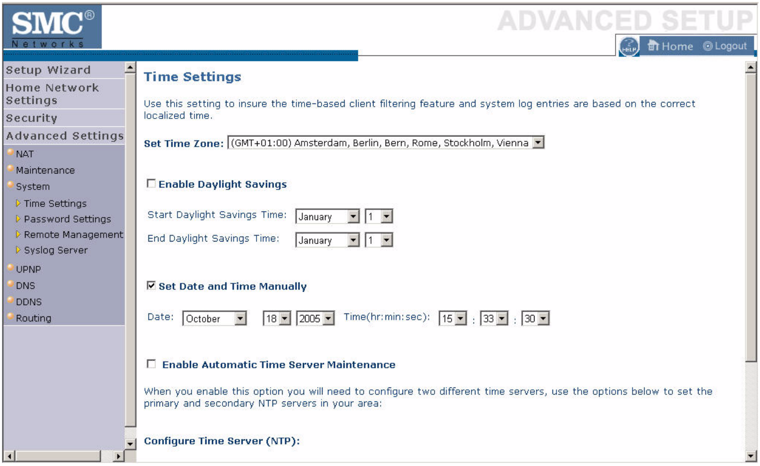
To perform a system reset, click the **Reboot Wireless Router** button in the screen above. The configurations that you have set previously will not be changed back to the factory default settings.

Note: You may also use the blue **Reset** button on the rear panel of the Barricade to perform a reset. Push for one second to perform a reboot. All of your settings will remain upon restarting. Push for six seconds to return the Barricade to factory default settings.

System

This section includes all the basic configuration tools for the Barricade, such as time settings, password settings, and remote management.

Time Settings



Time Settings

Use this setting to insure the time-based client filtering feature and system log entries are based on the correct localized time.

Set Time Zone: (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

□ Enable Daylight Savings

Start Daylight Savings Time: January 1

End Daylight Savings Time: January 1

☑ Set Date and Time Manually

Date: October 18 2005 Time(hr:min:sec): 15 : 33 : 30

□ Enable Automatic Time Server Maintenance

When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:

Configure Time Server (NTP):

Set the time zone and time server for the Barricade. This information is used for log entries and client access control.

- Set Time Zone

  Select your time zone from the drop-down list

- Enable Daylight Savings

  Check **Enable Daylight Savings**, and set the start and end dates if your area requires daylight savings.

- Set Date and Time Manually

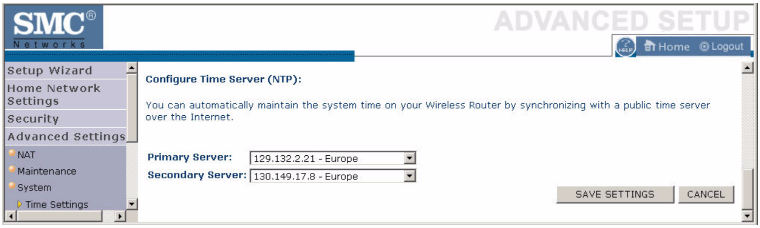
  For manually setting the date and time, configure the date and time by selecting the options from the drop-down list.

- Enable Automatic Time Server Maintenance

  Check **Enable Automatic Time Server Maintenance** to automatically maintain the Barricade's system time by synchronizing with a public time server over the Internet.

- Configure Time Server (NTP):

  Configure two different time servers by selecting the options in the Primary Server and Secondary Server fields.



Configure Time Server (NTP):

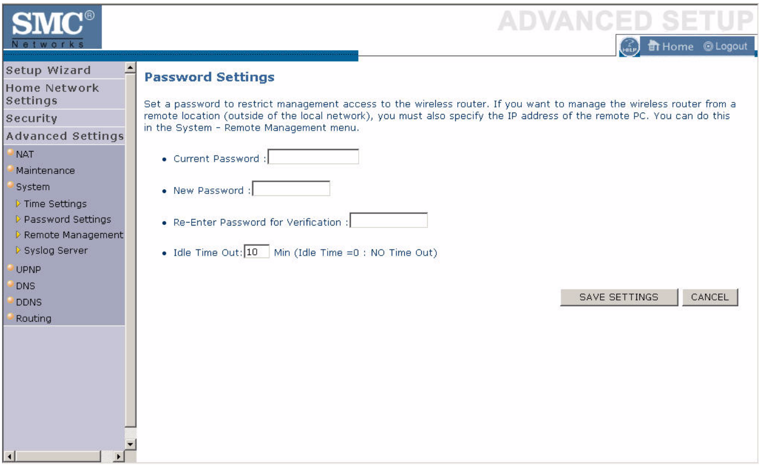
You can automatically maintain the system time on your Wireless Router by synchronizing with a public time server over the Internet.

Primary Server: 129.132.2.21 - Europe

Secondary Server: 130.149.17.8 - Europe

Password Settings

Use this page to restrict access based on a password. For security you should assign one before exposing the Barricade to the Internet.



Password Settings

Set a password to restrict management access to the wireless router. If you want to manage the wireless router from a remote location (outside of the local network), you must also specify the IP address of the remote PC. You can do this in the System - Remote Management menu.

- Current Password :
- New Password :
- Re-Enter Password for Verification :
- Idle Time Out: 10 Min (Idle Time =0 : NO Time Out)

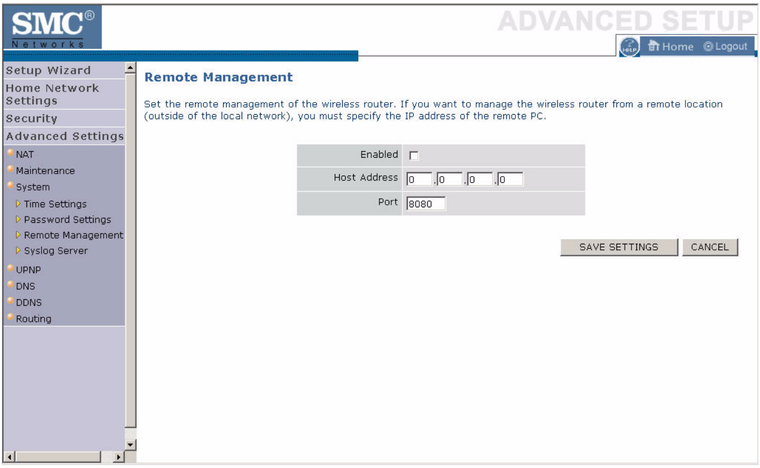
Passwords can contain from 3 to12 alphanumeric characters and are case sensitive.

Note: If your password is lost, or you cannot gain access to the user interface, press the **Reset** button (colored blue) on the rear panel (holding it down for at least six seconds) to restore the factory defaults. The default password is “smcadmin”.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time an inactive login session will be maintained. If the connection is inactive for longer than the maximum idle time, it will be logged out, and you will have to log in to the web management system again. Setting the idle time to 0, will mean the connection never times out.
(Default: 10 minutes)

Remote Management

By default, management access is only available to users on your local network. However, you can also manage the Barricade from a remote host by entering the IP address of a remote computer on this screen. Check the **Enabled** check box, and enter the IP address of the remote host and click **Save Settings**.



Remote Management

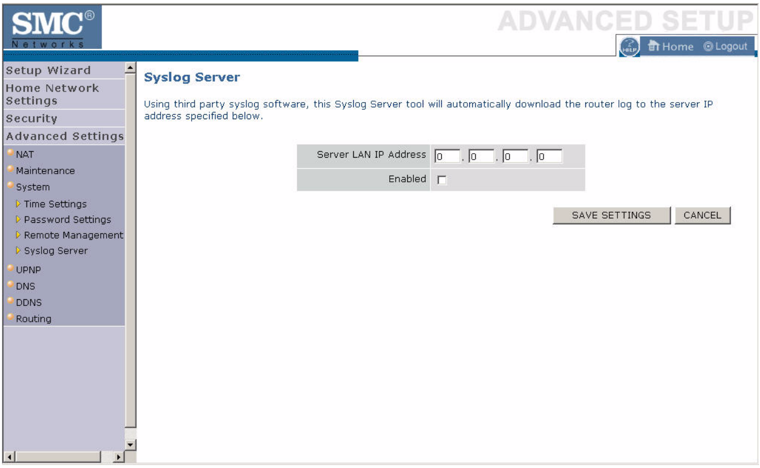
Set the remote management of the wireless router. If you want to manage the wireless router from a remote location (outside of the local network), you must specify the IP address of the remote PC.

Enabled	□
Host Address	0 . 0 . 0 . 0
Port	8080

Note: If you check **Enabled** and specify an IP address of 0.0.0.0, any host can manage the Barricade.

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080 in the address field of your web browser, for example, 212.120.68.20:8080.

Syslog Server



Syslog Server

Using third party syslog software, this Syslog Server tool will automatically download the router log to the server IP address specified below.

Server LAN IP Address 0 . 0 . 0 . 0

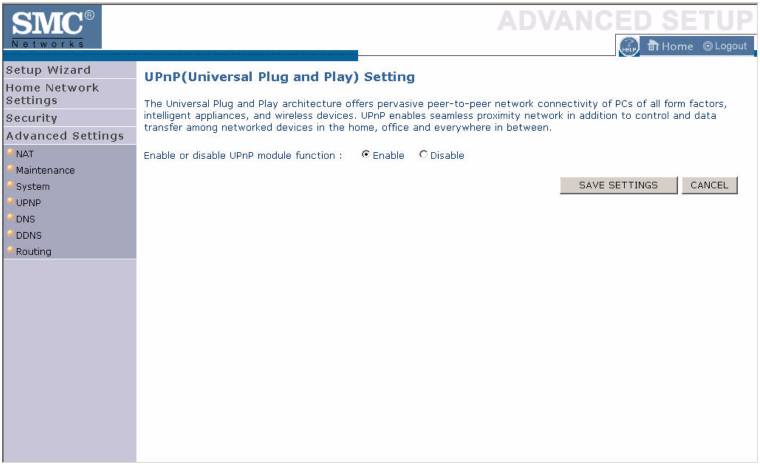
Enabled □

The Syslog Server downloads the Barricade log file to the server with the IP address specified on this screen. Syslog servers offer the possibility to capture the live logs of the router on a PC. There are many shareware syslogs servers available on the web. (Default: Disabled)

UPnP

Universal Plug and Play technology makes home networking simple and affordable. This architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP architecture leverages TCP/IP and the web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.

Click **Enable** to turn on the Universal Plug and Play function of the Barricade. This function allows the device to automatically and dynamically join a network.



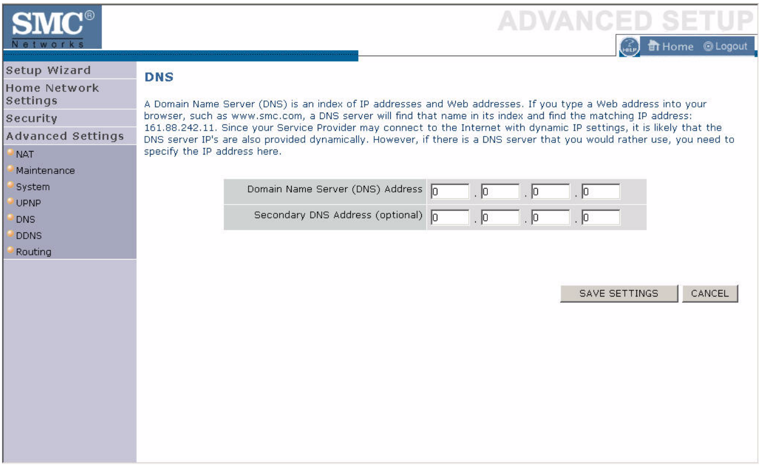
UPnP(Universal Plug and Play) Setting

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.

Enable or disable UPnP module function : ● Enable ○ Disable

Click **Save Settings** to proceed, or **Cancel** to change your settings.

DNS (Domain Name Server)



DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: 161.88.242.11. 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 0 . 0 . 0 . 0

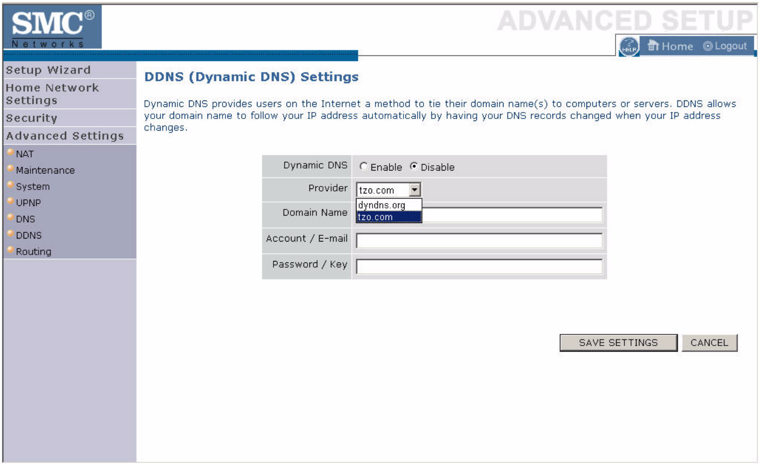
Secondary DNS Address (optional) 0 . 0 . 0 . 0

Domain Name Servers are used to map a domain name (e.g., www.somesite.com) to the equivalent numerical IP address (e.g., 64.147.25.20). Your ISP should provide the IP address of one or more Domain Name Servers. Enter those addresses on this page.

DDNS (Dynamic DNS)

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

The DDNS service dynamically updates DNS information to a static hostname, provided by the DDNS service provider, as clients' IP addresses change.



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.

Dynamic DNS	○ Enable ● Disable
Provider	tzo.com dyndns.org tzo.com
Domain Name	
Account / E-mail	
Password / Key	

Note: Please visit the web sites of the DDNS providers for details.

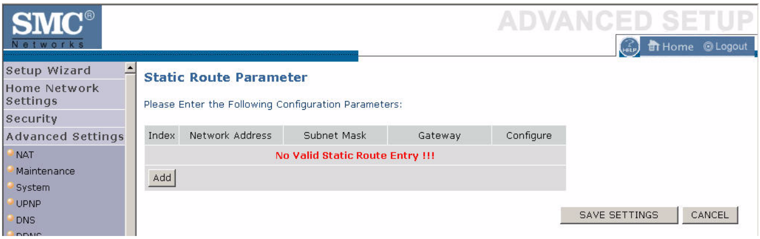
DDNS Service Provider	Web Site
DynDNS.org	http://www.dyndns.org
TZO.com	http://www.tzo.com

For using DDNS, click on the enable radio button, select the DDNS Service type, and then enter the Domain Name, Account/E-mail address, and Password/Key.

Routing

This section defines routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

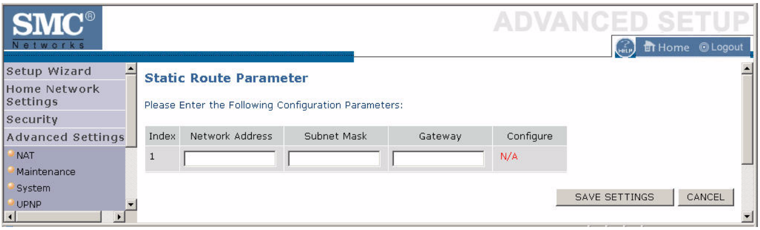
Static Route



Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
No Valid Static Route Entry !!!				



Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
1				N/A

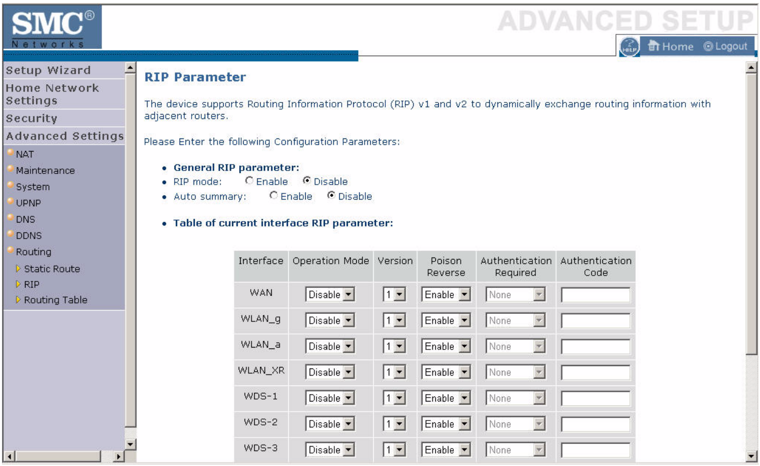
Click **Add** to add a new static route to the list.

Parameter	Description
Index	Index number of the route.
Network Address	Enter the IP address of the remote computer for which to set a static route.
Subnet Mask	Enter the subnet mask of the remote network for which to set a static route.
Gateway	Enter the WAN IP address of the gateway to the remote network.
Configure	Allows you to edit existing routes.

Click **Save Settings** to save the configuration.

RIP

RIP sends routing-update messages at regular intervals and when the network topology changes.



RIP Parameter

The device supports Routing Information Protocol (RIP) v1 and v2 to dynamically exchange routing information with adjacent routers.

Please Enter the following Configuration Parameters:

- **General RIP parameter:**
- RIP mode: ○ Enable ● Disable
- Auto summary: ○ Enable ● Disable

- **Table of current interface RIP parameter:**

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
WAN	Disable	1	Enable	None	
WLAN_g	Disable	1	Enable	None	
WLAN_a	Disable	1	Enable	None	
WLAN_XR	Disable	1	Enable	None	
WDS-1	Disable	1	Enable	None	
WDS-2	Disable	1	Enable	None	
WDS-3	Disable	1	Enable	None	

Parameter	Description
General RIP Parameters	
RIP mode	Globally enables or disables RIP.
Auto summary	If Auto summary is disabled, then RIP packets will include sub-network information from all subnetworks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all subnetworks.
Table of current Interface RIP parameter	
Interface	The WAN interface to be configured.
Operation Mode	Disable: RIP disabled on this interface. Enable: RIP enabled on this interface. Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.