

**ADSL Router with 4-Port LAN  
Switch and 802.11g WLAN  
3100-4g V2**

3100-4g V2  
April 2008  
R.01 f/w 0.72

# COMPLIANCES

## **EC Conformance Declaration**

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN 300 328

EN 301 489-1

EN 301 489-17

EN 60950-1

## **Industry Canada Statement**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- (1). this device may not cause interference and
- (2). this device must accept any interference, including interference that may cause undesired operation of the device

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la class A est conforme a la norme NMB-003 du Canada.

### **IMPORTANT NOTE:**

#### **IC Radiation Exposure Statement:**

This equipment complies with Canada radiation exposure limits set forth for uncontrolled environments. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2.4GHz operation of this product in Canada is firmware-limited to channels 1 through 11.

## **Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:

### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2.4GHz operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

## COMPLIANCES

### **FCC Part 68 statement**

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: ACYDL02BAR4505NWB. If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: ACYDL02BAR4505NWB. The digits represented by 02 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, Please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this [equipment ID] does not disable your alarm equipment.

If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

*COMPLIANCES*

**Contact information in the USA**

COMPANY: Alpha Telecom Inc. USA

ADDRESS: 1362 Borregas Avenue, Sunnyvale, CA 94089

TEL NO: 1-408-541-6186

Contact person: Judy Lee

# TABLE OF CONTENTS

<b>1</b>	<b>Introduction</b>	<b>1-1</b>
	About the ADSL router	1-1
	Features and Benefits	1-1
	Applications	1-2
<b>2</b>	<b>Installation</b>	<b>2-1</b>
	Package Contents	2-1
	System Requirements	2-2
	Hardware Description	2-2
	LED Indicators	2-3
	Rear Ports	2-4
	ISP Settings	2-5
	Connect the System	2-5
	Connecting the ADSL Line	2-6
	Connecting the network	2-6
	Connecting the Power Adapter	2-6
	Wall Mounting	2-7
<b>3</b>	<b>Configuring Client PC</b>	<b>3-1</b>
	TCP/IP Configuration	3-2
	Windows 2000	3-3
	Disable HTTP Proxy	3-4
	Obtain IP Settings from Your ADSL router	3-4
	Windows XP	3-6
	Disable HTTP Proxy	3-6
	Obtain IP Settings from Your ADSL router	3-6
	Configuring Your Macintosh Computer	3-8
	Disable HTTP Proxy	3-9

<b>4</b>	<b>Configuring the ADSL Router</b>	<b>4-1</b>
	Navigating the Management Interface	4-2
	Making Configuration Changes	4-3
	Set-up Wizard	4-4
	Selecting a Password	4-5
	Selecting a Time Zone	4-6
	Setting up Wireless Security	4-7
	Wizard_Setup Complete	4-10
	Advanced setup	4-11
	System	4-13
	WAN	4-17
	LAN	4-21
	Wireless	4-25
	NAT	4-32
	Routing	4-37
	Firewall	4-41
	UPnP	4-54
	QoS	4-55
	DDNS	4-58
	Tools	4-59
	Status	4-62
	Diagnostics	4-65
	Finding the MAC address of a Network Card	4-66
	Windows 2000/XP	4-66
	Macintosh	4-66
	Linux	4-66
<b>A</b>	<b>Troubleshooting</b>	<b>A-1</b>
<b>B</b>	<b>Cables</b>	<b>B-1</b>
	Ethernet Cable	B-1
	Specifications	B-1
	Wiring Conventions	B-1
	RJ-45 Port Connection	B-2
	Pin Assignments	B-3
<b>C</b>	<b>Specifications</b>	<b>C-1</b>

# CHAPTER 1

## INTRODUCTION

---

Congratulations on your purchase of the ADSL router. We are proud to provide you with a powerful yet simple communication device for connecting your local area network (LAN) to the Internet. For those who want to surf the Internet in the most secure way, the ADSL router provides a convenient and powerful solution.

### **About the ADSL router**

The ADSL router provides Internet access to multiple users by sharing a single-user account. Support is provided for both wired and wireless devices. New technology provides wireless security via Wired Equivalent Privacy (WEP) encryption and MAC address filtering. It is simple to configure and can be up and running in minutes.

### **Features and Benefits**

- Built-in ADSL2/2+ modem - supports download speeds up to 24Mbps
- Local network connection via four 10/100 Mbps Ethernet ports
- Built-in IEEE802.11g 54Mbps Wireless Access Point (AP)
- DHCP for dynamic IP configuration, and DNS for domain name mapping

- Firewall with Stateful Packet Inspection, client privileges, intrusion detection, and NAT
- NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as web, FTP, e-mail, and Telnet)
- VLAN and QoS (Quality of Service) support
- User-definable application sensing tunnel supports applications requiring multiple connections
- Easy setup through a web browser on any operating system that supports TCP/IP

## **Applications**

Many advanced networking features are provided by the ADSL router:

- **Wireless and Wired LAN**

The ADSL router provides connectivity to 10/100 Mbps devices, and wireless IEEE 802.11g compatible devices, making it easy to create a network in small offices or homes.

- **Internet Access**

This device supports Internet access through an ADSL connection. Since many DSL providers use PPPoE or PPPoA to establish communications with end users, the ADSL router includes built-in clients for these protocols, eliminating the need to install these services on your computer.

- **Shared IP Address**

The ADSL router provides Internet access for up to 253 users via a single shared IP address. Using only one ISP account, multiple users on your network can browse the web at the same time.

- **Virtual Server**

If you have a fixed IP address, you can set the ADSL router to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the ADSL router can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- **DMZ Host Support**

Allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

- **Security**

The ADSL router supports security features that deny Internet access to specified users, or filter all requests for specific services that the administrator does not want to serve. The firewall also blocks 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. WEP (Wired Equivalent Privacy), SSID Broadcast disable, and MAC filtering provide security over the wireless network.

# CHAPTER 2

## INSTALLATION

---

Before installing the ADSL router, verify that you have all the items listed under the Package Contents list. Also be sure that you have all the necessary cabling before installing the ADSL router. After installing the ADSL router, refer to “Configuring the ADSL Router” on page 4-1.

### **Package Contents**

After unpacking the ADSL router, check the contents of the box to be sure you have received the following items:

- ADSL router
- Power adapter
- One RJ-45 Cat-5 Ethernet cable
- Documentation CD

Immediately inform your dealer in the event of any incorrect, missing, or damaged parts. If possible, please retain the carton and original packing materials in case there is a need to return the product.

## **System Requirements**

You must meet the following minimum requirements:

- ADSL Internet Service installed.
- 2.4GHz Wireless adapter or Ethernet Adapter installed on each PC.
- TCP/IP network protocols installed on each PC that will access the Internet.
- A Java enabled web browser such as Internet Explorer 5.5 or above, Netscape 4.7 or above, Mozilla 1.7 or above and Firefox 1.0 or above.

## **Hardware Description**

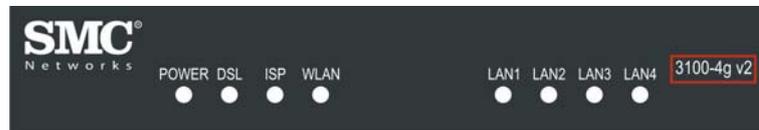
The ADSL router contains an integrated ADSL modem and connects to the Internet or to a remote site using its RJ-45 WAN port. It can be connected directly to your PC or to a local area network using any of the four Fast Ethernet LAN ports.

Access speed to the Internet depends on your service type. Full-rate ADSL provides up to 8 Mbps downstream and 1 Mbps upstream. G.lite (or splitterless) ADSL provides up to 1.5 Mbps downstream and 512 kbps upstream. ADSL2+ provides up to 24Mbps downstream and 1Mbps upstream. However, you should note that the actual rate provided by specific service providers may vary dramatically from these upper limits.

Data passing between devices connected to your local area network can run at up to 100 Mbps over the Fast Ethernet ports and 54 Mbps over the built-in wireless access point.

## LED Indicators

The ADSL router includes an LED display on the top for system power and port indications that simplifies installation and network troubleshooting.

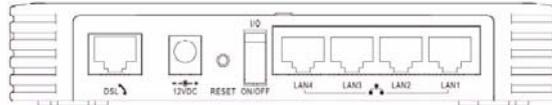


**Figure 2-1. Led indicators**

LED	Status	Description
Power	On	The ADSL router is receiving power. Normal operation.
	Off	Power off or failure.
DSL	On	ADSL connection is functioning correctly.
	Flashing	The ADSL router is establishing an ADSL link.
	Off	ADSL connection is not established.
ISP	On	WAN port connected.
	Off	No WAN port connection.
WLAN	Flashing	The WLAN port is sending or receiving data.
LAN1 to LAN4	On	Ethernet connection is established.
	Flashing	The indicated LAN port is sending or receiving data.
	Off	There is no LAN connection on the port.

## Rear Ports

The ADSL router also provides the following ports on the rear panel:



**Figure 2-2. Rear Panel**

Item	Description
DSL Port	WAN port (RJ-11). Connect your ADSL line to this port.
Power Inlet	Connect the included power adapter to this inlet. <b>Warning:</b> Using the wrong type of power adapter may damage the router.
Reset Button	Use this button to reset the power and restore the default factory settings. To reset without losing configuration settings, see “Reset” on page 4-61.
On/Off switch	Use this switch to turn the router ON and OFF.
LAN Ports	4 Fast Ethernet ports (RJ-45). Connect devices on your local area network to these ports (i.e., a PC, hub, or switch).

## **ISP Settings**

Please collect the following information from your ISP before setting up the ADSL router:

- ISP account user name and password
- Protocol, encapsulation and VPI/VCI circuit numbers
- DNS server address
- IP address, subnet mask and default gateway (for fixed IP users only)

## **Connect the System**

The ADSL router can be positioned at any convenient location in your office or home. No special wiring or cooling requirements are needed. You should, however, comply with the following guidelines:

- Keep the ADSL router away from any heating devices.
- Do not place the ADSL router in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the ADSL router.

### **Connecting the ADSL Line**

Connect the splitter to the phone line and the phone to the phone port of the splitter. Using the black RJ-11 cable provided connect the ADSL port of the ADSL router to the ADSL port of the splitter.

The splitter is required for connecting your ADSL router and phone to the same phone line. If you have a dedicated phone line for ADSL connect the ADSL router directly to the phone line.

**Note:** To prevent high frequency ADSL signals interfering with telephone calls, each phone must be connected to the same phone line through a splitter (also known as an ADSL microfilter).

### **Connecting the network**

Using the grey RJ-45 cable provided connect LAN port of the ADSL router to the network card of your computer or other network device, e.g., hub or switch. The corresponding LAN LED will illuminate green to indicate good link.

### **Connecting the Power Adapter**

Plug the power adapter into the power socket on the rear of the ADSL router, and the other end into a power outlet. Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to “Troubleshooting” on page A-1.

In case of a power input failure, the ADSL router will automatically restart and begin to operate once the input power is restored.

## **Wall Mounting**

There are 2 slots on the underside of the ADSL router that can be used for wall mounting. The distance between the 2 slots is 120 mm.

You will need 2 suitable screws, the diameter would be 5.0 mm to 7.0 mm, to wall mount the ADSL router.

When wall mounting the unit, ensure that it is within reach of the power outlet.

To wall mount the unit:

1. Ensure that the wall you use is smooth, flat, dry and sturdy and use the 2 screws holes which both are 120 mm apart.
2. Fix the screws into wall, leaving their heads 5 mm clear of the wall surface.
3. Remove any connections to the unit and locate it over the screw heads. When in line, gently push the unit on to the wall and move it downwards to secure.

# CHAPTER 3

## CONFIGURING CLIENT PC

---

After completing hardware setup by connecting all your network devices, you need to configure your computer to connect to the ADSL router.

See:

“Windows 2000” on page 3-3

“Windows XP” on page 3-6

or

“Configuring Your Macintosh Computer” on page 3-8

depending on your operating system.

## TCP/IP Configuration

To access the Internet through the ADSL router, you must configure the network settings of the computers on your LAN to use the same IP subnet as the ADSL router. The default IP settings for the ADSL router are:

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

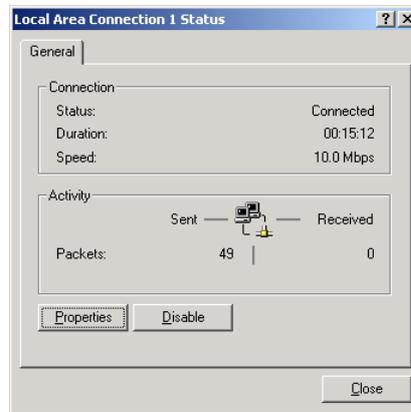
**Note:** These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the ADSL router's web configuration interface in order to make the required changes. (See "Configuring the ADSL Router" on page 4-1 for instruction on configuring the ADSL router.)

## Windows 2000

1. On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.

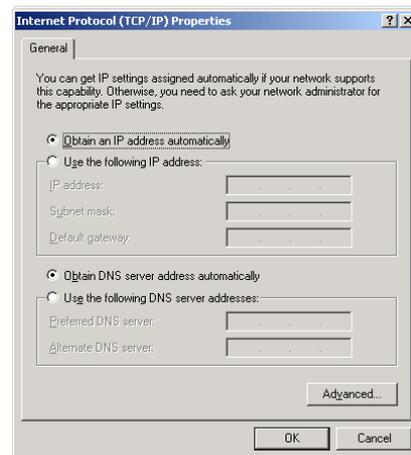
2. Click the icon that corresponds to the connection to your ADSL router.

3. The connection status screen will open. Click Properties.



4. Double-click Internet Protocol (TCP/IP).

5. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.



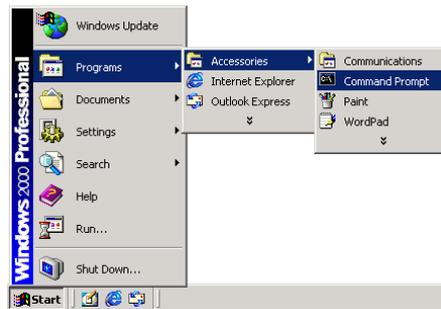
## Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the ADSL router’s HTML configuration pages.

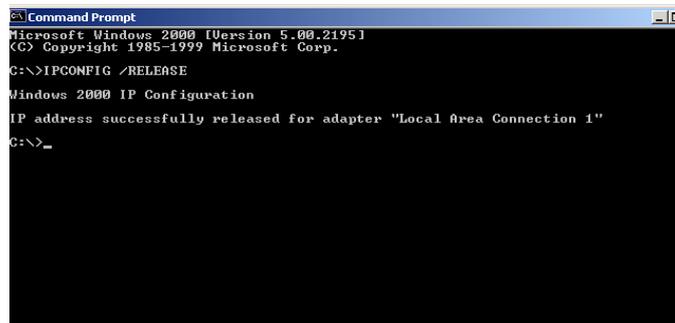
## Obtain IP Settings from Your ADSL router

Now that you have configured your computer to connect to your ADSL router, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL router, you can verify that you have configured your computer correctly.

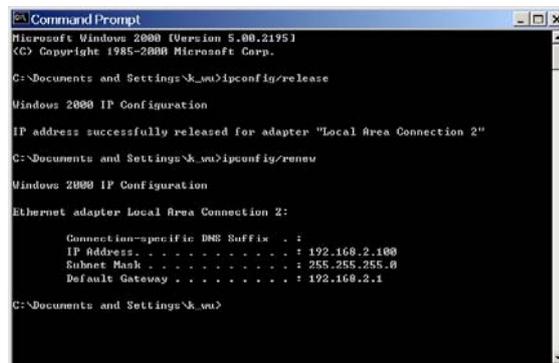
1. On the Windows desktop, click Start/Programs/Accessories/Command Prompt.



2. In the Command Prompt window, type “IPCONFIG/RELEASE” and press the ENTER key.



3. Type "IPCONFIG /RENEW" and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL Router is functioning.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\k_wa>ipconfig/release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection 2"

C:\Documents and Settings\k_wa>ipconfig/renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.2.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.1

C:\Documents and Settings\k_wa>
```

4. Close the Command Prompt window.

Your computer is now configured to connect to the ADSL router.

## Windows XP

1. On the Windows desktop, click Start/Control Panel.
2. In the Control Panel window, click Network and Internet Connections.
3. The Network Connections window will open. Double-click the connection for this device.
4. On the connection status screen, click Properties.
5. Double-click Internet Protocol (TCP/IP).
6. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select this option.

### Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the ADSL router’s HTML configuration pages.

### Obtain IP Settings from Your ADSL router

Now that you have configured your computer to connect to your ADSL router, it needs to obtain new network settings. By releasing old DHCP IP settings and renewing them with settings from your ADSL router, you can verify that you have configured your computer correctly.

1. On the Windows desktop, click Start/Programs/Accessories/Command Prompt.
2. In the Command Prompt window, type “IPCONFIG/RELEASE” and press the ENTER key.

*WINDOWS XP*

3. Type "IPCONFIG /RENEW" and press the ENTER key. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL router is functioning.
4. Close the Command Prompt window.

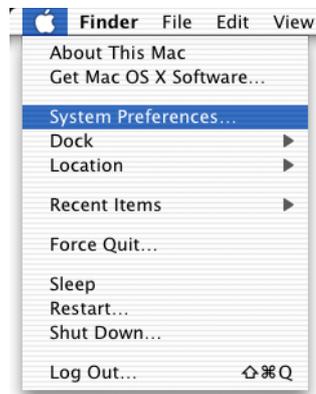
Your computer is now configured to connect to the ADSL router.

## Configuring Your Macintosh Computer

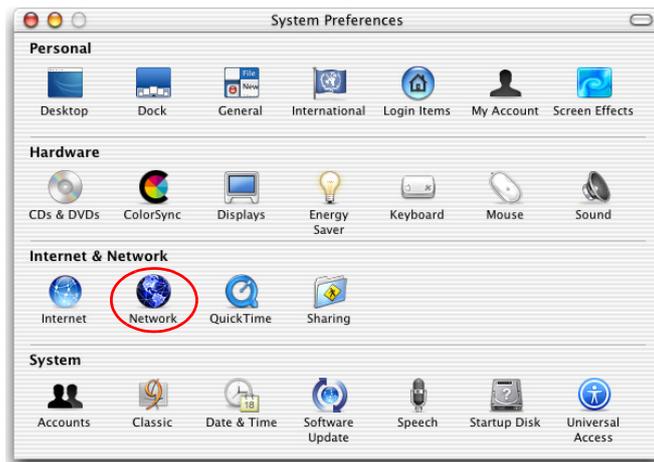
You may find that the instructions here do not exactly match your operating system. This is because these steps and screenshots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to Mac OS 10.2.

Follow these instructions:

1. Pull down the Apple Menu . Click System Preferences



2. Double-click the Network icon in the Systems Preferences window.



## CONFIGURING YOUR MACINTOSH COMPUTER

3. If “Using DHCP Server” is already selected in the Configure field, your computer is already configured for DHCP. If not, select this Option.



4. Your new settings are shown on the TCP/IP tab. Verify that your IP Address is now **192.168.2.xxx**, your Subnet Mask is **255.255.255.0** and your Default Gateway is **192.168.2.1**. These values confirm that your ADSL router is functioning.
5. Close the Network window.

Now your computer is configured to connect to the ADSL router.

### Disable HTTP Proxy

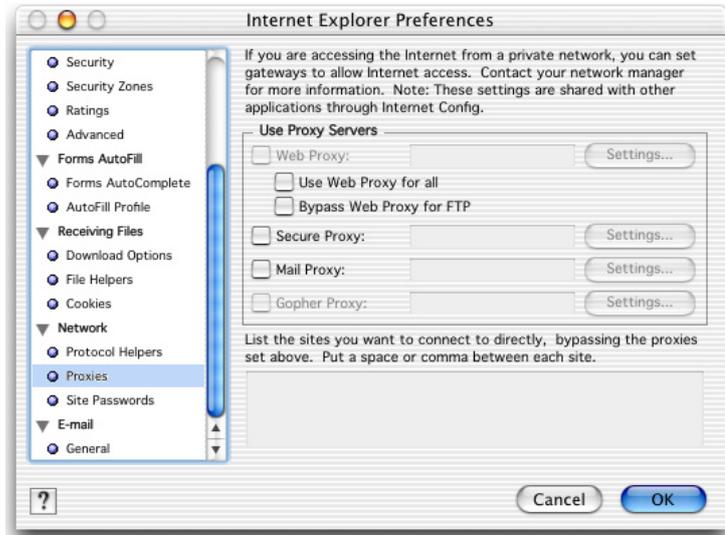
You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the ADSL router’s HTML configuration pages. The following steps are for Internet Explorer.

#### Internet Explorer

1. Open Internet Explorer and click the Stop button. Click Explorer/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.



3. Uncheck all check boxes and click OK.



# CHAPTER 4

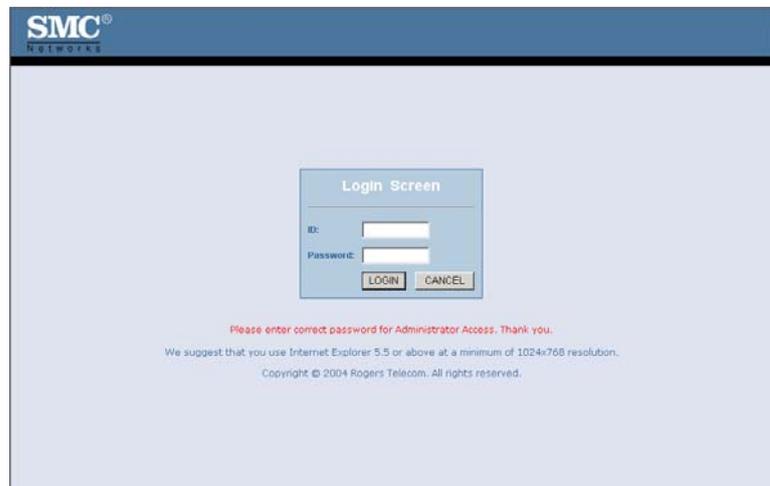
## CONFIGURING THE ADSL ROUTER

---

After you have configured TCP/IP on a client computer, you can configure the ADSL router using your web browser. Internet Explorer 5.5 or above, Netscape Navigator, Mozilla, Firefox and Opera are supported.

To access the management interface, enter the default IP address of the ADSL router in your web browser: <http://192.168.2.1>. Enter the default login ID: “administrator”, leave the password blank, and click **LOGIN**.

**Note:** Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

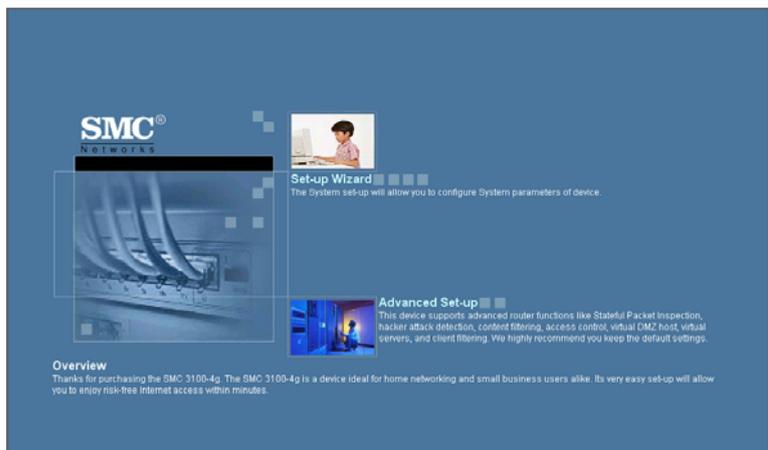


## Navigating the Management Interface

On initial configuration the first screen is Country Selection. Select your country from the drop-down list. This configures the correct channels for the wireless AP. The Country Selection screen only appears on initial configuration or when the ADSL router is reset to factory defaults.



Two items are available on the following screen: Set-up Wizard, and Advanced Set-up.



## NAVIGATING THE MANAGEMENT INTERFACE

Use the Setup Wizard for quick and easy configuration of your Internet connection and basic wireless settings. Go to “Set-up Wizard” on page 4-4 for details.

For Advanced set-up, refer to section “Advanced setup” on page 4-11.

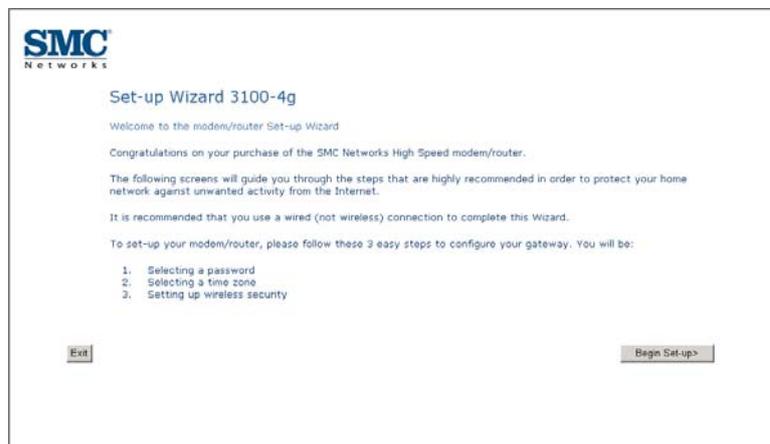
### **Making Configuration Changes**

Configurable parameters have a dialog box or a drop-down menu. Once a configuration change has been made on a screen, click the **APPLY**, **SAVE SETTINGS** or **NEXT** button on the screen to enable the new setting.

**Note:** To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.5 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”

## Set-up Wizard

The set-up wizard is designed to help you to quickly and easily configure your ADSL router. Follow the instruction on the screen, and click Begin set-up.



## Selecting a Password

By default, the ADSL router comes with no password. For security reasons, you should set up a new password.

SMC Networks

Select Password    Select Time Zone    Wireless Setup    Setup Completed

### 1. Selecting a Password

By default, your new modem/router is not password protected. That means an unauthorized person can access the modem/router and modify its configuration. To protect it, you should set up a new password.

**PLEASE REMEMBER AND WRITE DOWN THIS NEW PASSWORD.** You will need it in the future.

**Please enter a new password below:**

User name: administrator

Current Password:

(If you are setting up your password for the first time, please leave the "Current Password" field blank.)

New Password:

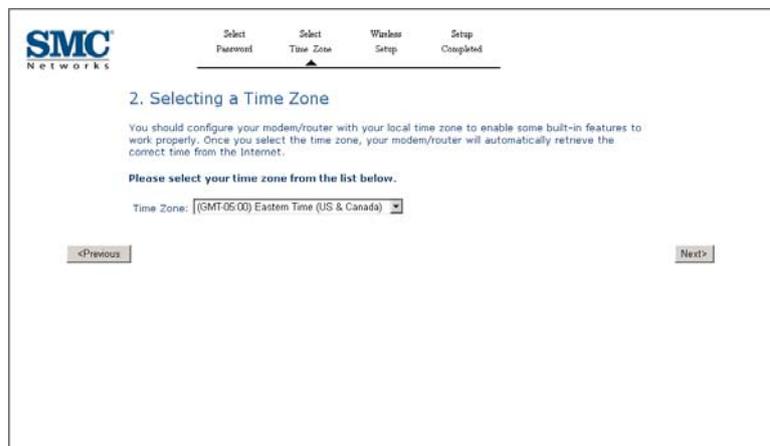
Re-enter new password:

<Previous    Next>

- The user name is “administrator” by default.
- Current password: by default, there is no password.
- New password: enter the new password in this field.
- Enter the new password again in the re-enter the password field.

## Selecting a Time Zone

To keep the time on the router correct, select your local time zone from the drop-down menu. This information is used for log entries and client filtering.



The screenshot shows the SMC Networks configuration interface. At the top, there is a navigation bar with four tabs: "Select Password", "Select Time Zone", "Wireless Setup", and "Setup Completed". The "Select Time Zone" tab is currently selected. Below the navigation bar, the page title is "2. Selecting a Time Zone". The main content area contains the following text: "You should configure your modem/router with your local time zone to enable some built-in features to work properly. Once you select the time zone, your modem/router will automatically retrieve the correct time from the Internet." Below this, it says "Please select your time zone from the list below." and "Time Zone: [(GMT-05:00) Eastern Time (US & Canada)]". At the bottom of the page, there are two buttons: "<Previous" and "Next>".

Click **NEXT** to continue.

## Setting up Wireless Security

This screen allows you to configure the wireless security. The ADSL router supports WEP and WPA.

The screenshot shows the SMC Networks Setup Wizard interface. At the top, there is a progress bar with four steps: 'Select Password', 'Select Time Zone', 'Wireless Setup', and 'Setup Completed'. The 'Wireless Setup' step is currently active and highlighted with an upward-pointing arrow. Below the progress bar, the title '3. Setting up Wireless Security' is displayed. A paragraph of text explains that wireless access is enabled by default but not secure, and recommends applying WEP security. Below this, there is a section titled 'Please select your wireless configuration:' with two radio button options: 'Disable wireless configuration' and 'Enable wireless configuration'. The 'Enable wireless configuration' option is selected. To the right of this section is a 'More Info' button. Below the radio buttons is a dropdown menu labeled 'Please select a security setting:' with 'None' selected. At the bottom of the screen, there are '<Previous' and 'Next>' navigation buttons.

- Select Disable/Enable wireless configuration, if you disable wireless configuration, there is no need to setup the security function. If you select Enable wireless configuration, then select the security settings from the drop-down menu.

For WEP security function, go to next page.

For WPA security function, go to page 4-9.

Click **NEXT** to continue.

*WEP\_Security*

Choosing WEP as the wireless security for your wireless network.

The screenshot shows the SMC Networks configuration interface. At the top, there is a progress bar with four steps: 'Select Password', 'Select Time Zone', 'Wireless Setup', and 'Setup Completed'. The 'Wireless Setup' step is currently active. Below the progress bar, the title is '4. Setting up Wireless Security(Con't)'. The main text explains that to enable WEP security, a secret key must be entered into the modem/router and all wireless clients. It suggests using a pass-phrase tool to generate this key. An important note states that the secret key must be written down for use in wireless clients. A warning indicates that the connection will drop when wireless security is enabled if the wireless client is updated, recommending a wired connection for the setup. Below this text, there is a section titled 'Please enter a pass-phrase:' with two input fields: 'Pass phrase:' and 'Key:'. The 'Key:' field contains the hexadecimal value '01010101'. A 'Generate Key' button is located to the right of the 'Pass phrase:' field. At the bottom of the page, there are '<Previous' and 'Next>' navigation buttons. The footer contains the copyright notice: 'Copyright © SMC Networks Inc. 2002. All rights reserved.'

Enter a string in the passphrase field, then click **Generate Key**.

Click **Next** to continue. The Set-up complete screen will then appear.

*WPA\_Security*

Choosing WPA as the security mechanism for your wireless network.

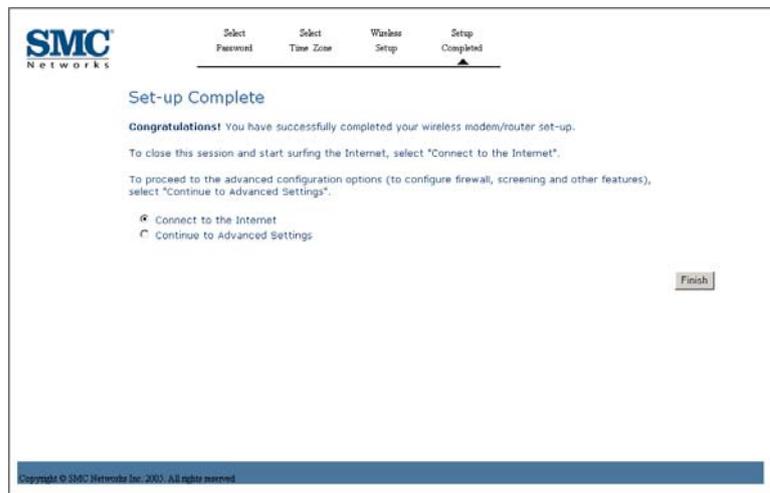
The screenshot shows the SMC Networks Setup Wizard interface. At the top, there is a progress bar with four steps: 'Select Password', 'Select Time Zone', 'Wireless Setup', and 'Setup Completed'. The 'Wireless Setup' step is currently active. Below the progress bar, the title is '4. Setting up Wireless Security(Con't)'. The main text explains that to enable WPA security, a secret key must be entered into the modem/router and all wireless clients. It provides instructions on how to generate a key using a pass-phrase tool. Below this, there are two radio button options: 'Pass phrase:' and 'Key:'. Each option has a corresponding text input field. At the bottom of the form, there are '<Previous' and 'Next>' buttons. A copyright notice for SMC Networks Inc. 2003 is visible at the very bottom.

you can select to use the passphrase function or encryption key as the security method, then enter the string in the corresponding field.

Click **Next** to complete this setup.

## Wizard\_Setup Complete

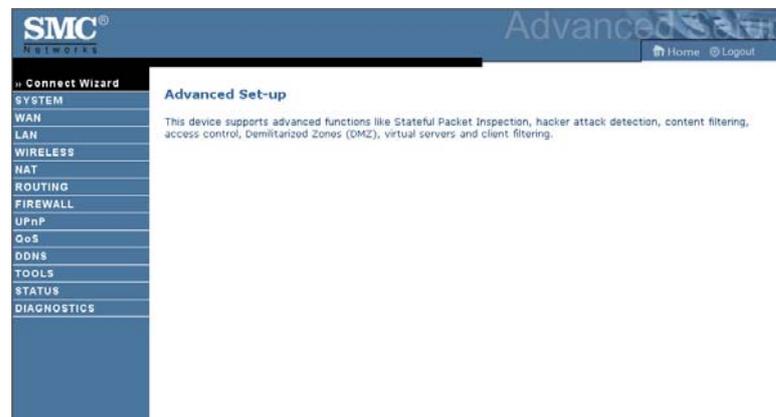
This screen shows that you have configured your ADSL router using the Setup Wizard.



- Connect to the Internet: select this option, and then click **Finish** to connect to the internet.
- Continue to Advanced Settings: select this option, and then click **Finish** to continue with more configurations for the ADSL router.

## Advanced setup

The left-hand side displays the main menu and the right-hand side shows descriptive information. There are 13 main menu items as described in the following table.



Menu	Description
System	Sets the local time zone, the password for administrator access, and the IP address of a PC that will be allowed to manage the ADSL router remotely.
WAN	Specifies the Internet connection settings.
LAN	Sets the TCP/IP configuration for the ADSL router LAN interface and DHCP clients.
Wireless	Configures the radio frequency, SSID, and security for wireless communications.
NAT	Configures Address Mapping, virtual server and special applications.
Routing	Sets the routing parameters and displays the current routing table.
Firewall	Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, intruder detection, and DMZ.
UPnP	Enables the Universal Plug and Play function.

## CONFIGURING THE ADSL ROUTER

<b>Menu</b>	<b>Description</b>
QoS	Allows you to prioritize your network traffic.
DDNS	Configures Dynamic DNS function.
Tools	Contains options to ping network connection, trace route, backup & restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system.
Status	Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information. Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number. Shows the security and DHCP client log.
Diagnostics	This function is used to diagnose the connection.

## System

### Time Settings

Select your local time zone from the drop-down menu. This information is used for log entries and client filtering.

**SMC®** Advanced Setup  
Home Logout

**Connect Wizard**

**SYSTEM**

- Time Settings
- Password Settings
- Remote Management
- DNS

**WAN**

**LAN**

**WIRELESS**

**NAT**

**ROUTING**

**FIREWALL**

**UPnP**

**QoS**

**DDNS**

**TOOLS**

**STATUS**

**DIAGNOSTICS**

**Time Settings**

Current Time: 08/01/2003 04:18:52 am

**Set Time Zone:**

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

(GMT-05:00)Eastern Time (US & Canada)

**Configure Time Server (NTP):**

You can automatically maintain the system time on this device by synchronizing with a public time server over the Internet. 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:

Enable Automatic Time Server Maintenance

Primary Server: 132.163.4.102 - North America

Secondary Server: 192.5.41.41 - North America

HELP SAVE SETTINGS CANCEL

If you want to automatically synchronize the ADSL router with a public time server, check the **Enable Automatic Time Server Maintenance** check box. Then select the desired servers from the drop-down menus.

## Password Settings

Use this screen to change the password for accessing the management interface.

The screenshot shows the 'Password Settings' page in the SMC Networks Advanced Management System. The page has a blue header with the SMC logo and 'Advanced' text. A navigation menu on the left lists various system settings. The main content area is titled 'Password Settings' and contains the following elements:

- Instruction: "Set a password to restrict management access to this device."
- Form fields:
  - Current Password: [ ]
  - New Password: [ ]
  - Re-Enter Password for Verification: [ ]
- Idle Time Out: 10 Min (Idle Time =0: NO Time Out)
- Buttons: HELP, SAVE SETTINGS, CANCEL

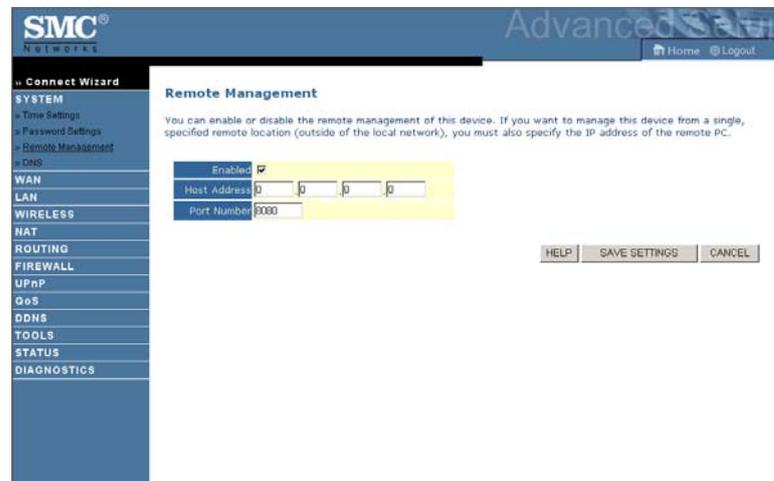
Passwords can contain from 3~12 alphanumeric characters and are case sensitive.

**Note:** If you lost the password, or you cannot gain access to the user interface, press the blue reset button on the rear panel, holding it down for at least five seconds to restore the factory defaults. By default, there is no password.

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time for which the login session is maintained during inactivity. If the connection is inactive for longer than the maximum idle time, it will perform system logout, and you have to log in again to access the management interface. (Default: 10 minutes)

### Remote Management

By default, management access is only available to users on your local network. However, you can also manage the ADSL router 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**.



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

For remote management via WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by:8080, for example, 211.20.16.1:8080.



## CONFIGURING THE ADSL ROUTER

### DNS

A Domain Name Server (DNS) is an index of IP addresses and web addresses. Most ISPs provide a DNS server as part of the Internet access service. However, if there is a DNS server that you would rather use, you will need to specify the IP address here.

The screenshot shows the SMC Advanced Router's web interface. The top navigation bar includes the SMC logo, the word "Advanced", and links for "Home" and "Logout". A left-hand menu lists various configuration categories: "Connect Wizard", "SYSTEM" (with sub-items: Time Settings, Password Settings, Remote Management, DNS), "WAN", "LAN", "WIRELESS", "NAT", "ROUTING", "FIREWALL", "UPnP", "QoS", "DDNS", "TOOLS", "STATUS", and "DIAGNOSTICS". The "DNS" page is active, displaying a title "DNS" and a descriptive paragraph: "A Domain Name Server (DNS) is an index of IP addresses and Web addresses. Most ISPs provide a DNS server as part of the Internet Access service. However, if there is a DNS server that you would rather use, you will need to specify the IP address here." Below this text are two input fields: "Domain Name Server (DNS) Address" and "Secondary DNS Address (optional)", each with four individual input boxes for IP address octets. At the bottom right of the form area are three buttons: "HELP", "SAVE SETTINGS", and "CANCEL".

## WAN

Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

The screenshot shows the SMC Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, UPnP, QoS, DDNS, TOOLS, STATUS, and DIAGNOSTICS. The 'WAN' section is expanded, showing sub-options like 'Cloned MAC Address'. The main content area is titled 'ATM Interface' and contains a configuration table for interface 'ATM1'.

ATM1	
Protocol	PPPoE
VPI/VCI	1483 Bridging
Encapsulation	LLC
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Always Connected
Idle Time (Minute)	20
Username	
Password	
Confirm Password	
MTU	1492

At the bottom right of the configuration area are three buttons: HELP, SAVE SETTINGS, and CANCEL.

The following protocols are supported:

- 1483 Bridging
- PPPoE

## ATM Interface

### 1483 Bridging

Enter the Bridging settings provided by your ISP.

ATM1	
Protocol	1483 Bridging
VLAN	Default
VPI/VCI	3 / 35
Encapsulation	LLC

Parameter	Description
VLAN	Select VLAN group from the drop-down menu. New VLAN groups can be created from the LAN menu.
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.

PPPoE

Enter the PPPoE settings provided by your ISP.

ATM1	
Protocol	PPPoE
VPI/VCI	8 / 35
Encapsulation	LLC
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Always Connected
Idle Time (Minute)	20
Username	
Password	
Confirm Password	
MTU	1492

Parameter	Description
VPI/VCI	Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP.
Encapsulation	Select the encapsulation used by ISP from the drop-down menu.
IP assigned by ISP	Select Yes if you have a dynamic IP address. Select No if you have a static IP address.
IP Address	Enter the IP address provided by your ISP. For dynamic IP, leave this field blank.
Subnet Mask	Enter the Subnet Mask address provided by your ISP. For dynamic IP, leave this field blank.
Connect Type	Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected.

Parameter	Description
Idle Time (Minute)	Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic.
Username	Enter user name provided by your ISP.
Password	Enter password provided by your ISP.
Confirm Password	Confirm password.
MTU	Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP.

### Clone MAC Address

Some ISPs require you to register your MAC address with them. If this is the case, the MAC address of the ADSL router must be changed to the MAC address that you have registered with your ISP.



## LAN

Use the LAN menu to configure the LAN IP address, VLAN binding and to enable the DHCP server for dynamic client address allocation.

**SMC®** Advanced Setup

Home Logout

**LAN Settings**

By default, the IP address of this device (on the LAN side) is 192.168.2.1. On this page, you can change this address to another one. Normally, you would not need to change it. You can also enable or disable the DHCP server function, which dynamically allocates IP addresses to your client PCs. If this function is enabled, you can select the range of IP addresses that would be used for this purpose.

Virtual LAN (VLAN) binding defines the mapping of physical ports to VLAN profiles.

**LAN IP**

IP Address: 192 . 168 . 2 . 1

IP Subnet Mask: 255.255.255. 0

**VLAN Binding**

LAN1: Default

LAN2: Default

LAN3: Default

LAN4: Default

**DHCP Server**

Parameter	Description
LAN IP	
IP Address	The IP address of the router.
IP Subnet Mask	The subnet mask of the network.
VLAN Binding	
LAN1 to LAN4	Select VLAN group for the corresponding LAN port. By default all ports members of the Default VLAN.
DHCP Server	
DHCP Server	Enable or Disable the DHCP server function. By default the DHCP server is enabled for automatic IP address assignment to client devices.
DHCP Option 60 Vendor ID	Enter the ID in this field.

## CONFIGURING THE ADSL ROUTER

<b>Parameter</b>	<b>Description</b>
Lease Time	Set the IP lease time. For home networks this may be set to Forever, which means there is no time limit on the IP address lease.
IP Address Pool	
Start IP Address	Specify the start IP address of the DHCP pool. Do not include the IP address of the ADSL router in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx.
End IP Address	Specify the end IP address of the DHCP pool.
Domain Name	If your network uses a domain name, enter it here. Otherwise, leave this field blank.
IP assignment based on MAC	You can assign a specific IP address to a specific MAC address. Enter the matching IP address and MAC address on the table.

## VLAN

VLANs are organized and controlled by VLAN Profiles. Up to 4 VLAN profiles can be created. Once a VLAN profile is created, you should add interfaces into the VLAN by changing the VLAN setting of that interface. Please note that only those interfaces of IEEE 802 bridging type (ex. LAN ports and 1483 Bridging PVCs) can be added to a VLAN.



Click **Add VLAN** to setup the profile.

**VLAN Profile**

Enter parameters of the profile to define a VLAN.

Description	<input type="text"/>			
IP Address	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
NAT Domain	<input checked="" type="radio"/> Private <input type="radio"/> Public			
IGMP Snooping	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			
IGMP Quener	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled			

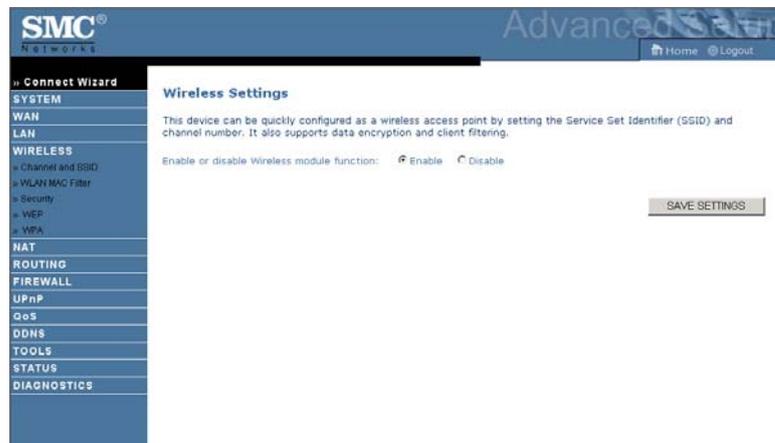
- Description: enter a name or description for the VLAN.
- IP Address: enter the IP address.
- Subnet Mask: enter the subnet mask.

## CONFIGURING THE ADSL ROUTER

- NAT Domain: select private or public.
- IGMP Snooping: Internet Group Management Protocol (IGMP) snooping is a method by which Layer 2 devices can “listen in” on IGMP conversations between hosts and routers. When a switch hears a group join message from a host, it notes which switch interface it heard the message on, and adds that interface to the group. Similarly, when a Layer 2 switch hears a group leave message or a response timer expires, the switch will remove that host’s switch interface from the group.
- IGMP Querier: if the IGMP Querier is enabled, then the router will periodically query all multicast group members on the specified VLAN.

## Wireless

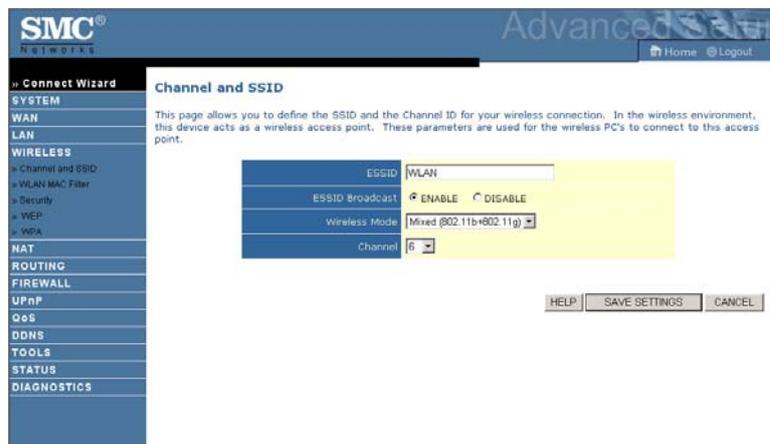
The ADSL router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the SSID, and the security options.



- Enable or disable Wireless module function: check Enable and then click SAVE SETTINGS.

### Channel and SSID

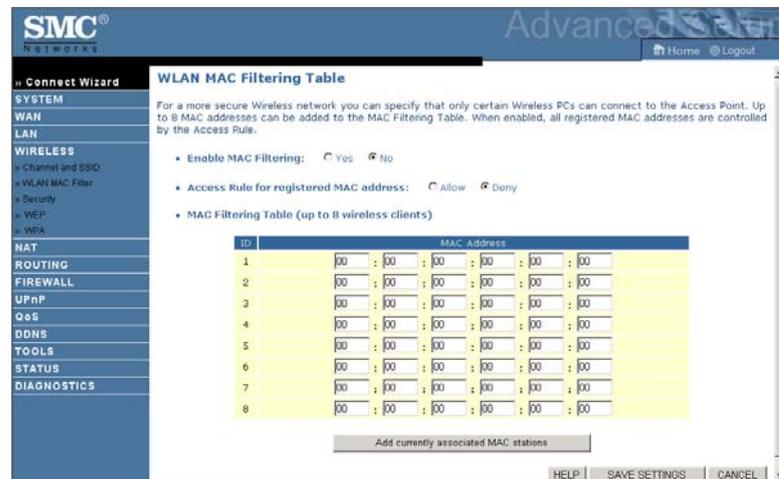
You must specify a common radio channel and SSID (Service Set ID) to be used by the ADSL router and all of its wireless clients. Be sure you configure all of its clients to the same values.



Parameter	Description
SSID	Service Set ID (SSID) is the name given to the wireless network. The SSID must be the same on the ADSL router and all of its wireless clients.
SSID Broadcast	Enable or disable the broadcasting of the SSID. Disabling broadcasting of the SSID provides added security by hiding your wireless network.
Wireless Mode	This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have.
Channel	The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the ADSL router and all of its wireless clients.  The ADSL router will automatically assign itself a radio channel, or you may select one manually.

### WLAN MAC Filter

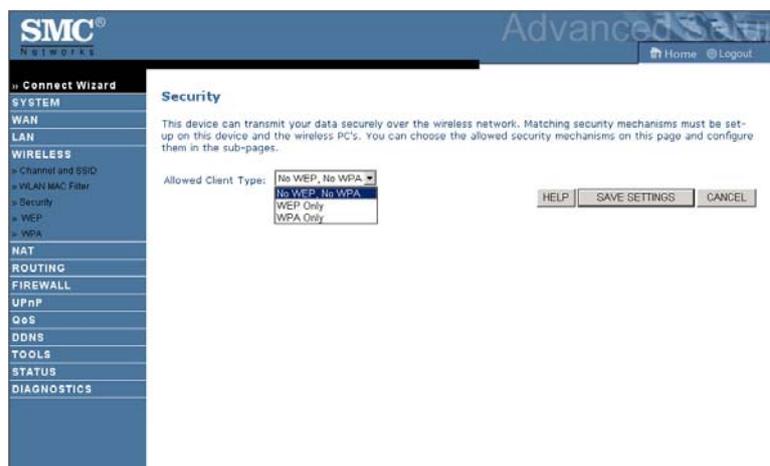
Using this MAC filter functionality, you can restrict wireless access based on MAC address. Each PC has a unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, the computers whose MAC address you have listed in the filtering table will be able to connect (or will be denied access) to the ADSL router.



- Enable MAC Filtering: select to turn on/off this feature.
- Access Rule for registered MAC address: select to allow/deny access for the registered MAC addresses. Selecting Allow means only MAC addresses registered here will be able to connect to the router. Selecting Deny means only the MAC addresses registered here will be denied access to the router.
- MAC Filtering table: enter the MAC address in the table, or you can use the option to quickly copy the currently associated client entry to the MAC Filtering table.

## Security

To make your wireless network safe, you should turn on the security function. The ADSL router supports WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected).

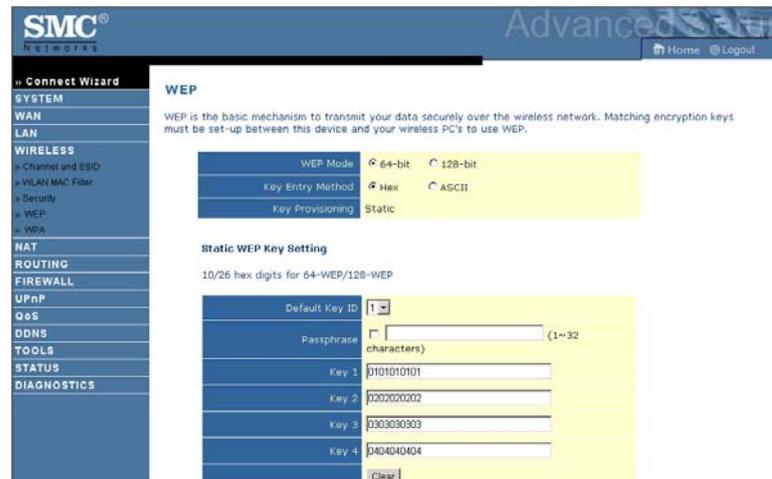


Three options are available:

- No WEP, No WPA
- WEP only
- WPA only

## WEP

If you want to use WEP to protect your wireless network, you need to set the same parameters for the ADSL router and all your wireless clients.



Parameter	Description
WEP Mode	Select 64 bit or 128 bit key to use for encryption.
Key Entry Method	Select Hex or ASCII to use for encryption key
Key Provisioning	Select Static if there is only one fixed key for encryption. If you want to select Dynamic, you would need to enable 802.1X function first.

When the key entry method is set to Hex, you can automatically generate encryption keys using the passphrase or manually enter the keys. To generate the keys using passphrase, check the box, enter a string of text, and click **GENERATE**. Select the default key from the drop-down menu and click **SAVE SETTINGS**.

## CONFIGURING THE ADSL ROUTER

Before saving settings the key is shown in clear text. If your wireless client does not have a passphrase utility, make a note of the default key before saving settings. This is so you can configure your wireless client with the correct key.

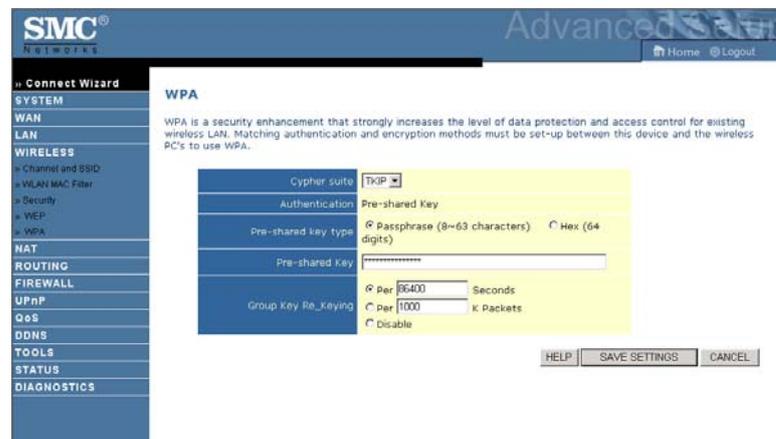
To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.)

Note that WEP protects data transmitted between wireless nodes, but does not protect any transmissions over your wired network or over the Internet.

**Note:** The passphrase can consist of up to 32 alphanumeric characters.

**WPA**

Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service.



Parameter	Description
Cypher suite	TKIP is the security mechanism used in WPA for encryption.
Authentication	Pre-shared key: for the SOHO network environment without an authentication server.
Pre-shared key type	Select the key type to be used in the Pre-shared Key.
Pre-shared Key	Type in the key here.
Group Key Re_keying	The period of renewing broadcast/multicast key.

## NAT

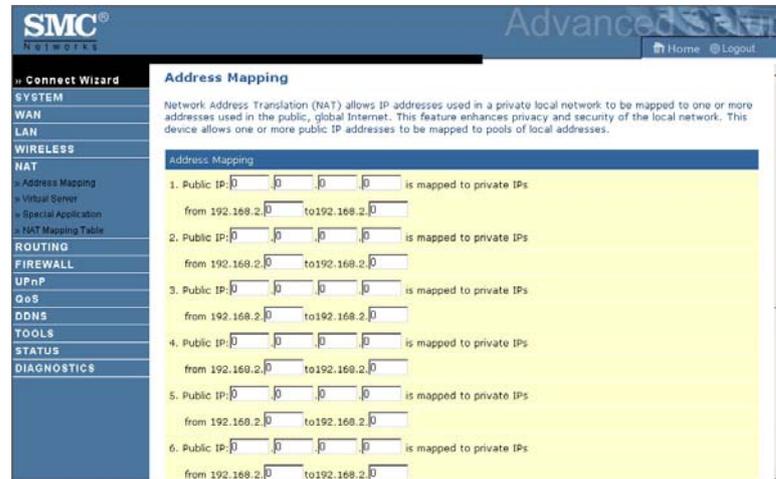
Network Address Translation allows multiple users to access the Internet sharing one public IP.



- Enable or disable NAT module function: select to turn on/turn off this function.

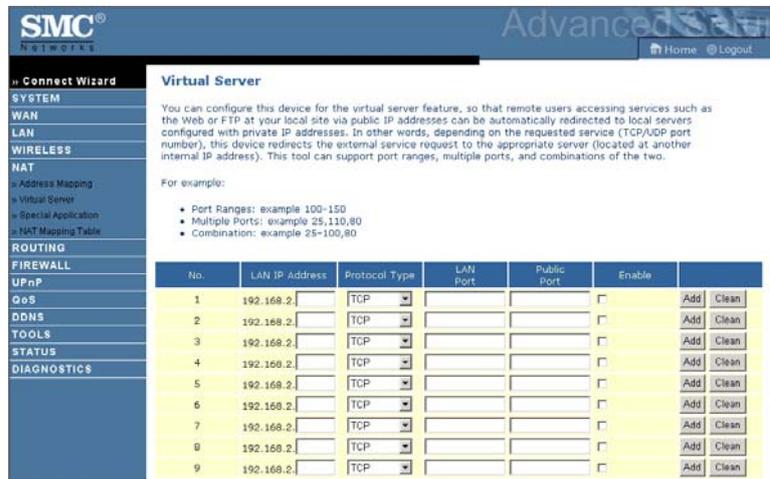
### Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security. 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 into the “from” field.



### Virtual Server

If you configure the ADSL 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 ADSL 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.

A list of ports is maintained at the following link:  
<http://www.iana.org/assignments/port-numbers>.

### Special Application

Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these screens to specify the additional public ports to be opened for each application.

**Special Applications**

Some applications, such as Internet gaming, video conferencing and Internet telephony, require multiple connections in order to work properly. 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 the 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	Public Type	Enabled
1.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
6.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
7.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

### NAT Mapping Table

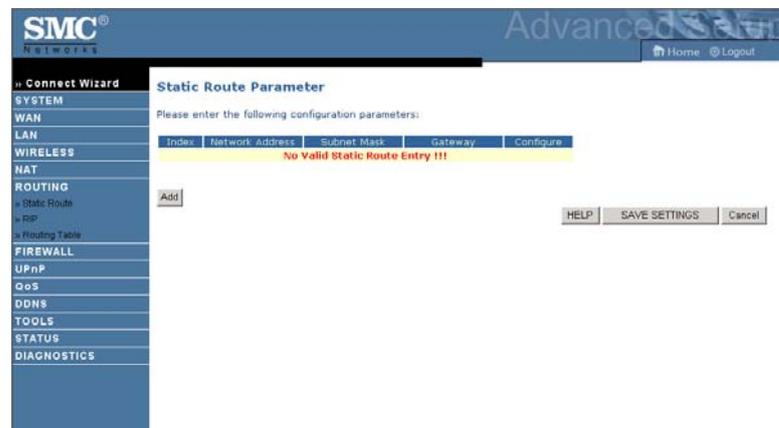
This screen displays the current NAPT (Network Address Port Translation) address mappings.



## Routing

These screens define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

### Static Route

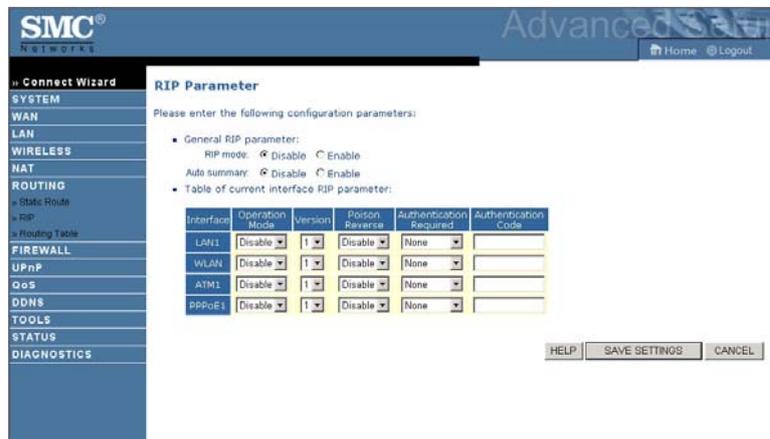


Parameter	Description
Index	Check the box of the route you wish to delete or modify.
Network Address	Enter the IP address of the remote computer for which to set a static route.
Subnet Mask	Enter the subnet mask of the remote network for which to set a static route.
Gateway	Enter the WAN IP address of the gateway to the remote network.

Click **Add** to add a new static route to the list, or check the box of an already entered route and click **Modify**. Clicking **Delete** will remove an entry from the list.

**RIP**

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.



Parameter	Description
<b>General RIP Parameters</b>	
RIP mode	Globally enables or disables RIP.
Auto summary	If Auto summary is disabled, then RIP packets will include sub-network information from all sub-networks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all sub-networks.
<b>Table of current Interface RIP parameter</b>	
Interface	The WAN interface to be configured.

<b>Parameter</b>	<b>Description</b>
Operation Mode	<p>Disable: RIP disabled on this interface.</p> <p>Enable: RIP enabled on this interface.</p> <p>Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.</p>
Version	Sets the RIP (Routing Information Protocol) version to use on this interface.
Poison Reverse	A method for preventing loops that would cause endless retransmission of data traffic.
Authentication Required	<ul style="list-style-type: none"> <li>• None: No authentication.</li> <li>• Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.</li> <li>• MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.</li> </ul>
Authentication Code	Password or MD5 Authentication key.

## Routing Table




---

### Parameter Description

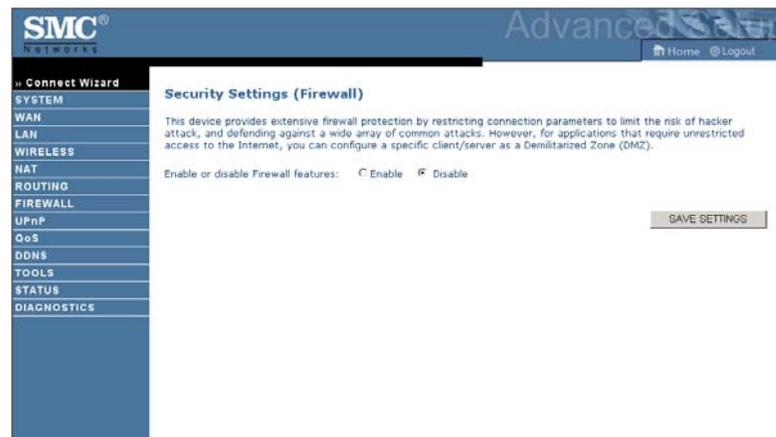
Flags	Indicates the route status: C = Direct connection on the same subnet. S = Static route. R = RIP (Routing Information Protocol) assigned route. I = ICMP (Internet Control Message Protocol) Redirect route.
Network Address	Destination IP address.
Netmask	The subnetwork associated with the destination.  This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the subnet mask number; each bit that corresponds to "0" is part of the host number.
Gateway	The IP address of the router at the next hop to which frames are forwarded.
Interface	The local interface through which the next hop of this route is reached.
Metric	When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

---

## Firewall

The ADSL router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

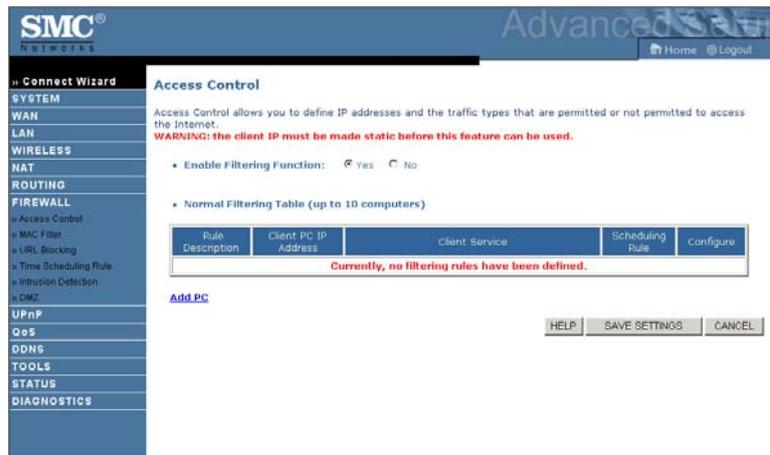


The ADSL router protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (For details see page 4-48.)

The firewall does not significantly affect system performance, so we advise leaving it enabled to protect your network. Select **Enable** and click the **SAVE SETTINGS** button to open the Firewall submenus.

### Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface.



Parameter	Description
Enable Filtering Function	Click Yes to turn on the filtering function.
Normal Filtering Table	Displays a summary of the filtering rules configured.

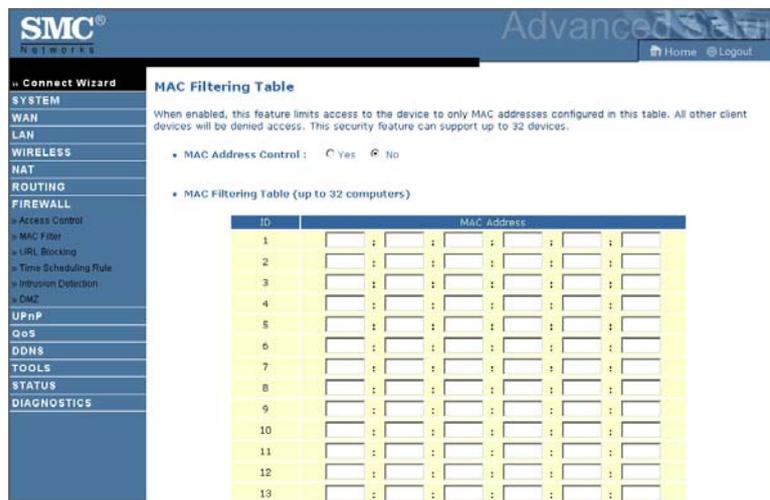
To add the PC to the filtering table:

1. Click **Add PC** on the Access Control screen.
2. Define the appropriate settings for client PC services.
3. Click **OK** and then click **SAVE SETTINGS** to save your settings.



### MAC Filter

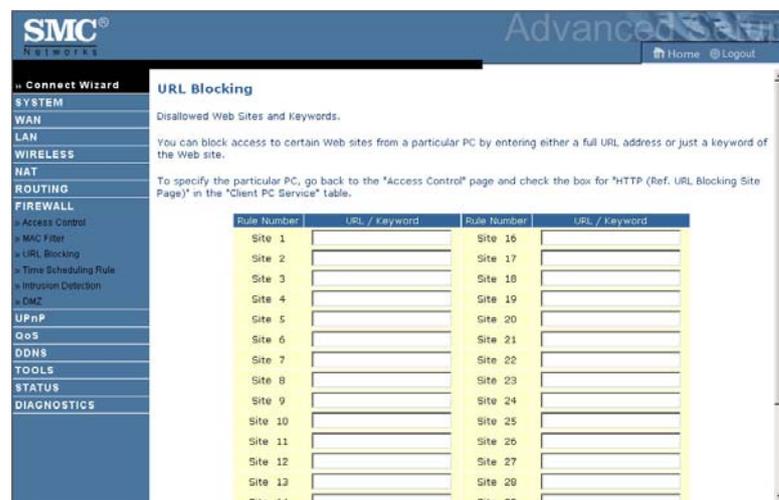
The ADSL router can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the ADSL router to enter up to 32 MAC addresses that are not allowed access to the WAN port. Please note that this filter only applies to ethernet clients.



- Click **Yes** to enable, or **No** to disable this function.
- Enter the MAC address in the space provided.

### URL Blocking

The ADSL router allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.



You can define up to 30 sites here.

### Time Scheduling Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the Time Scheduling Rule screen, and apply the rule on the Access Control screen.



Follow these steps to add a schedule rule:

1. Click **Add Scheduling Rule** on the Time schedule rule screen.
2. Define the appropriate settings for a schedule rule.
3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

The screenshot displays the SMC Network Advanced Setup interface. On the left is a navigation menu with categories: SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL (with sub-items: Access Control, MAC Filter, URL Blocking, Time Scheduling Rule, Intrusion Detection), DMZ, UPnP, QoS, DDNS, TOOLS, STATUS, and DIAGNOSTICS. The main content area is titled 'Edit Scheduling Rule' and includes a 'Name:' text box, a 'Comment:' text box, and an 'Activate Time Period:' section. This section contains a table with columns for 'Week Day', 'Start Time (hh:mm)', and 'End Time (hh:mm)'. The table lists days from 'Every Day' to 'Saturday', each with input fields for hours and minutes. Below the table are 'OK' and 'Cancel' buttons.

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

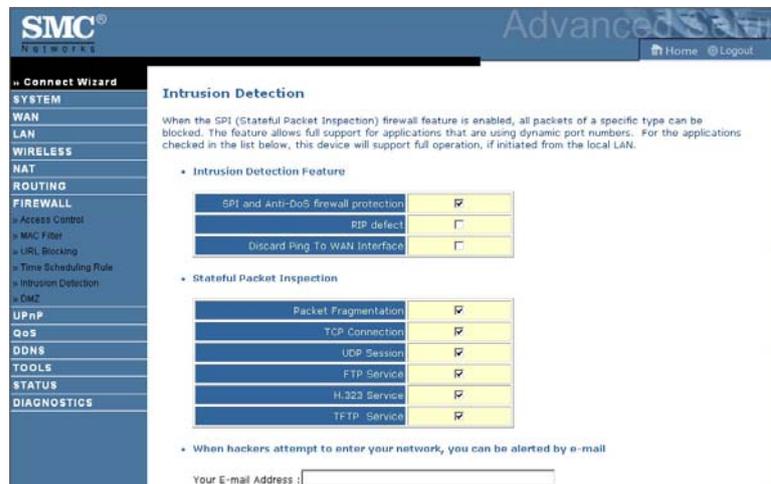
## Intrusion Detection

- **Intrusion Detection Feature**

Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: enabled) — The Intrusion Detection Feature of the ADSL router 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 in the Stateful Packet Inspection section.

RIP Defect (Default: disabled) — If an RIP request packet is not acknowledged 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 from accumulating.

Discard Ping to WAN (Default: disabled) — Prevent a ping on the WAN port of the ADSL router from being routed to the network.



Scroll down to view more information.

ADVANCED SETUP

SMC Networks Advanced Setup

Home Logout

Connect Wizard

- SYSTEM
- WAN
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
  - Access Control
  - MAC Filter
  - URL Blocking
  - Time Scheduling Rule
  - Intrusion Detection
  - DMZ
- UPnP
- QoS
- DDNS
- TOOLS
- STATUS
- DIAGNOSTICS

When hackers attempt to enter your network, you can be alerted by e-mail

Your E-mail Address :

SMTP Server Address :

POP3 Server Address :

User name :

Password :

Connection Policy

Fragmentation half-open wait:  sec.

TCP SYN wait:  sec.

TCP FIN wait:  sec.

TCP connection idle timeout:  sec.

UDP session idle timeout:  sec.

H.323 data channel idle timeout:  sec.

DoS Detect Criteria:

SMC Networks Advanced Setup

Home Logout

Connect Wizard

- SYSTEM
- WAN
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
  - Access Control
  - MAC Filter
  - URL Blocking
  - Time Scheduling Rule
  - Intrusion Detection
  - DMZ
- UPnP
- QoS
- DDNS
- TOOLS
- STATUS
- DIAGNOSTICS

UDP session idle timeout:  sec.

H.323 data channel idle timeout:  sec.

DoS Detect Criteria:

Total incomplete TCP/UDP sessions HIGH:  session

Total incomplete TCP/UDP sessions LOW:  session

Incomplete TCP/UDP sessions (per min) HIGH:  session

Incomplete TCP/UDP sessions (per min) LOW:  session

Maximum incomplete TCP/UDP sessions number from same host:

Incomplete TCP/UDP sessions detect sensitive time period:  msec.

Maximum half-open fragmentation packet number from same host:

Half-open fragmentation detect sensitive time period:  msec.

Flooding cracker block time:  sec.

HELP SAVE SETTINGS CANCEL

- **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, or TFTP Service.

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

Enter your email 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.

<b>Parameter</b>	<b>Defaults</b>	<b>Description</b>
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 for which a TCP session will be managed if there is no activity.
UDP session idle timeout	30 sec	The length of time for which a UDP session will be managed if there is no activity.
H.323 data channel idle timeout	180 sec	The length of time for which an H.323 session will be managed 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 new unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions.
Total incomplete TCP/UDP sessions LOW	250 sessions	Defines the rate of new unestablished sessions that will cause the software to <i>stop</i> 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.
Maximum incomplete TCP/UDP sessions number from same host	10	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	10000 msec	Length of time before a half-open fragmentation session is detected as half-open.
Flooding cracker block time	300 second	Length of time from detecting a flood attack to blocking the attack.

**Note:** The firewall does not significantly affect system performance, so we advise enabling the prevention features, and leaving them at the default settings to protect your network.

### DMZ

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

The screenshot shows the SMC Network Advanced Setup interface. The left sidebar contains a navigation menu with categories: SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, and TOOLS. The main content area is titled "DMZ (Demilitarized Zone)".

**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. You can define one DMZ host for each public IP address that you have (usually only one).

Enable DMZ:  Yes  No

To use the DMZ, you must set a static IP address for that PC. DMZ should be used only as a last resort, when you cannot use Virtual Server or Special Application from the NAT menu. Even then, you should disable DMZ immediately after the session for which you had to enable it.

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

At the bottom right, there are three buttons: HELP, SAVE SETTINGS, and CANCEL.

## UPnP

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 office, home and everywhere within your network.



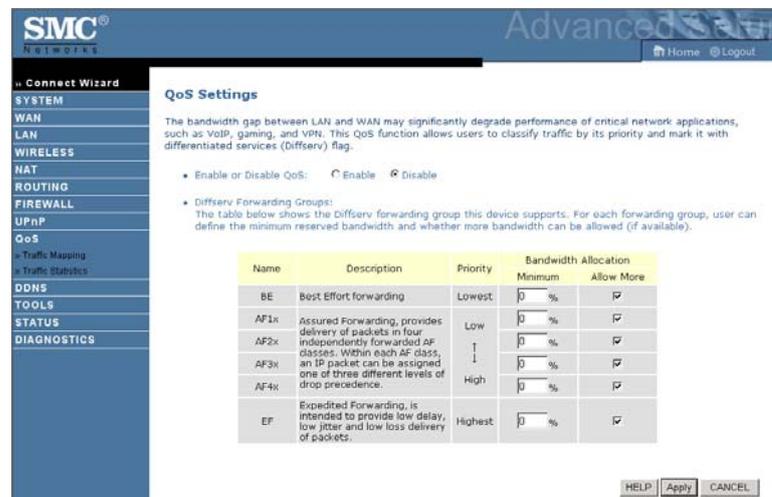
UPnP allows the device to automatically:

- join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices.

Check the **Enable** option to activate the function.

## QoS

The QoS (Quality of Service) function allows you to differentiate traffic types and provide high-priority forwarding service for applications such as VoIP or gaming.



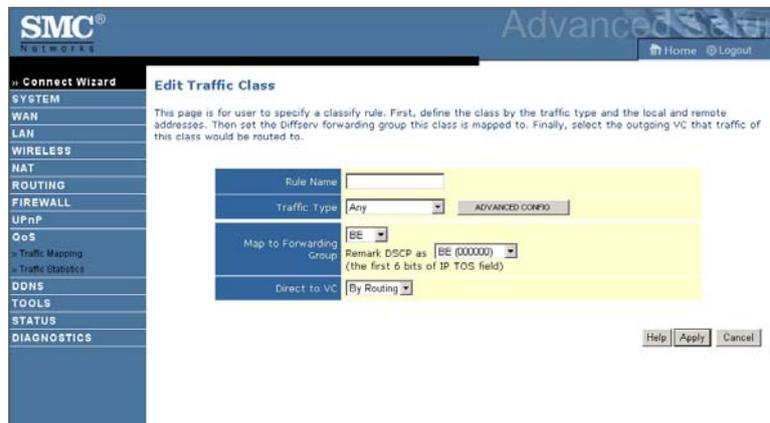
Parameter	Description
Enable or disable QoS module function	Check to enable or disable this function.
Diffserv Forwarding Groups	
BE	Best Effort forwarding, set the percentage for this type of QoS.
AF1x	Set the percentage for four different types of Assured Forwarding.
AF2x	
AF3x	
AF4x	
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.

## Traffic Mapping

Use this screen to classify traffic into Diffserv forwarding groups and outgoing VCs.



Click **Add traffic class** to add a new rule for traffic class.



### Traffic Statistics

This screen shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours.

**Traffic Statistics**

This page shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours.

Forwarding Behavior	Average sent byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

Forwarding Behavior	Average dropped byte/sec			
	5 min	1 hour	6 hour	12 hour
BE	0	0	0	0
AF1x	0	0	0	0
AF2x	0	0	0	0
AF3x	0	0	0	0
AF4x	0	0	0	0
EF	0	0	0	0

HELP Refresh

Click **Refresh** to renew the list.

## DDNS

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

The screenshot shows the SMC Advanced Networking web interface. On the left is a sidebar with a menu including: Connect Wizard, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, UPnP, QoS, DDNS, TOOLS, STATUS, and DIAGNOSTICS. The main content area is titled "DDNS (Dynamic DNS) Settings". Below the title is a descriptive paragraph: "Dynamic DNS provides users on the Internet a method to tie their fixed domain name(s) to their dynamically assigned IP addresses. When this feature is enabled, this device will automatically update your DDNS records whenever IP address changes." Below this is a form with the following fields: "Dynamic DNS" with radio buttons for "Enable" (selected) and "Disable"; "Provider" with a dropdown menu showing "DynDNS.org"; "Domain Name" with a text input field containing "TZO.com"; "Account / E-mail" with an empty text input field; and "Password / Key" with an empty text input field. At the bottom right of the form area are three buttons: "HELP", "SAVE SETTINGS", and "CANCEL".

This DDNS feature is powered by:

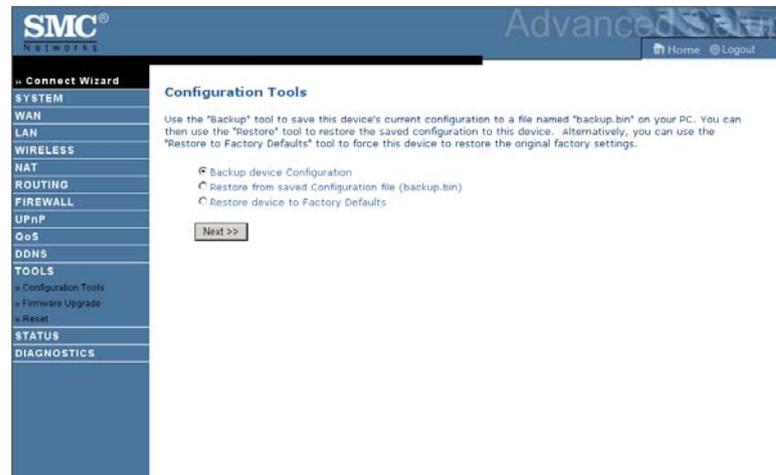
- DynDNS.org
- TZO.com

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.

## Tools

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

### Configuration Tools



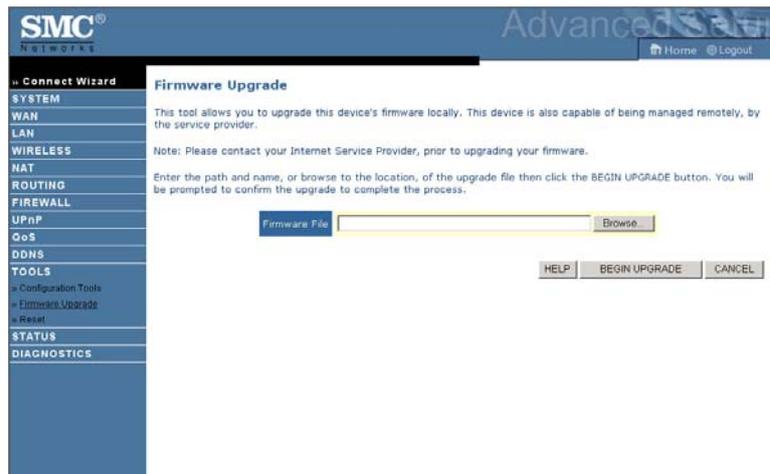
- Backup allows you to save the ADSL router's configuration to a file.
- Restore can be used to restore the previously saved backup configuration file.
- Restore to Factory Defaults resets the ADSL router back to the original settings.

Choose a function and click **Next**.

## Firmware Upgrade

Use this screen to update the firmware or user interface to the latest versions.

1. Download the upgrade file from the SMC web site first, and save it to your hard drive.
2. In the Firmware file field, click “**Browse...**” to look for the downloaded file. Click **BEGIN UPGRADE**.
3. Check the Status screen Information section to confirm that the upgrade process was successful.



### Reset

Click **REBOOT ROUTER** to reset the ADSL router. The reset will be complete when the power LED stops blinking.



If you perform a reset from this screen, the configurations will not be changed back to the factory default settings.

**Note:** If you use the Reset button on the back panel, the ADSL router performs a power reset. If the button is pressed for over five seconds, all the LEDs will illuminate and the factory default 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. The security log may be saved to a file by clicking “Save” and choosing a location.



Scroll down to view more information.

**SMC NETWORKS** Advanced Setup

Home Logout

**Connect Wizard**

- SYSTEM
- WAN
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
- UPnP
- QoS
- DDNS
- TOOLS
- STATUS
- DIAGNOSTICS

**ATM PVC**

VC	
VPI/VCI	8/35
Encapsulation	LLC
Protocol	PPPoE
IP Address	Down
Subnet Mask	---
Gateway	---
Primary DNS	---
Secondary DNS	---

Disconnect Connect

**ADSL Status Information:**

- Status:
 

	Configured	Current
Line Status	---	QUIET1
Link Type	---	Fast Path
- Data Rate:
 

Stream Type	Actual Data Rate
Up Stream	0 (Kbps.)
Down Stream	0 (Kbps.)
- Operation Data / Defect Indication:
 

Operation Data	Upstream	Downstream
	0 dB	0 dB

**SMC NETWORKS** Advanced Setup

Home Logout

**Connect Wizard**

- SYSTEM
- WAN
- LAN
- WIRELESS
- NAT
- ROUTING
- FIREWALL
- UPnP
- QoS
- DDNS
- TOOLS
- STATUS
- DIAGNOSTICS

**ADSL Status Information:**

- Status:
 

	Configured	Current
Line Status	---	QUIET1
Link Type	---	Fast Path
- Data Rate:
 

Stream Type	Actual Data Rate
Up Stream	0 (Kbps.)
Down Stream	0 (Kbps.)
- Operation Data / Defect Indication:
 

Operation Data	Upstream	Downstream
Noise Margin	0 dB	0 dB
Attenuation	0 dB	0 dB

Indicator Name	Near End Indicator	Far End Indicator
Fast Path FEC Correction	0	0
Interleaved Path FEC Correction	0	0
Fast Path CRC Error	0	0
Interleaved Path CRC Error	0	0
Loss of Signal Defect	0	---
Fast Path HEC Error	0	0
Interleaved Path HEC Error	0	0
- Statistics:
 

Received Cells	0
Transmitted Cells	0

CONFIGURING THE ADSL ROUTER

The screenshot displays the SMC Advanced Router web interface. The left sidebar contains a navigation menu with the following items: Connect Wizard, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, UPnP, QoS, DDNS, TOOLS, STATUS, and DIAGNOSTICS. The main content area is divided into several sections:

- Statistics:** A table showing network performance metrics:
 

Fast Path FEC Correction	0	0
Interleaved Path FEC Correction	0	0
Fast Path CRC Error	0	0
Interleaved Path CRC Error	0	0
Loss of Signal Defect	0	—
Fast Path HEC Error	0	0
Interleaved Path HEC Error	0	0
- Statistics (continued):** A small table showing cell counts:
 

Received Cells	0
Transmitted Cells	0
- Security Log:** A log of network access attempts. The entries are:
 

```
08/01/2003 05:21:56 192.168.2.2 lo
08/01/2003 05:21:56 User from 192.
08/01/2003 04:40:28 192.168.2.2 lo
08/01/2003 04:40:28 User from 192.
08/01/2003 04:10:49 sending ACK to
08/01/2003 04:09:51 192.168.2.2 lo
08/01/2003 04:09:51 User from 192.
08/01/2003 02:50:00 sending ACK to
08/01/2003 02:50:00 sending OFFER
```
- DHCP Client Log:** A log of LAN DHCP clients currently linked to the router. The entries are:
 

```
ip=192.168.2.2 mac=00-E0-29-BB-07
ip=192.168.2.3 mac=00-13-02-11-9D
ip=192.168.2.4 mac=00-18-77-10-99
ip=192.168.2.5 mac=00-16-6F-8F-63
ip=192.168.2.6 mac=00-1C-10-01-FE
```

At the bottom of the Security Log and DHCP Client Log sections, there are buttons for 'Save', 'Clear', and 'Refresh'. A 'HELP' button is located at the bottom right of the interface.

## Diagnostics

The diagnostics screen provides a quick view for you to troubleshoot the connection status for LAN ports, WAN port, and Internet access.

The screenshot shows the 'Diagnostics' page in the SMC Advanced Setup interface. The page is divided into a sidebar menu and a main content area. The sidebar menu includes options like SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTING, FIREWALL, UPnP, CoS, DDNS, TOOLS, STATUS, and DIAGNOSTICS. The main content area is titled 'Diagnostics' and displays connection status for LAN, Ethernet, WAN, and Internet Access. It includes fields for IP addresses, link status, and buttons for testing connections like 'Ping', 'Query', and 'Diagnose Again'.

LAN Connection (LAN IP=192.168.2.1, Subnet=255.255.255.0)			
LAN1:	N/A	Link Down	
LAN2:	N/A	Link Down	
LAN3:	100 Mbps Full-Duplex	Link Up	ARP Table
LAN4:	N/A	Link Down	

WAN Connection (WAN IP=0.0.0.0, Subnet=255.255.255.0)			
ADSL	VPI/VCI=0/33	Physical Down	Rescan
PPPoE Server			
Authentication	UserName/Password=a1Gjz7NeEP@dsl.rogers.ca/?jagohq:8P		Retry

Internet Access			
Ping Gateway	Gateway IP= 0.0.0.0		Ping
Query 1st DNS	1st DNS IP= 0.0.0.0 Host Name=		Query
Query 2nd DNS	2nd DNS IP= 0.0.0.0 Host Name=		Query
Ping a Server	Host Name=		Ping

Diagnose Again

## **Finding the MAC address of a Network Card**

### **Windows 2000/XP**

Click Start/Programs/Command Prompt. Type “ipconfig /all” and press “ENTER”.

The MAC address is listed as the “Physical Address.”

### **Macintosh**

Click System Preferences/Network.

The MAC address is listed as the “Ethernet Address” on the TCP/IP tab.

### **Linux**

Run the command “/sbin/ifconfig.”

The MAC address is the value after the word “HWaddr.”

# APPENDIX A

## TROUBLESHOOTING

---

This section describes common problems you may encounter and possible solutions to them. The ADSL router can be easily monitored through panel indicators to identify problems.

<b>Troubleshooting Chart</b>	
<b>Symptom</b>	<b>Action</b>
LED Indicators	
Power LED is Off	<ul style="list-style-type: none"><li>• Check connections between the ADSL router, the external power supply, and the wall outlet.</li><li>• 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. However, 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 still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.</li></ul>

<b>Troubleshooting Chart</b>	
<b>Symptom</b>	<b>Action</b>
LED Indicators	
Link LED is Off	<ul style="list-style-type: none"> <li>• Verify that the ADSL router and attached device are powered on.</li> <li>• Be sure the cable is plugged into both the ADSL router and the corresponding device.</li> <li>• Verify that the proper cable type is used and that its length does not exceed the specified limits.</li> <li>• Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode.</li> <li>• Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.</li> </ul>
Network Connection Problems	
Cannot ping the ADSL router from the attached LAN	<ul style="list-style-type: none"> <li>• Verify that the IP addresses are properly configured. For most applications, you should use the ADSL router's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure 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 ADSL router and any attached LAN devices.</li> <li>• Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP.</li> </ul>

<b>Troubleshooting Chart</b>	
<b>Symptom</b>	<b>Action</b>
Management Problems	
Cannot connect using the web browser	<ul style="list-style-type: none"> <li>• Be sure to have configured the ADSL router with a valid IP address, subnet mask, and default gateway.</li> <li>• Check that you have a valid network connection to the ADSL router and that the port you are using has not been disabled.</li> <li>• Check the network cabling between the management station and the ADSL router.</li> </ul>
Forgot or lost the password	<ul style="list-style-type: none"> <li>• Press the Reset button on the rear panel (holding it down for at least five seconds) to restore the factory defaults.</li> </ul>

<b>Troubleshooting Chart</b>	
<b>Symptom</b>	<b>Action</b>
Wireless Problems	
A wireless PC cannot associate with the ADSL router.	<ul style="list-style-type: none"> <li>• Make sure the wireless PC has the same SSID settings as the ADSL router. See “Channel and SSID” on page 4-26.</li> <li>• You need to have the same security settings on the clients and the ADSL router. See “Security” on page 4-28.</li> </ul>
The wireless network is often interrupted.	<ul style="list-style-type: none"> <li>• Move your wireless PC closer to the ADSL router to find a better signal. If the signal is still weak, change the angle of the antenna.</li> <li>• There may be interference, possibly caused by a microwave ovens or wireless phones. Change the location of the interference sources or of the ADSL router.</li> <li>• Change the wireless channel on the ADSL router. See “Channel and SSID” on page 4-26.</li> <li>• Check that the antenna, connectors, and cabling are firmly connected.</li> </ul>
The ADSL router cannot be detected by a wireless client.	<ul style="list-style-type: none"> <li>• The distance between the ADSL router and wireless PC is too great.</li> <li>• Make sure the wireless PC has the same SSID and security settings as the ADSL router. See ADSL router. See “Channel and SSID” on page 4-26 and “Security” on page 4-28.</li> </ul>

# APPENDIX B

## CABLES

---

### Ethernet Cable

**Caution:** DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

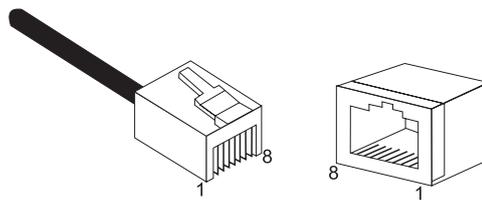
### Specifications

Cable Types and Specifications			
Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

### Wiring Conventions

For Ethernet connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-45 connectors in a specific orientation. The following figure illustrates how the pins on an Ethernet RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



**Figure B-1. RJ-45 Ethernet Connector Pin Numbers**

### **RJ-45 Port Connection**

Use the straight-through CAT-5 Ethernet cable provided in the package to connect the ADSL router to your PC. When connecting to other network devices such as an Ethernet switch, use the cable type shown in the following table.

<b>Attached Device Port Type</b>	<b>Connecting Cable Type</b>
MDI-X	Crossover
MDI	Straight-through

## Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

<b>RJ-45 Pin Assignments</b>	
Pin Number	Assignment <sup>1</sup>
1	Tx+
2	Tx-
3	Rx+
6	Rx-

1: The “+” and “-” signs represent the polarity of the wires that make up each wire pair.

## Straight-Through Wiring

If the port on the attached device has internal crossover wiring (MDI-X), then use straight-through cable.

<b>Straight-Through Cable Pin Assignments</b>	
End 1	End 2
1 (Tx+)	1 (Tx+)
2 (Tx-)	2 (Tx-)
3 (Rx+)	3 (Rx+)
6 (Rx-)	6 (Rx-)

**Crossover Wiring**

If the port on the attached device has straight-through wiring (MDI), use crossover cable.

<b>Crossover Cable Pin Assignments</b>	
End 1	End 2
1 (Tx+)	3 (Rx+)
2 (Tx-)	6 (Rx-)
3 (Rx+)	1 (Tx+)
6 (Rx-)	2 (Tx-)

# APPENDIX C

## SPECIFICATIONS

---

### **Physical Characteristics**

#### **Ports**

Four 10/100Mbps RJ-45 Ports

One ADSL RJ-11

#### **ADSL Features**

Supports DMT line modulation

Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 & T1.413, Issue 2)

Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps upstream

Supports ADSL2/2+: up to 24Mbps downstream, up to 1Mbps upstream

Dying GASP support

#### **ATM Features**

RFC1483 Encapsulation (IP, Bridging and encapsulated routing)

PPP over ATM (LLC & VC multiplexing) (RFC2364)

Classical IP (RFC1577)

Traffic shaping (UBR, CBR)

OAM F4/F5 support

PPP over Ethernet Client

#### **Management Features**

Firmware upgrade via WEB Based Management

WEB Based Management (configuration)

Power Indicators

Event and History logging

Network Ping

**Security Features**

Password protected configuration access  
User authentication (PAP/CHAP) with PPP  
Firewall NAT NAPT  
VPN pass through

**LAN Features**

IEEE 802.1D (self-learning transparent Bridging)  
DHCP Server  
DNS Proxy  
Static Routing, RIPv1 and RIP

**Applications**

Netmeeting, ICQ, Real Player, QuickTime, DialPad, PC Anywhere, Telnet,  
SNTP, NNTP

**Modulation Type**

OFDM, CCK

**Operating Channels IEEE 802.11b compliant:**

11 channels (US, Canada)  
13 channels (ETSI)  
14 channels (Japan)

**Operating Channels IEEE 802.11g compliant:**

11 channels (US, Canada)  
13 channels (ETSI)  
13 channels (Japan)

**Environmental**

Temperature: IEC 68-2-14  
0 to 40 degrees C (Standard Operating)  
-20 to 70 degree C (Non-operation)  
Humidity: 10% to 95% (Noncondensing)

**Vibration:** IEC 68-2-36, IEC 68-2-6

**Shock:** IEC 68-2-29

**Drop:** IEC 68-2-32

## SPECIFICATIONS

### **Dimensions**

159.3 x 133.4 x 32.1 (mm)

### **Weight**

290 g

### **Input Power**

12 V 1 A

### **IEEE Standards**

IEEE 802.3, 802.3u, 802.11g, 802.1D

ITU G.dmt

ITU G.Handshake

ITU T.413 issue 2 - ADSL full rate

### **Standards Conformance Electromagnetic Compatibility**

CE

R&TTE

ETSI

FCC part 15 Class B

FCC part 68

RoHS

### **Safety**

EN 60950-1 & IEC 60950-1

### **Internet Standards**

RFC 826 ARP

RFC 791 IP

RFC 792 ICMP

RFC 768 UDP

RFC 793 TCP

RFC 783 TFTP

RFC 1483 AAL5 Encapsulation

RFC 1661 PPP

RFC 1866 HTML

RFC 2068 HTTP

RFC 2364 PPP over ATM