

DOCSIS 3.0 Wireless Cable Modem Gateway

SMCD3GN3 Administrator User Manual

FastFind Links

Getting to Know the Gateway

Installing the Gateway

Configuring Your Computer for TCP/IP

Configuring the Gateway

SMC Networks
20 Mason
Irvine, CA. 92618
U.S.A.

Copyright © 2011 SMC Networks
All Rights Reserved

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written permission of SMC.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Apple and Macintosh are registered trademarks of Apple, Inc. All other brands, product names, trademarks, or service marks are property of their respective owners.

This product (Model :SMCD3GN3) includes software code developed by third parties, including software code subject to the GNU General Public License (“GPL”) or GNU Lesser General Public License (LGPL”). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL used in this product, are available to you at <http://gpl.smc.com/>. The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and LGPL.

Contents

Preface	vi
Key Features	vii
Document Organization.....	viii
Document Conventions	viii
Safety and Warnings	viii
Typographic Conventions.....	ix
1 Getting to Know the Gateway	10
Unpacking Package Contents	11
System Requirements	11
Front Panel.....	12
Configuring Wireless Security	14
Rear Panel	14
Restoring Factory Defaults.....	15
2 Installing the Gateway	16
Finding a Suitable Location	17
Connecting to the LAN	17
Connecting the WAN.....	18
Powering on the Gateway	18
3 Configuring Your Computer for TCP/IP	19
Configuring Microsoft Windows 2000.....	20
Configuring Microsoft Windows XP	21
Configuring Microsoft Windows Vista.....	22
Configuring Microsoft Windows 7	24
Configuring an Apple [®] Macintosh [®] Computer	26
4 Configuring the Gateway	28
Pre-configuration Guidelines	29
Disabling Proxy Settings.....	29
Disabling Proxy Settings in Internet Explorer	29
Disabling Proxy Settings in Firefox.....	29
Disabling Proxy Settings in Safari	30
Disabling Firewall and Security Software	30
Accessing the Gateway's Web Management.....	31
Understanding the Web Management Interface Screens	32

Web Management Interface Menus and Submenus	33
System Settings Menu.....	36
Password Settings Menu.....	38
Remote Management Menu	43
Customer UI Setup Menu	44
WAN Settings Menu	46
MAC Spoofing Menu	49
LAN Settings Menu.....	50
Ether Switch Port Control Menu	53
LAN Access Control Menu	54
Controlling LAN Access	56
Adding and Deleting Trusted Client Stations	56
Adding and Deleting Untrusted Client Stations	57
Additional Public Lan Menu	58
Adding Public Subnets	59
Public IP Access Control Menu	60
QoS Settings Menu	62
Port Based QoS Menu.....	64
CoS Settings Menu.....	65
DSCP Based QoS Menu	67
Queue Settings Menu	69
DSCP Remarking Menu	71
Routing Menus	73
Static Routes Menu	73
RIP Control Menu	75
OSPF Control Menu	79
Adding OSPF Areas to the Cable Interface.....	81
Wireless Basic Settings Menu	83
Wireless Encryption Settings Menu.....	85
WPS Setup.....	88
MAC Filtering.....	91
Adding and Deleting Wireless Client Stations	92
Advanced Wireless Settings Menu.....	93
NAT Settings	95
Port Forwarding Menu	96
Adding Predefined Services	97
Adding Customer-Defined Services	99
1-to-1 Mapping Menu	102
Security Settings (Firewall) Menu.....	105
Enabling or Disabling Firewall	105
Configuring Access Control	107
Configuring Special Applications	119

Configuring URL Blocking	122
Configuring Schedule Rules	124
Configuring Email and Syslog Alerts	125
Configuring DMZ Settings	129
Using the Configuration Tools Menu	130
Switching Working Scripts	132
Backing Up the Gateway's Current Configuration Locally	132
Restoring the Gateway's Current Configuration Locally	133
Backing Up the Gateway's Current Configuration Remotely	134
Restoring the Gateway's Current Configuration Remotely	135
Restoring Factory Defaults	136
Using the Reboot Menu to Reboot the Gateway	137
Using the Diagnostics Menu	138
Using the Ping Tool	139
Using the Trace Route Tool	141
Sending Inspected Traffic to a Log Server	143
Using the SNTP Menu	144
Configuring VPN Settings	145
Using the VPN Menu	145
Using the Access Control Menu to Allow CPEs to Access IPSec VPN Tunnel	147
Using the VPN – Tunnel Configuration Menu	148
Using the VPN – PPTP / L2TP User Configuration Menu	153
Viewing Status Information	156
Viewing Cable Status Information	158
Appendix A - Compliances	160
Index	161

Preface

Congratulations on your purchase of the SMCD3GN3 Wireless Cable Modem Gateway. The SMCD3GN3 Wireless Cable Modem Gateway is the ideal all-in-one wired and wireless solution for the home or business environment. SMC is proud to provide you with a powerful, yet simple communication device for connecting your local area network (LAN) to the Internet.

This user manual contains all the information administrators need to install and configure your new SMCD3GN3 Wireless Cable Modem Gateway.



Key Features

The following list summarizes the Gateway's key features.

- Integrated, CableLabs-compliant DOCSIS 1.1/ 2.0 /3.0 cable modem
- Four 10/100/1000 Mbps Auto-Sensing LAN ports with Auto-MDI/MDIX
- High-speed 300 Mbps IEEE 802.11n Wireless Access Point
- Dynamic Host Configuration Protocol (DHCP) for dynamic IP configuration, and Domain Name System (DNS) for domain name mapping
- One USB 2.0 port
- IEEE 802.11 b/g/n interoperability with multiple vendors
- Wireless WEP, WPA, and WPA2 encryption, Hide SSID, and MAC Filtering
- VPN pass-through support using PPTP, L2TP, or IPSec
- Advanced SPI firewall Gateway for enhanced network security from attacks over the Internet:
 - Firewall protection with Stateful Packet Inspection
 - Client privileges
 - Hacker prevention
 - Protection from denial of service (DoS) attacks
 - Network Address Translation (NAT)
- Universal Plug and Play (UPnP) enables seamless configuration of attached devices
- Quality of Service (QoS) ensures high-quality performance with existing networks
- Effortless plug-and-play installation
- Intuitive graphical user interface (GUI) configuration, regardless of operating system
- Comprehensive front panel LEDs for network status and troubleshooting
- Compatible with all popular Internet applications

Document Organization

This document consists of four chapters and two appendixes.





- **Chapter 1** - describes the contents in the Gateway package, system requirements, and an overview of the Gateway's front and rear panels.
- **Chapter 2** - describes how to install the Gateway.
- **Chapter 3** - describes how to configure TCP/IP settings on the computer you will use to configure the Gateway.
- **Chapter 4** - describes how to configure the Gateway.
- **Appendix A** - contains compliance information.

Document Conventions

This document uses the following conventions to draw your attention to certain information.

Safety and Warnings

This document uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device.
	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

Typographic Conventions

This document also uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
<i>Italic</i>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
<code>screen/code</code>	Indicates text that is displayed on screen or entered by the user.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Italic font is also used to indicate variables.
[] square brackets	Indicates optional values.
{ } braces	Indicates required or expected values.
vertical bar	Indicates that you have a choice between two or more options or arguments.

1 Getting to Know the Gateway

Before you install the SMCD3GN3 Wireless Cable Modem Gateway, check the package contents and become familiar with the Gateway's front and back panels.

The topics covered in this chapter are:

- Unpacking Package Contents (page 11)
- System Requirements (page 11)
- Front Panel (page 12)
- Configuring Wireless Security (page 14)
- Rear Panel (page 14)
- Restoring Factory Defaults (page 15)

Unpacking Package Contents

The SMCD3GN3 package should include the following items:

- One SMCD3GN3 Wireless Cable Modem Gateway
- One power cord
- One Category 5E Ethernet cable
- One CD that contains this User Manual

System Requirements

To complete the installation, you will need the following items:

- Provisioned Internet access on a cable network that supports cable modem service
- A computer with a wired network adapter with TCP/IP installed
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.5 or above
- Microsoft® Windows® 2000 or higher for USB driver support

Front Panel

The front panel of the SMCD3GN3 Wireless Cable Modem Gateway contains a set of light-emitting diode (LED) indicators. These LEDs show the status of the Gateway and simplify troubleshooting. The front panel also contains a **WPS** button for configuring wireless security automatically.

Figure 1 shows the front panel of the SMCD3GN3 Wireless Cable Modem Gateway. Table 1 describes the front panel LEDs.



Figure 1. Front Panel of the SMCD3GN3 Wireless Cable Modem Gateway

Table 1. Front Panel LEDs

LED	Color	Description
POWER	Green	ON = power is supplied to the Gateway. OFF = power is not supplied to the Gateway.
DS	Green	Blinking = scanning for DS channel. ON = synchronized on 1 channel only.
	Blue	ON = synchronized with more than 1 channel (DS Bond mode).
DS and US		Both DS and US blinking together = operator is performing maintenance.
US	Green	Blinking = ranging is in progress. ON = ranging is complete on 1 channel only. OFF = scanning for DS channel.
	Blue	ON = ranging is complete, operate with more than 1 channel (US Bond mode).
ONLINE	Green	Blinking = cable interface is acquiring IP, ToD, CM configuration. ON = Gateway is operational. OFF = Gateway is offline.
ETH 1 – ETH 4	Green	Blinking = data is transmitting. ON = connected at 10 or 100 Mbps. OFF = no Ethernet link detected.
	Blue	Blinking = data is transmitting. ON = connected at 1 Gbps. OFF = no Ethernet link detected.
WIFI	Green	Blinking = data is transmitting. ON = Wi-Fi is enabled. OFF = Wi-Fi is disabled.
USB	Green	Reserved for future use.

Configuring Wireless Security

The front panel has a **WPS** button for configuring wireless security automatically. Pressing this button for 5 seconds automatically configures wireless security. If the client device supports WPS Push Button Configuration (PBC), press the button on the client within 60 seconds to automatically configure security on the client.

After pressing this button for 5 seconds, the **WPS** LED on the front panel flashes. When a client joins the network successfully, the LED remains ON until the next WPS action or the device reboots. If no client joins, the LED stops blinking after 4 minutes.

Rear Panel

The rear panel of the SMCD3GN3 Wireless Cable Modem Gateway contains a reset button and the ports for attaching the supplied power adapter and making additional connections. Figure 2 shows the rear panel components and Table 2 describes their meanings.



Figure 2. Rear View of the SMCD3GN3 Wireless Cable Modem Gateway

Table 2. SMCD3GN3 Wireless Cable Modem Gateway Rear Panel Components

	Item	Description
≡	USB	USB 2.0 high-speed port for storing configurations externally.
☒	ETH 1 - 4	Four 10/100/1000 auto-sensing RJ-45 switch ports. Connect devices on your local area network such as a computer, hub, or switch to these ports.
⊂	Reset button	Use this button to reset the power or restore the default factory settings (see "Restoring Factory Defaults," below). This button is recessed to prevent accidental resets of the Gateway.
⊂	Cable	Connect your coaxial cable line to this port.
⊂	Power	Connect the supplied power cord to this port.

Restoring Factory Defaults

The Reset button on the back panel can be used to return the Gateway to its factory default settings. As a result, any changes made to the Gateway's default settings will be lost.

If you do not have physical access to the Gateway, you can use the GUI to either power cycle the Gateway (see "Using the Reboot Menu to Reboot the Gateway" on page 137) or return the Gateway to its factory default settings (see "Restoring Factory Defaults" on page 136).

The following procedure describes how to use the Reset button to power cycle the Gateway and return it to its original factory default settings.

1. Leave power plugged into the Gateway.
2. Find the Reset button on the back panel, then press and hold it for at least 10 seconds.
3. Release the Reset button.

2 Installing the Gateway

This chapter describes how to install the SMCD3GN3 Wireless Cable Modem Gateway. The topics covered in this chapter are:

- Finding a Suitable Location (page 17)
- Connecting to the LAN (page 17)
- Connecting the WAN (page 18)
- Powering on the Gateway (page 18)

Finding a Suitable Location

The SMCD3GN3 Wireless Cable Modem Gateway can be installed in any location with access to the cable network. All of the cables connect to the rear panel of the Gateway for better organization and utility. The LED indicators on the front panel are easily visible to provide users with information about network activity and status.

For optimum performance, the location you choose should:

- Be close to a working AC power outlet
- Allow sufficient air flow around the Gateway to keep the device as cool as possible
- Not expose the Gateway to a dusty or wet environment
- Be an elevated location such as a high shelf, keeping the number of walls and ceilings between the Gateway and your other devices to a minimum
- Be away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone
- Be away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal

Connecting to the LAN

Using an Ethernet LAN cable, you can connect the Gateway to a desktop computer, notebook, hub, or switch. The SMCD3GN3 Wireless supports auto-MDI/MDIX, so you can use either a standard straight-through or crossover Ethernet cable.

1. Connect either end of an Ethernet cable to one of the four **ETH** ports on the rear panel of the Gateway (see Figure 3).

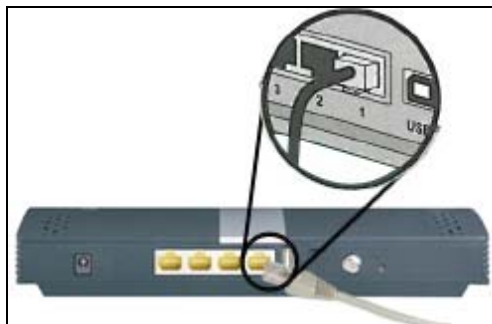


Figure 3. Connecting to an ETH Port on the Gateway Rear Panel

2. Connect the other end of the cable to your computer's network-interface card (NIC) or to another network device (see Figure 4).

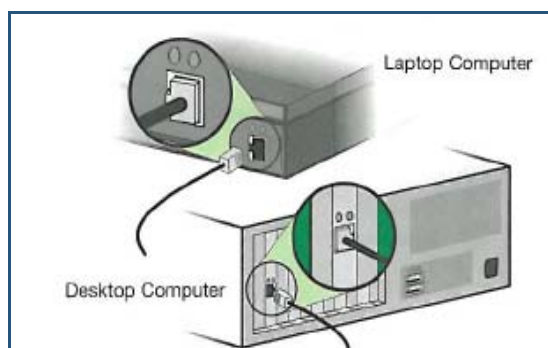


Figure 4. Connecting the Gateway to the a Laptop or Desktop Computer

Connecting the WAN

To connect the Gateway to a Wide Area Network (WAN) interface:

3. Connect a coaxial cable to the port labeled **Cable** on the rear panel of the Gateway from a cable port in your home or office (see Figure 2 on page 14). Use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.
4. Hand-tighten the connectors to secure the connection.

Powering on the Gateway

After making your LAN and WAN connections, use the following procedure to power on the Gateway:

1. Connect the supplied power cord to the port on the rear panel of the Gateway (see Figure 2 on page 14).
2. Connect the other end of the power cord to a working power outlet. The Gateway powers on automatically, the **POWER** LED on the front panel goes ON, and the other front panel LEDs show the Gateway's status (see Table 1 on page 13).



WARNING: Only use the power cord supplied with the Gateway. Using a different power cord can damage the Gateway and void the warranty.

3 Configuring Your Computer for TCP/IP

After you install the SMCD3GN3 Wireless Cable Modem Gateway, configure the TCP/IP settings on a computer that will be used to configure the Gateway. This chapter describes how to configure TCP/IP for various Microsoft Windows and Apple Macintosh operating systems.

The topics covered in this chapter are:

- Configuring Microsoft Windows 2000 (page 20)
- Configuring Microsoft Windows XP (page 21)
- Configuring Microsoft Windows Vista (page 22)
- Configuring Microsoft Windows 7 (page 24)
- Configuring an Apple[®] Macintosh[®] Computer (page 26)

Configuring Microsoft Windows 2000

Use the following procedure to configure your computer if your computer has Microsoft Windows 2000 installed.

1. On the Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double-click the **Network and Dial-up Connections** icon. If the Ethernet adapter in your computer is installed correctly, the **Local Area Connection** icon appears.
3. Double-click the **Local Area Connection** icon for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears (see Figure 5).

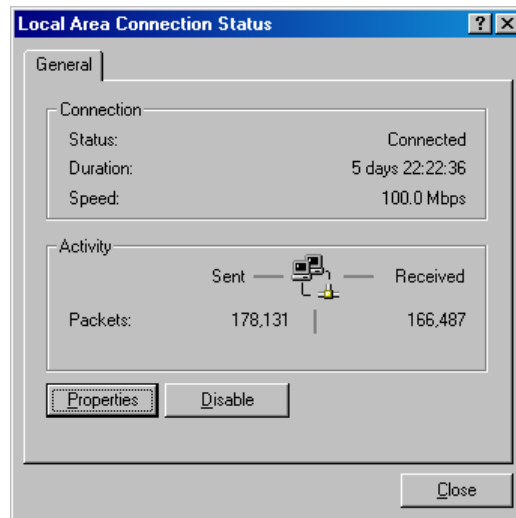


Figure 5. Local Area Connection Status Window

4. In the Local Area Connection Status dialog box, click the **Properties** button. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button.
6. Click **Obtain an IP address automatically** to configure your computer for DHCP.
7. Click the **OK** button to save this change and close the Local Area Connection Properties dialog box.
8. Click **OK** button again to save these new changes.
9. Restart your computer.

Configuring Microsoft Windows XP

Use the following procedure to configure a computer running Microsoft Windows XP with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 20.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then click **Network and Internet Connections**.
2. Click the **Network Connections** icon.
3. Click **Local Area Connection** for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears.
4. In the Local Area Connection Status dialog box, click the **Properties** button (see Figure 6). The Local Area Connection Properties dialog box appears.

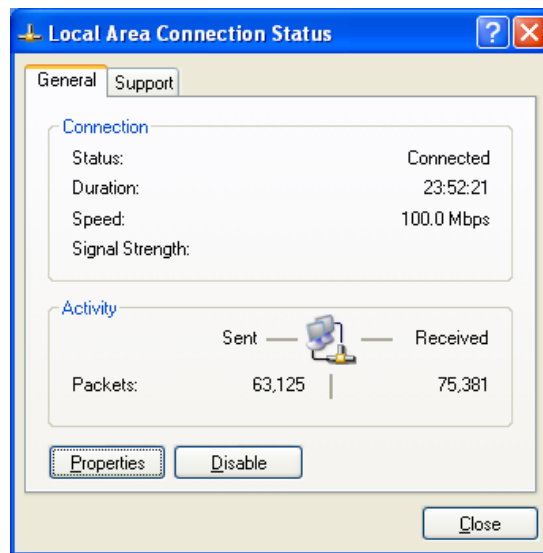


Figure 6. Local Area Connection Status Window

5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button. The Internet Protocol (TCP/IP) Properties dialog box appears.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP. Click the **OK** button to save this change and close the Internet Protocol (TCP/IP) Properties dialog box.
7. Click the **OK** button again to save your changes.
8. Restart your computer.

Configuring Microsoft Windows Vista

Use the following procedure to configure a computer running Microsoft Windows Vista with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000” on page 20.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then select the **Network and Internet** icon.
2. Click **View Networks Status and tasks** and then click **Management Networks Connections**.
3. Right-click the **Local Area Connection** icon and click **Properties**.
4. Click **Continue**. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IPv4)** is checked. Then select **Internet Protocol (TCP/IPv4)** and click the **Properties** button (see Figure 7). The Internet Protocol Version 4 Properties dialog box appears.

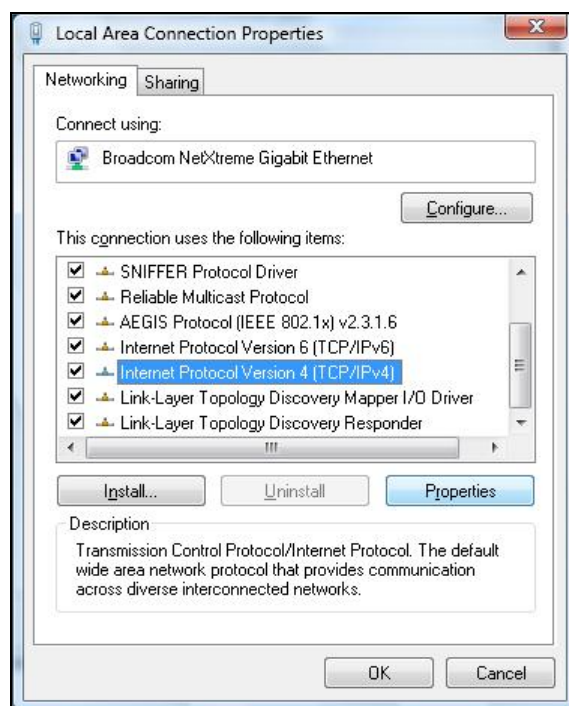


Figure 7. Local Area Connection Properties Window

6. In the Internet Protocol Version 4 Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 8).

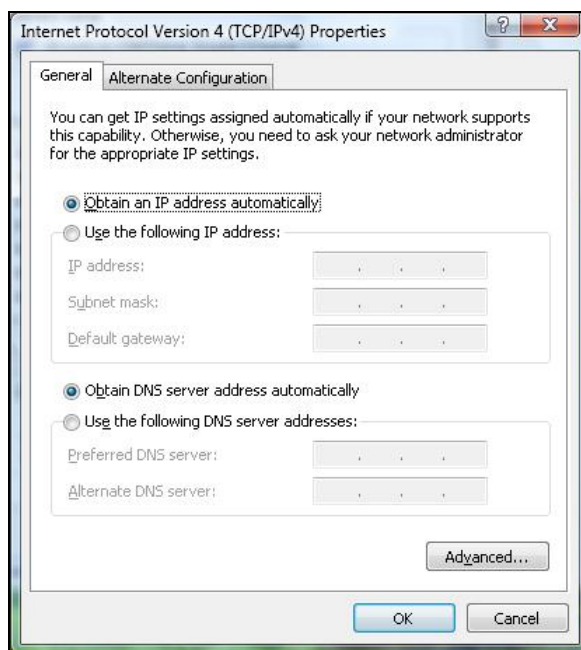


Figure 8. Internet Protocol Properties Window

7. Click the **OK** button to save your changes and close the dialog box.
8. Click the **OK** button again to save your changes.

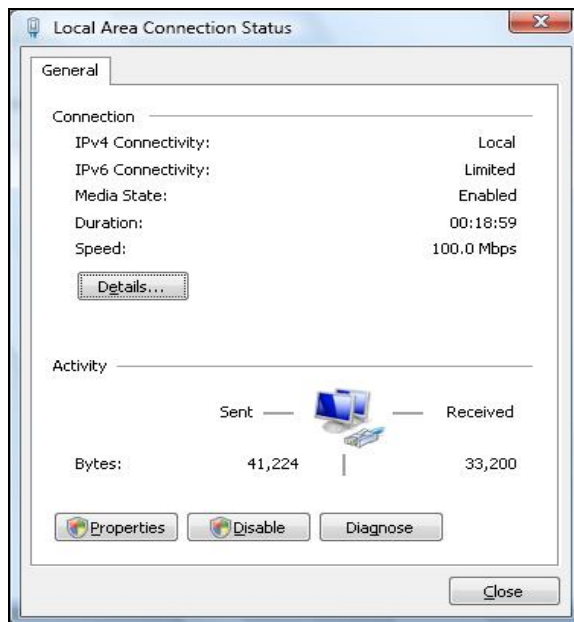


Figure 9. Local Area Connection Status Window

Configuring Microsoft Windows 7

Use the following procedure to configure a computer running Microsoft Windows 7.

1. In the Start menu search box, type: **ncpa.cpl**

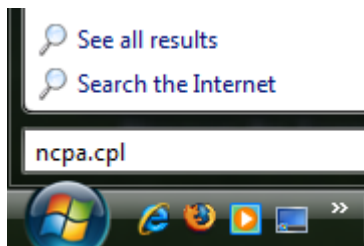


Figure 10. Typing ncpa.cpl in the Start Menu Box

The Network Connections List appears.

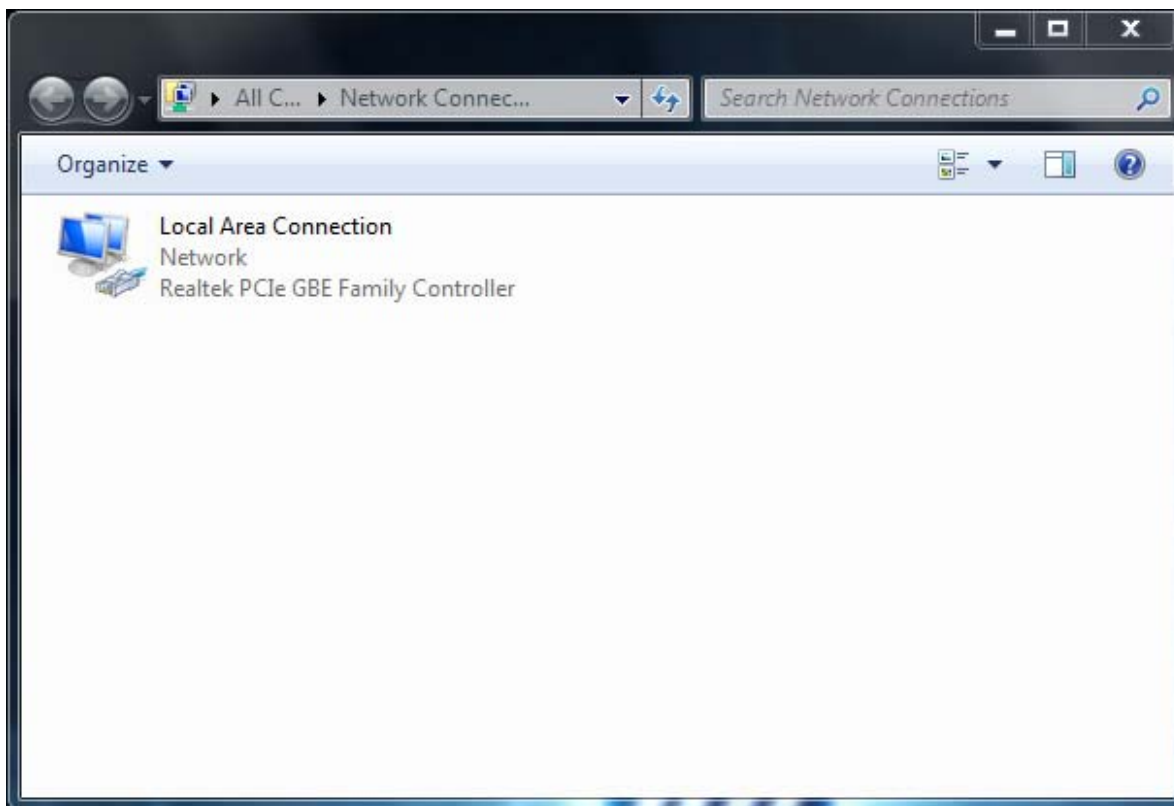


Figure 11. Example of Network Connections List

2. Right-click the **Local Area Connection** icon and click **Properties**.
3. In the **Networking** tab, click either **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.

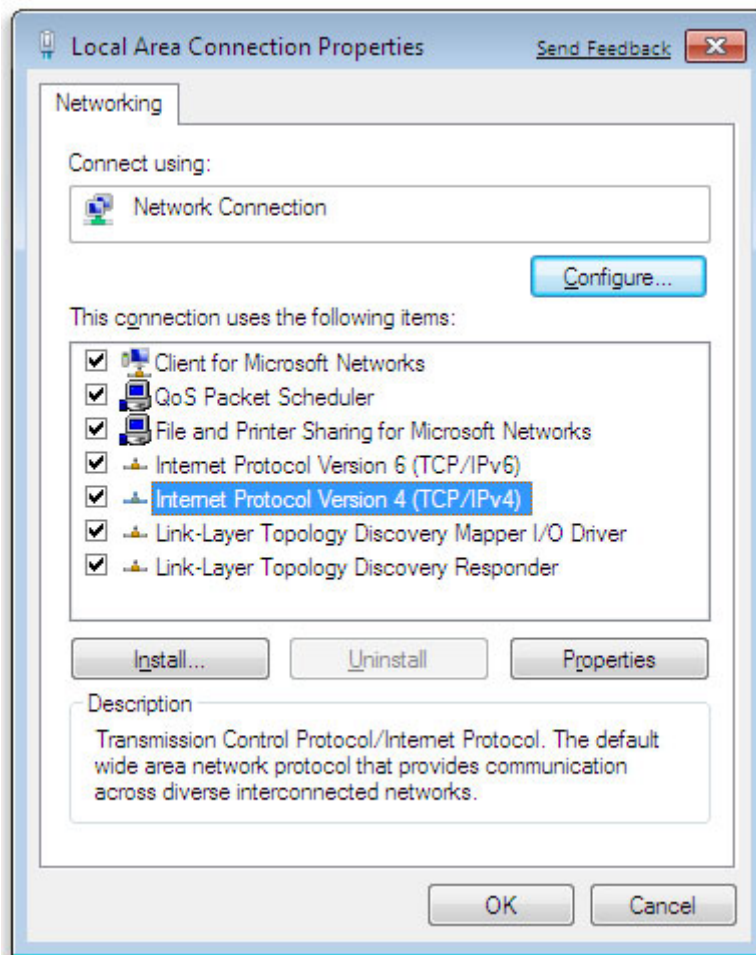


Figure 12. Local Area Network Connection Properties Dialog Box

4. In the properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 13).

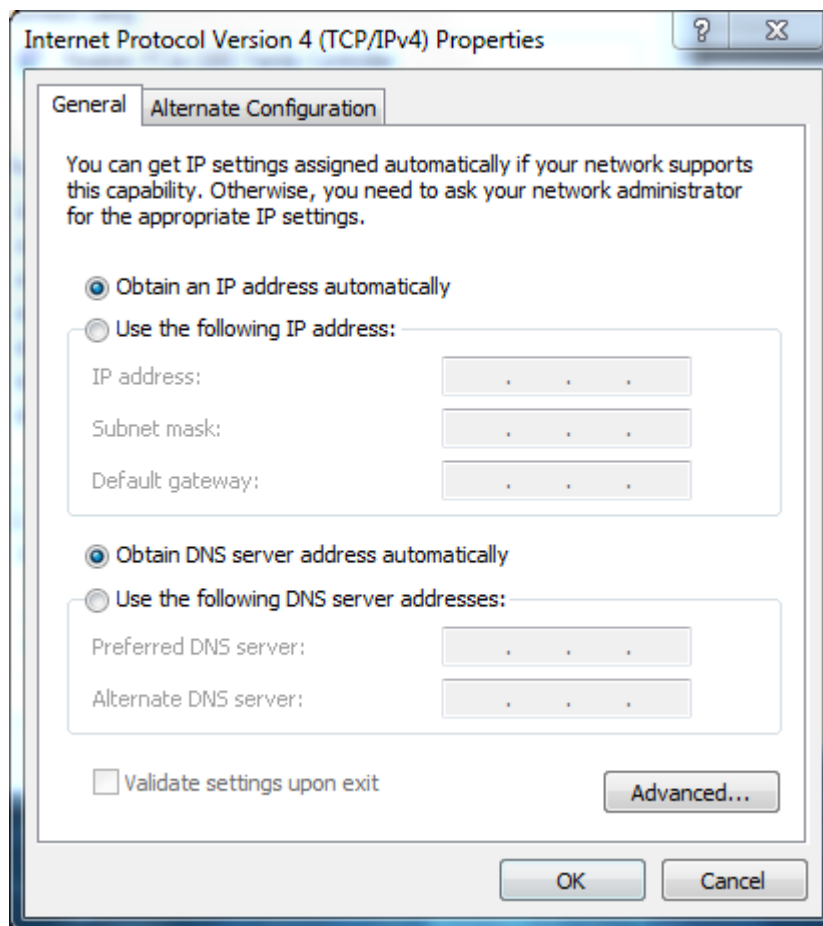


Figure 13. Properties Window

5. Click the **OK** button to save your changes and close the dialog box.
6. Click the **OK** button again to save your changes.

Configuring an Apple® Macintosh® Computer

The following procedure describes how to configure TCP/IP on an Apple Macintosh running Mac OS 10.2. If your Apple Macintosh is running Mac OS 7.x or later, the steps you perform and the screens you see may differ slightly from the following. However, you should still be able to use this procedure as a guide to configuring your Apple Macintosh for TCP/IP.

- a. Pull down the Apple Menu, click **System Preferences**, and select **Network**.

7. Verify that the NIC connected to the SMCD3GN3 is selected in the **Show** field.
8. In the **Configure** field on the **TCP/IP** tab, select **Using DHCP** (see Figure 14).
9. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.

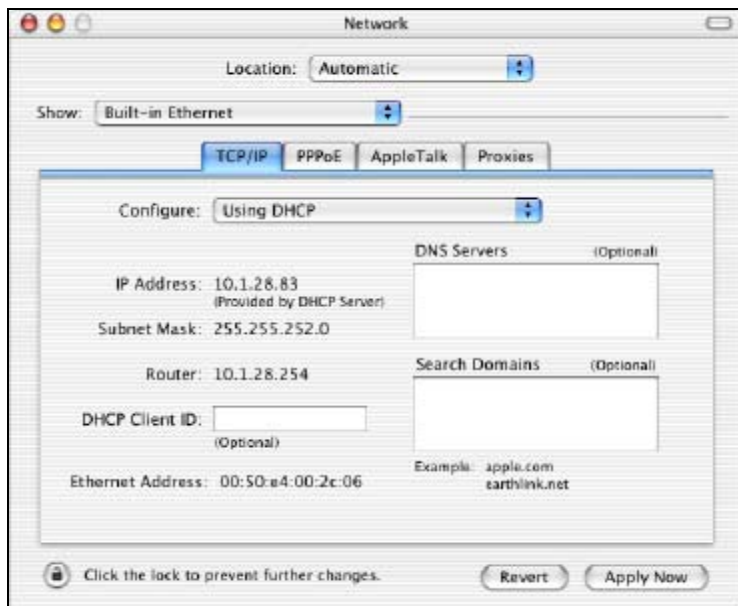


Figure 14. Selecting Using DHCP in the Configure Field

4 Configuring the Gateway

This chapter describes how to use a Web browser to configure the Gateway.

The topics covered in this chapter are:

- Pre-configuration Guidelines (page 29)
- Accessing the Gateway's Web Management (page 31)
- Understanding the Web Management Interface Screens (page 32)
- Web Management Interface Menus (page 33)

Pre-configuration Guidelines

Before you configure the Gateway, observe the guidelines in the following sections.

Disabling Proxy Settings

Disable proxy settings in your Web browser. Otherwise, you will not be able to view the Gateway's Web-based configuration pages.

Disabling Proxy Settings in Internet Explorer

The following procedure describes how to disable proxy settings in Internet Explorer 5 and later.

1. Start Internet Explorer.
2. On your browser's **Tool** menu, click **Options**. The Internet Options dialog box appears.
3. In the Internet Options dialog box, click the **Connections** tab.
4. In the **Connections** tab, click the **LAN settings** button. The Local Area Network (LAN) Settings dialog box appears.
5. In the Local Area Network (LAN) Settings dialog box, uncheck all check boxes.
6. Click **OK** until the Internet Options window appears.
7. In the Internet Options window, under **Temporary Internet Files**, click **Settings**.
8. For the option **Check for newer versions of stored pages**, select **Every time I visit the webpage**.
9. Click **OK** until you close all open browser dialog boxes.

Disabling Proxy Settings in Firefox

The following procedure describes how to disable proxy settings in Firefox.

1. Start Firefox.
2. On your browser's **Tools** menu, click **Options**. The Options dialog box appears.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Network** tab.
5. Click the **Settings** button.
6. Click **Direct connection to the Internet**.
7. Click the **OK** button to confirm this change.

Disabling Proxy Settings in Safari

The following procedure describes how to disable proxy settings in Safari.

1. Start Safari.
2. Click the **Safari** menu and select **Preferences**.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Change Settings** button.
5. Choose your location from the **Location** list (this is generally **Automatic**).
6. Select your connection method. If using a wired connection, select **Built-in Ethernet**. For wireless, select **Airport**.
7. Click the **Proxies** tab.
8. Be sure each proxy in the list is unchecked.
9. Click **Apply Now** to finish.

Disabling Firewall and Security Software

Disable any firewall or security software that may be running on your computer. For more information, refer to the documentation for your firewall.

Accessing the Gateway's Web Management

After configuring your computer for TCP/IP and performing the preconfiguration guidelines on the previous page, you can now easily configure the Gateway from the convenient Web-based management interface. From your Web browser (Microsoft Internet Explorer version 5.5 or later), you will log in to the interface to define system parameters, change password settings, view status windows to monitor network conditions, and control the Gateway and its ports.

To access the SMCD3GN3 Wireless Cable Modem Gateway's web-based management screens, use the following procedure.

1. Launch a Web browser.



Note: The cable modem does not have to be online to configure the Gateway.

2. In the browser address bar, type <http://192.168.0.1> and press the Enter key. For example:



The Login User Password screen appears (see Figure 15)

LOGIN USER PASSWORD

Login Screen

Username:

Password:

LOGIN CANCEL

Figure 15. Login User Password Screen

3. In the Login User Password screen, enter the default administrator username and the default administrator password provided by SMC Networks. Both the username and password are case sensitive.
4. Click the **Login** button to access the Gateway. The Status page appears, showing connection status information about the Gateway.

Understanding the Web Management Interface Screens

The left side of the management interface contains a menu bar you use to select menus for configuring the Gateway. When you click a menu, information and any configuration settings associated with the menu appear in the main area of the interface (see Figure 16). If the displayed information exceeds what can be shown in the main area, scroll bars appear to the right of the main area so you can scroll up and down through the information.

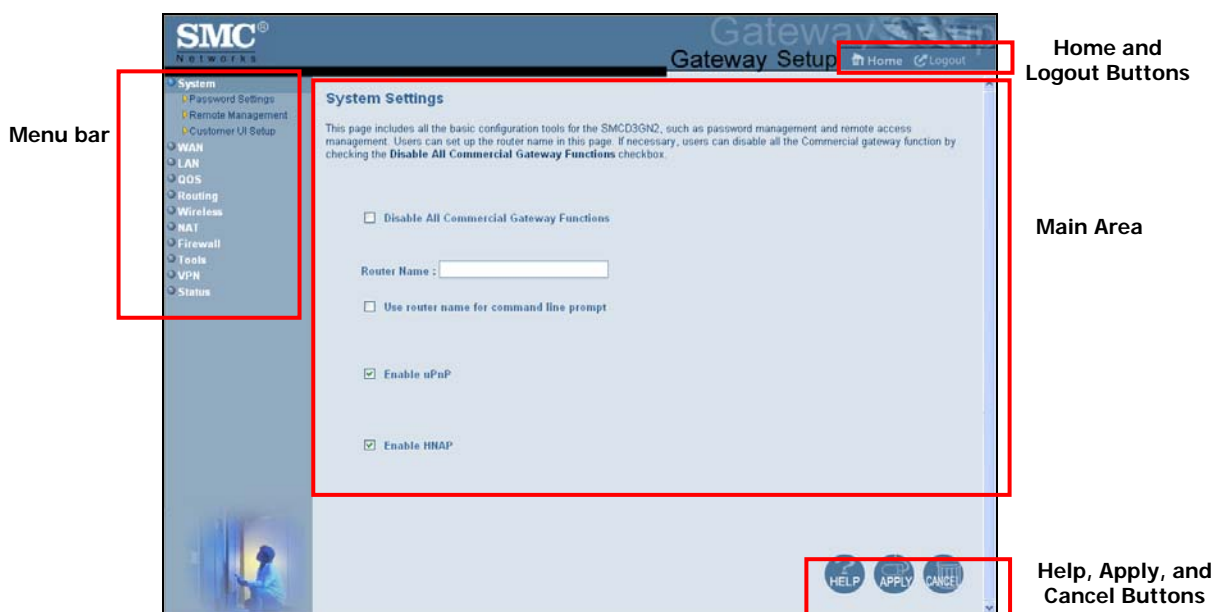


Figure 16. Main Areas on the Web Management Interface

Some menus have submenus associated with them. If you click a menu that has submenus, the submenus appear below the menu. For example, if you click the **System** menu, the submenus **Password Settings**, **Remote Management**, and **Customer UI Setup** appear below the **System** menu (see Figure 17).

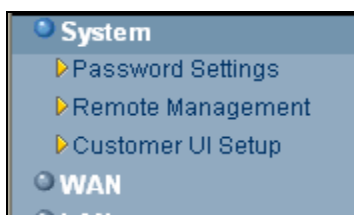


Figure 17. Example of System Submenus

The top-right side of the page contains a **Home** button that displays the Home (Status) page and a **Logout** button for logging out of the Web management interface.

The bottom right side of the screen contains three buttons:

- **Help** displays online help
- **Apply** click this button to save your configuration changes to the displayed page
- **Cancel** click this button to discard any configuration changes made to the current page

Web Management Interface Menus and Submenus

Table 3 describes the menus and submenus in the Web management interface.



Note: Some menus and submenus described in this chapter may not apply to your Gateway. Please check your Gateway's GUI to see which menus and submenus are available.

Table 3. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
System	Lets you disable all commercial Gateway functions, define a router name, use the router name at command prompts, and enable or disable UPnP and HNAP. Submenus let you:	36
System > Password Settings	<ul style="list-style-type: none"> • Define user and admin password settings, RADIUS authentication, TACACS+ authentication, and TACACS authentication. 	38
System > Remote Management	<ul style="list-style-type: none"> • Allow users to manage the Gateway remotely using the Gateway's Web interface and/or Telnet, and enable or disable remote management of the Gateway's administrator interface. 	43
System > Customer UI Setup	<ul style="list-style-type: none"> • Select which configuration options on the Gateway's user configuration menus are shown to or hidden from users. 	44
WAN	Lets you configure Wide Area Network (WAN) and Media Access Channel (MAC) spoofing settings. The submenu lets you:	46
WAN > MAC Spoofing	<ul style="list-style-type: none"> • Clone ("spoof") the Gateway's MAC address if necessary. 	49
LAN	Lets you configure settings for your public and private LAN, auto-negotiation, and duplex mode. The submenu lets you:	50
LAN > Ether Switch Control	<ul style="list-style-type: none"> • Specify fixed speed and duplex settings, and disable individual LAN ports. 	53
LAN > Ether Access Control	<ul style="list-style-type: none"> • Allow all EtherLAN client stations to access the Internet through the Gateway, allow certain trusted EtherLAN client stations to access the Internet through the Gateway, or deny certain trusted EtherLAN client stations from accessing the Internet through the Gateway. 	54
LAN > Additional Public LAN	<ul style="list-style-type: none"> • Add more than one public subnet, except for 20.20.1, to the LAN interface. 	58
LAN > Public LAN IP Access Control	<ul style="list-style-type: none"> • Block specific public IP addresses from accessing the Internet. 	60
QoS	Lets you configure Quality of Service (QoS) settings. If you enable QoS, the following submenus become available for:	62
QoS > Port	<ul style="list-style-type: none"> • Prioritizing performance of the four Gateway LAN ports. 	64

QoS > COS	<ul style="list-style-type: none"> Defining four queues to which the Class of Service (CoS) is mapped. 	65
QoS > DSCP	<ul style="list-style-type: none"> Defining the QoS class queue to which the customized DSCP is mapped. 	67
QoS > Queue	<ul style="list-style-type: none"> Specifying whether QoS behavior runs with strict or weighted priority. 	69
QoS > DSCP Remarking	<ul style="list-style-type: none"> Defining the DSCP remarking action and mode. 	71
Routing	Lets you set up routing tables manually and automatically using the Routing Information Protocol (RIP). Submenus let you:	73
Routing > Static Routes	<ul style="list-style-type: none"> Add static routes manually. 	73
Routing > RIP Control	<ul style="list-style-type: none"> Configure how the Gateway adjusts to physical changes in the network's layout and exchange routing tables with other routers. 	75
Routing > OSPF Control	<ul style="list-style-type: none"> Control how the Gateway uses the Open Shortest Path First (OSPF) protocol. 	79
Wireless	Lets you configure basic wireless settings, such as enabling or disabling wireless operation, selecting wireless mode, and configuring the Service Set Identifier (SSID) and channel settings. Submenus let you:	83
Wireless > Encryption	<ul style="list-style-type: none"> Use encryption to protect the data transmitted across your wireless network 	85
Wireless > WPS	<ul style="list-style-type: none"> Enable or disable Wi-Fi Protected Setup (WPS). 	88
Wireless > MAC Filtering	<ul style="list-style-type: none"> Allow all wireless client stations or only trusted PCs to connect over a wireless connection. 	91
Wireless > Advanced Settings	<ul style="list-style-type: none"> Configure advanced wireless settings for the Gateway. 	93

NAT	Allows multiple users at your local site to access the Internet using a single public IP address. The submenus let you:	
NAT > Port Forwarding	<ul style="list-style-type: none"> Configure predefined and custom port forwarding settings to let Internet users access local services such as the Web Server or FTP server at your local site. 	95
NAT > 1-to-1 Mapping	<ul style="list-style-type: none"> Perform 1-to-1 mapping between global IP addresses on the cable modem WAN interface and the private IP address on the LAN. 	102
Firewall	Lets you enable or disable the Gateway's firewall. Submenus let you:	105
Firewall > Access Control	<ul style="list-style-type: none"> Block traffic at the Gateway's LAN interfaces from accessing the Internet. 	107
Firewall > Special Application	<ul style="list-style-type: none"> Detect port triggers for detect multiple-session applications and allow them to pass the firewall. 	108
Firewall > URL Blocking	<ul style="list-style-type: none"> Block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. 	122
Firewall > Schedule Rule	<ul style="list-style-type: none"> Define schedule rules that work with the Gateway's URL blocking feature. 	124
Firewall > Email/Syslog Alert	<ul style="list-style-type: none"> Send email notifications or add entries to the syslog when traffic is blocked, attempts are made to intrude onto the network, and local computers try to access block URLs. 	125
Firewall > DMZ	<ul style="list-style-type: none"> Configure a local client computer for unrestricted two-way Internet access by defining it as a Virtual DMZ host. 	129
Tools	Provides the following submenus with utilities for performing the following activities:	
Tools > Configuration Tools	Back up and restore Gateway configuration settings locally and remotely over the WAN, and restore Gateway factory default settings.	130
Tools > Reboot	Reboot the Gateway.	137
Tools > Diagnostics	Perform trace route and ping diagnostic operations.	138
Tools > SNTP Client	Configure the Gateway to act as a SNTP client.	144
VPN	Lets you enable or disable the Gateway's VPN functions. When VPN functions are enabled, submenus let you:	145
VPN > Access Control	<ul style="list-style-type: none"> Allow PC clients behind the Gateway to access the IPSec VPN tunnel. 	147
VPN > IPsec Tunnel Configuration	<ul style="list-style-type: none"> Define up to five tunnels and view, clear, refresh, and save the VPN log. 	148
VPN > PPTP/L2TP Configuration	<ul style="list-style-type: none"> Set up to 50 Point-to-Point Tunneling Protocol (PPTP) / Layer Two Tunneling Protocol (L2TP) user accounts and define a pre-shared phrase. 	153
Status	Shows the connection status of the Gateway interfaces, firmware, hardware version numbers, illegal attempts to access your network, and information about DHCP client PCs current connected to the Gateway. The submenu lets you:	156
Status > Cable Status	<ul style="list-style-type: none"> View cable initialization procedures, and cable downstream and upstream status. 	158

System Settings Menu

The System Settings menu lets you:

- Enable or disable all commercial Gateway functions
- Define the Gateway's name and enable it for command line prompt
- Enable or disable UPnP and HNAP

To access the System Settings menu, click **System** in the menu bar. Figure 18 shows an example of the menu and Table 4 describes the setting you can select.

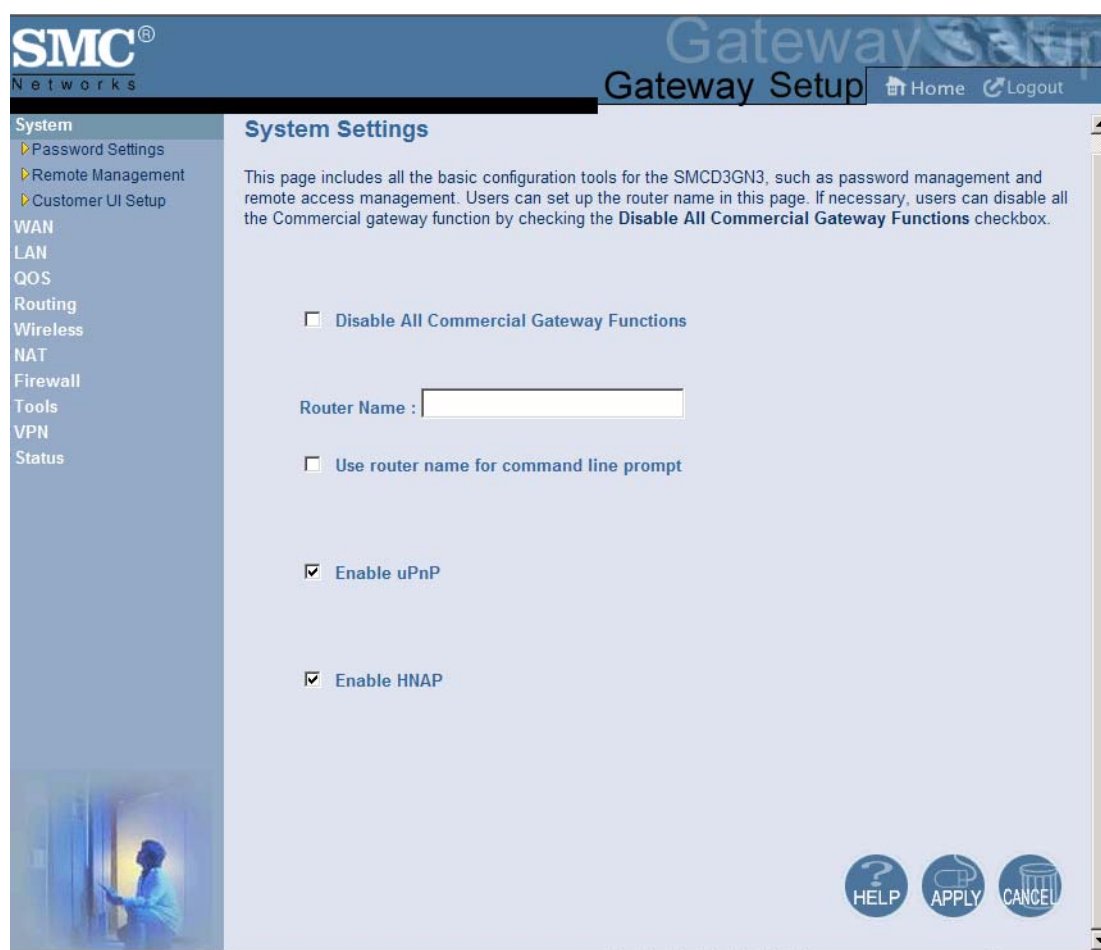


Figure 18. System Settings Menu

Table 4. System Settings Menu Option

Option	Description
Disable All Commercial Gateway Functions	<p>Enables or disables all commercial Gateway functions.</p> <ul style="list-style-type: none"> • Checked = all commercial Gateway functions are disabled. • Unchecked = all commercial Gateway functions are enabled. (<i>default</i>)
Router Name	<p>The name you want to assign to the Gateway. Assign a name so that this device will not be confused with other devices on your wireless network. We recommend you use a name that is meaningful to you so you can identify the Gateway easily.</p>
Use router name for command line prompt	<p>Determines whether the router name you specified appears in DOS command line prompts (for example, if you Telnet into the Gateway).</p> <ul style="list-style-type: none"> • Checked = router name appears in command line prompts. • Unchecked = router name does not appear in command line prompts. (<i>default</i>)
Enable UPnP	<p>Configures the Gateway as a Universal Plug and Play (UPnP) Internet gateway. UPnP allows for dynamic connectivity between devices on a network. A UPnP-enabled device like the Gateway can obtain an IP address, advertise its capabilities, learn about other connected UPnP devices and then communicate directly with those devices. The same device can end its connection cleanly when it wishes to leave the UPnP community. The intent of UPnP is to support zero-configuration, "invisible" networking of devices including intelligent appliances, PCs, printers, and other smart devices using standard protocols.</p> <ul style="list-style-type: none"> • Checked = UPnP is enabled on the Gateway. (<i>default</i>) • Unchecked = UPnP is disabled on the Gateway.
Enable HNAP	<p>Configures the Gateway as a Home Network Administration Protocol (HNAP) device. HNAP allows the Gateway to be configured and managed by remote entities, such as Network Magic or any software application that discovers and manages network devices.</p> <ul style="list-style-type: none"> • Checked = HNAP is enabled on the Gateway. • Unchecked = HNAP is disabled on the Gateway. (<i>default</i>)

Password Settings Menu


The Password Settings menu lets you change the Gateway's default administrator username and password and the user's password.

The Password Settings menu also lets you change the number of minutes of inactivity that can occur before your Web management session times out automatically. The default setting is 10 minutes.

In addition, you can configure Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access-Control System Plus (TACACS+), and Terminal Access Controller Access-Control System (TACACS) configuration settings.

- RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service
- TACACS is a remote authentication protocol used to communicate with an authentication server commonly used in UNIX networks. TACACS lets a remote access server communicate with an authentication server determine whether the user has access to the network.
- TACACS+ is a Cisco-proprietary protocol that provides access control for the Gateway and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services.

To access the Password Settings menu, click **System** in the menu bar and then click the **Password Settings** submenu. Figure 19 shows an example of the menu and Table 5 describes the settings you can select.



Gateway Setup
Home
Logout

- System
 - ▶ Password Settings
 - ▶ Remote Management
 - ▶ Customer UI Setup
- WAN
- LAN
- QOS
- Routing
- Wireless
- NAT
- Firewall
- Tools
- VPN
- Status

Password Settings

Set a password to restrict management access to the SMCD3GN3. Also a timeout value could be set here for automatic logout if the page is not active for the timeout period.

- Current Password :
- MSO Username :
- New Password :
- Re-Enter Password for Verification :
- Customer New Password :
- Re-Enter Customer New Password for Verification :
- Commercial New Password :
- Re-Enter Commercial New Password for Verification :

• Idle Time Out : Min

RADIUS Authentication

Timeout	<input type="text" value="3"/>	seconds
Retry	<input type="text" value="3"/>	times

Primary

RADIUS Server IP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Port	<input type="text" value="1812"/>			
Authentication Algorithm	<input type="text" value="CHAP"/>			
Key	<input type="text" value="*****"/>			

Secondary

RADIUS Server IP	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Port	<input type="text" value="1812"/>			
Authentication Algorithm	<input type="text" value="CHAP"/>			
Key	<input type="text" value="*****"/>			

The screenshot displays a configuration interface for password settings. It is divided into two main sections: TACACS+ Authentication and TACACS Authentication. Each section has a checkbox at the top and is further divided into Primary and Secondary settings. The TACACS+ section uses IP addresses and ASCII algorithms, while the TACACS section uses server IP, authentication algorithms, and line styles. At the bottom right, there are three circular buttons: HELP, APPLY, and CANCEL. A small image of a person in a white lab coat is visible in the bottom left corner of the window.

TACACS+ Authentication	
Primary	
TACACS+ Server IP	0 0 0 0
Port	49
Authentication Algorithm	ASCII
Shared Secret	•••••
Secondary	
TACACS+ Server IP	0 0 0 0
Port	49
Authentication Algorithm	ASCII
Shared Secret	•••••

TACACS Authentication	
Primary	
TACACS Server IP	0 0 0 0
Port	49
Authentication Algorithm	Authentication
Line	1
Style	
Secondary	
TACACS Server IP	0 0 0 0
Port	49
Authentication Algorithm	Authentication
Line	1
Style	

Figure 19. Password Settings Menu

Table 5. Password Settings Menu Options

Option	Description
Current Password	Enter the current case-sensitive administrator password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes.
MSO Username	Enter the current new case-sensitive administrator username.
New Password	Enter the new case-sensitive administrator password you want to use. A password can contain up to 32 alphanumeric characters. Spaces count as password characters. For security purposes, every typed character appears as a dot (•).
Re-Enter Password for Verification	Enter the same case-sensitive administrator password you typed in the New Password field. For security purposes, every typed character appears as a dot (•).
Commercial New Password	Enter the new case-sensitive password your commercial users will use to log in to the Gateway Web management interface. A password can contain up to 32 alphanumeric characters. Spaces count as password characters. For security purposes, every typed character appears as a dot (•). If you leave this field blank, the default user password will be password .
Re-Enter Commercial New Password for Verification	Enter the same case-sensitive user password you typed in the Commercial New Password field. For security purposes, every typed character appears as a dot (•).
Customer New Password	Enter the new case-sensitive password your customers will use to log in to the Gateway Web management interface. A password can contain up to 32 alphanumeric characters. Spaces count as password characters. For security purposes, every typed character appears as a dot (•). If you leave this field blank, the default user password will be password .
Re-Enter Customer New Password for Verification	Enter the same case-sensitive user password you typed in the Customer New Password field. For security purposes, every typed character appears as a dot (•).
Idle Time Out	Your Web management interface sessions timeout after 10 minutes of idle time. To change this duration, enter a new timeout value.
RADIUS Authentication	To enable RADIUS authentication, check this box and then select the options for the primary and secondary authentication servers.
Timeout	Amount of time the Gateway waits for a response from the RADIUS servers before it tries to connect to the RADIUS servers again. Default is 3 seconds.
Retry	Maximum number of connection attempts the Gateway makes to connect to the RADIUS servers before giving up. Default is 3.
Primary/Secondary	For the primary and secondary authentication servers, enter the: <ul style="list-style-type: none"> • IP address of the RADIUS servers. • Port number that RADIUS uses for authentication. Default is 1812. • Authentication algorithm used for authentication. Choices are CHAP, MS-CHAP, and MS-CHAPv2. Default is CHAP. • Secret shared between the Gateway and RADIUS servers. For security purposes, every typed character appears as a dot (•).

Option	Description
TACACS+ Authentication	<p>To enable TACACS+ authentication, check this box and then select the options for the primary and secondary authentication servers:</p> <ul style="list-style-type: none">• IP address of the TACACS+ servers.• Port number that TACACS+ uses for authentication. Default is 49.• Authentication algorithm used for authentication. Choices are ASCII, PAP, and CHAP. Default is ASCII for the primary server and ASCII for the secondary server.• Secret shared between the Gateway and TACACS+ servers. For security purposes, every typed character appears as a dot (•).
TACACS Authentication	<p>To enable TACACS authentication, check this box and then select the options for the primary and secondary authentication servers:</p> <ul style="list-style-type: none">• IP address of the TACACS+ servers.• Port number that TACACS uses for authentication. Default is 49.• Authentication algorithm used for authentication. Choices are Authentication and Login. Default is Authentication.• Line the request is for. Default is 1.• Style of authentication to be performed.

Remote Management Menu

Administrative users can use the Gateway's Web-based management or Telnet to manage the device remotely using the public Internet.

- To use Web-based management, users specify the WAN IP address and remote management port in the URL entered in the Browser's address field
- For Telnet, users specify the WAN IP address and the remote Telnet management port

Using the Remote Management menu, you can enable HTTP, Telnet, HTTPS, and SSH and specify the port numbers for each of these settings. You can also limit remote management to specific IP addresses.

To access the Remote Management menu, click **System** in the menu bar and then click the **Remote Management** submenu in the menu bar. Figure 20 shows an example of the menu and Table 6 describes the settings you can select.

The SMC Gateway Setup interface shows the following settings for Remote Management:

WAN IP Address	10.30.20.229		
Http Port	8080		<input type="checkbox"/>
Telnet Port	2323		<input checked="" type="checkbox"/>
Https Port	8181		<input type="checkbox"/>
SSH Port	2222		<input type="checkbox"/>
Mso remote management	<input checked="" type="checkbox"/>		
Customer remote management	<input type="checkbox"/>		

Limit remote management to:

All IP Addresses

Single Address: [] [] [] [] to [] [] [] [] Add

Permitted IP Addresses:

Delete

HELP APPLY CANCEL

Figure 20. Remote Management Menu

Table 6. Remote Management Settings Menu Options

Option	Description
WAN IP Address	IP address used to access the Gateway's Web management interface via the Internet. For example, if the WAN IP address is 123.45.67.8 and the Web management port is 8080, remote users type http://123.45.67.8:8080 to access the Web management interface. To change the value shown, check the box to the right of this option and enter a new value.
Http Port	Port number used to access the Gateway's Web management interface. Range is from 1024 to 65535. Default is 8080. To change the value shown, check the box to the right of this option and enter a new value.
Telnet Port	Port number used to Telnet into the Gateway. Range is from 1 to 65535. Default is 2323. To change the value shown, check the box to the right of this option and enter a new value.
Https Port	Port number used to access the Gateway via a secure HTTPS connection. Default is 8181. To change the value shown, check the box to the right of this option and enter a new value.
SSH Port	Port number used to access the Gateway via a Secure Sockets Shell (SSH) connection. Default is 2222. To change the value shown, check the box to the right of this option and enter a new value.
Mso remote management	Enables or disables remote access to administrator configuration options. <ul style="list-style-type: none"> • Checked = administrator remote management is enabled. (<i>default</i>) • Unchecked = administrator remote management is disabled.
Customer remote management	Enables or disables remote access to user configuration options. <ul style="list-style-type: none"> • Checked = user remote management is enabled. • Unchecked = user remote management is disabled. (<i>default</i>)
Limit remote management to	By default, enabling remote management makes the device available to all IP addresses. To limit remote management to a subset of IP addresses, uncheck All IP addresses , select Single Address or Address Range from the drop-down list, enter the IP address or address range in the fields, and click Add . The IP addresses appear in Permitted IP Addresses . To delete an IP address or address range, click the address in Permitted IP Addresses and click Delete . No precautionary message appears before you delete an IP address.

Customer UI Setup Menu

The Customer UI Setup menu lets you select which menus, submenus, and configuration options are shown to **(Enable)** or hidden from **(Disable)** users. Using this menu, for example, you can hide options that, if changed by users, could adversely affect the Gateway. These settings do not affect the configuration options displayed for administrators. A **Reset to Defaults** button at the bottom-left side of the menu lets you return the parameters on this menu to their factory default settings.

To access the Customer UI Setup menu, click **System** in the menu bar and then click the **Customer UI Setup** submenu in the menu bar. Figure 21 shows an example of the menu.

Item	comadmin		cusadmin	
	Enable	Disable	Enable	Disable
System Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Disable All Commercial Gateway Functions	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Router Name Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
UPnP Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
HWAP Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Password Settings Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Idle Time Out Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Customer Password Change Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
LAN Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Private LAN IP Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Private Domain Name Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
DHCP Server Enable Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
DHCP Lease Time Setting	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Enable Manual DNS Assign Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
DNS Assign Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Private IP Address Pool Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
PPTP IP Address Pool Setting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Ether Switch Control Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Ether Access Control Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
QoS Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cos Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
DSCP Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Queue Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Routing Page	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Static Routes Sub-Page	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Wireless Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Wireless ON/OFF	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Wireless Mode	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SSID Settings	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Wireless Channel	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encryption Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
WPS Sub-Page	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Wireless MAC Filtering Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Wireless Advanced Settings Sub-Page	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
NAT Page	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Enable NAT Module setting	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port Forwarding Sub-Page	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Predefined Service Table	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Customer Defined Service Table	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

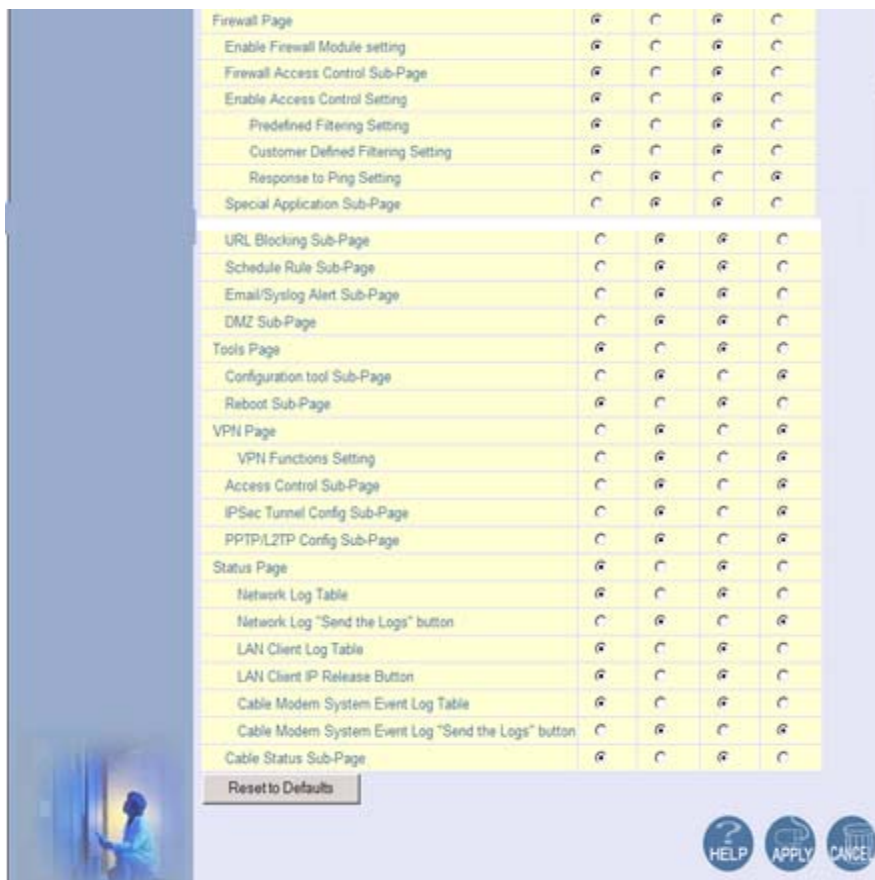


Figure 21. Customer UI Setup Menu

WAN Settings Menu

The Gateway can connect to the cable service provider using either a static IP address or an IP address automatically assigned by a Dynamic Host Configuration protocol (DHCP) server. Using the WAN Settings menu, you can assign your own static WAN IP and DNS addresses to the Gateway. By default, both options are disabled, allowing the Gateway to obtain these settings automatically from a DHCP server.

To access the WAN Settings menu, click **WAN** in the menu bar. Figure 22 shows an example of the menu and Table 7 describes the settings you can select.

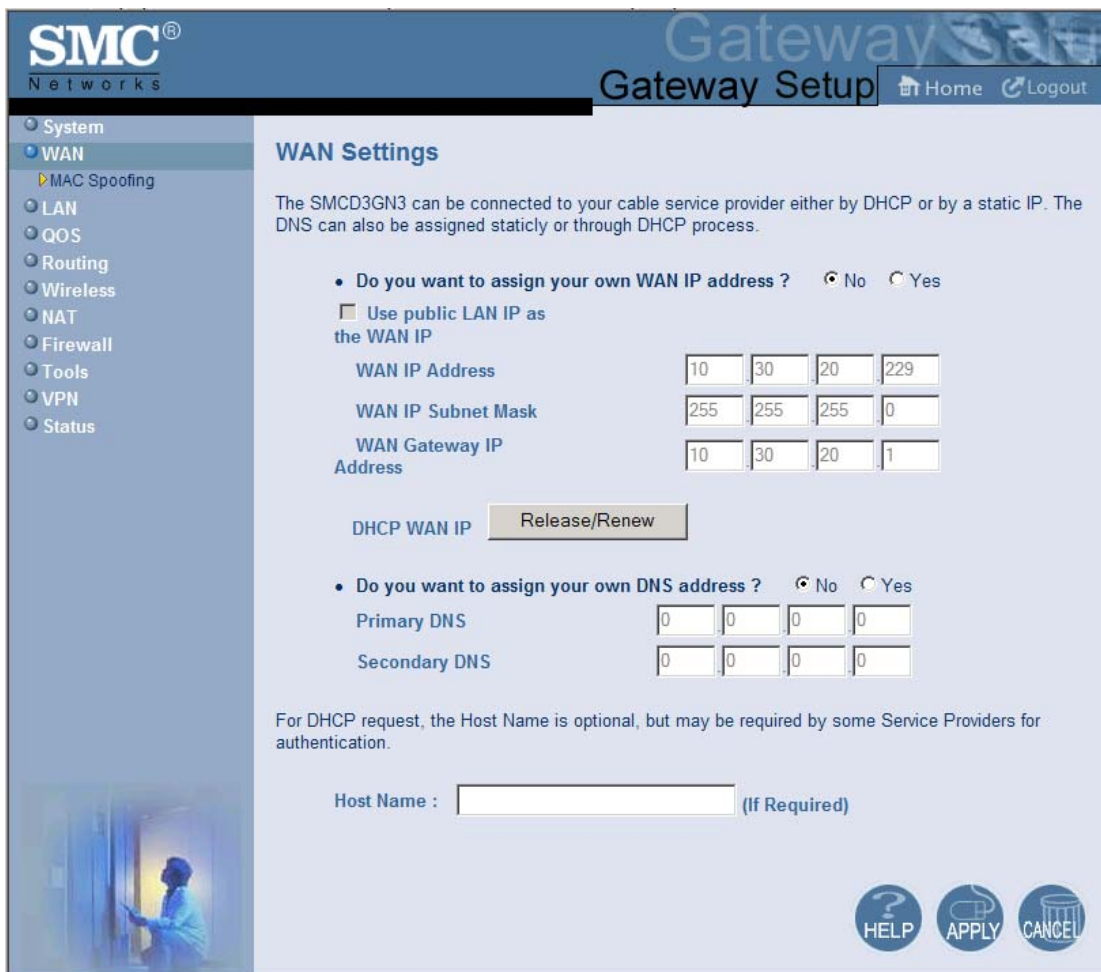


Figure 22. WAN Settings Menu

Table 7. WAN Settings Menu Options

Option	Description
Do you want to assign your own WAN IP address?	By default, this option is set to No . Cable modem providers typically use dynamic assignment of IP addresses. To assign a static WAN IP address to the Gateway and make the WAN fields below this option available, click Yes .
Use public LAN IP as the WAN IP	Check this box if you want to use the static public LAN IP address for the WAN IP address. This checkbox is available if Do you want to assign your own WAN IP address is set to Yes .
WAN IP Address	Enter a unique static IP address the Gateway.
WAN IP Subnet Mask	Enter the subnet mask for the Gateway
WAN Gateway IP Address	Enter the Gateway IP address.
Release/Renew button	Click this button to release and then renew the Gateway's IP address. This button is available for DHCP only. It is gray and unavailable when Do you want to assign your own WAN IP address is set to Yes .
Do you want to assign your own DNS address?	By default, this option is set to No . Cable modem providers typically use dynamic assignment of IP addresses. To assign your own IP addresses to primary and secondary DNS servers and make the DNS fields below this option available, click Yes .
Primary DNS	Enter a primary DNS server IP address.
Secondary DNS	Enter the secondary DNS server IP address.
Host Name	This setting is optional. If you will require a host name for DHCP requests, enter it here.

MAC Spoofing Menu

If you need to re-register your MAC address, you can use the MAC Spoofing menu to clone (or “spoof”) the Gateway’s registered MAC address as necessary.

If you use the public static LAN IP address as the WAN IP for NAT translation, no MAC spoofing is necessary,

To access the MAC Spoofing menu, click **WAN** in the menu bar and then click the **MAC Spoofing** submenu. Figure 23 shows an example of the menu and Table 8 describes the settings you can select.

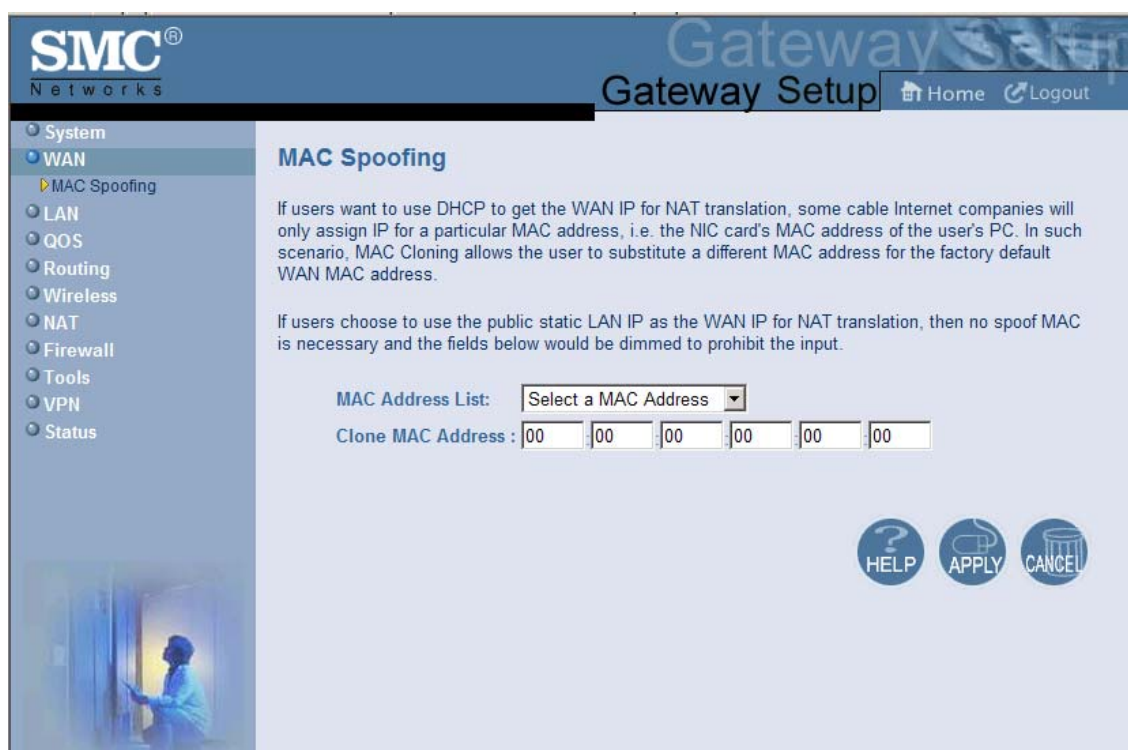


Figure 23. MAC Spoofing Menu

Table 8. MAC Spoofing Menu Options

Option	Description
MAC Address List	Select the MAC address you want to spoof.
Clone MAC Address	Clone the MAC address of the NIC communicating with the cable modem.

LAN Settings Menu

IP addresses are close to being used up and thus very hard to get. One solution to this problem is "private" IP addresses. Private IP addresses are ranges of IP addresses set aside expressly for use by a company or other entity internally. Private IP addresses are non-routable and, therefore, cannot be used to connect directly to the Internet.

Some of the advantages of private IP addresses include:

- Increased security, since private IP addresses are not routable across the Internet
- You conserve the world-wide pool of IP addresses
- You do not have to register or pay for these IP addresses in any way

The LAN Settings menu lets you configure private LAN IP settings and private IP address pools for the Gateway. To access the LAN Settings menu, click **LAN** in the menu bar. Figure 24 shows an example of the menu and Table 9 describes the settings you can select.

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

- System
- WAN
- LAN**
 - Ether Switch Control
 - Ether Access Control
 - Additional Public Lan
 - Public IP Access Control
- QOS
- Routing
- Wireless
- NAT
- Firewall
- Tools
- VPN
- Status

LAN Settings

Users can set up the public LAN IP, also the private LAN IP in this page. The private LAN IP is also the IP of the DHCP server which will dynamically allocate IP address for the client PCs behind the Gateway.

Public LAN IP

IP address	172	16	255	254
IP Subnet Mask	255	255	255	252
Domain Name	<input type="text"/>			
As WAN IP	<input type="checkbox"/>			

Private LAN IP

IP address	192	168	0	1
IP Subnet Mask	255	255	255	0
Domain Name	<input type="text"/>			

Enable DHCP Server

Lease Time: One Week

Assign DNS Manually

Primary DNS	0	0	0	0
Secondary DNS	0	0	0	0

Private IP Address Pool

Start IP	192	168	0	10
End IP	192	168	0	199

PPTP IP Address Pool

Start IP	192	168	0	200
End IP	192	168	0	249

HELP APPLY CANCEL

Figure 24. LAN Settings Menu

Table 9. LAN Settings Menu Options

Option	Description
Public LAN IP	
IP Address	IP address of the Gateway's private LAN settings. Default IP address is 192.168.0.1. if you change this setting, the Gateway reboots after displaying a message.
IP Subnet Mask	Subnet mask of the Gateway's private LAN settings. Default subnet mask is 255.255.255.0.
Domain Name	Domain name of the Gateway's private LAN settings.
As WAN IP	Check this box if you want to use the static public LAN IP address for the WAN IP address.
Private LAN IP	
IP Address	IP address of the Gateway's private LAN settings. Default IP address is 192.168.0.1. if you change this setting, the Gateway reboots after displaying a message.
IP Subnet Mask	Subnet mask of the Gateway's private LAN settings. Default subnet mask is 255.255.255.0.
Domain Name	Domain name of the Gateway's private LAN settings.
Enable DHCP Server	Enables or disables the DHCP server to allow automatic allocation of IP addresses to LAN client PCs. <ul style="list-style-type: none"> • Checked = DHCP server is enabled. (<i>default</i>) • Unchecked = DHCP server is disabled.
Lease Time	Amount of time a DHCP network user is allowed connection to the Gateway with their current dynamic IP address. Default is One Week. This option is available when Enable DHCP Server is checked.
Assign DNS Manually	Enables or disables the DHCP server to allow automatic allocation of primary and secondary IP addresses for DSN servers on the LAN. <ul style="list-style-type: none"> • Checked = use static IP addresses for primary and secondary DNS servers. If checked, enter the IP addresses of the primary and secondary DNS server in the Primary DNS and Secondary DNS fields. • Unchecked = allocate IP addresses for primary and secondary DNS servers automatically. (<i>default</i>)
Primary DNS	Static IP address of the primary DNS server. This option is available when Assign DNS Manually is checked.
Secondary DNS	Static IP address of the secondary DNS server. This option is available when Assign DNS Manually is checked.
Private IP Address Pool	
Start IP	Starting IP address range for the pool of allocated for private IP addresses.
End IP	Ending IP address range for the pool of allocated for private IP addresses.
PPTP IP Address Pool	
Start IP	Starting IP address range for the pool of allocated for point-to-point tunneling protocol (PPTP) IP addresses.
End IP	Ending IP address range for the pool of allocated for PPTP IP addresses.

Ether Switch Port Control Menu

By default, the Gateway LAN ports are enabled to auto-negotiate the highest supported speed and appropriate duplex mode. If these settings prevent the Gateway from successfully connecting with other devices, you can use the Ether Switch Port Control menu to configure the Gateway to use fixed speed and duplex settings. The Ether Switch Port Control menu also let you disable the individual LAN ports. For your convenience, each port can be configured independently of the other LAN ports on the Gateway.

To access the Ether Switch Control menu, click **LAN** in the menu bar and then click the **Ether Switch Control** submenu in the menu bar. Figure 25 shows an example of the menu.

The screenshot shows the SMC Networks Gateway Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN (selected), Ether Switch Control (highlighted), Ether Access Control, Additional Public Lan, Public IP Access Control, QOS, Routing, Wireless, NAT, Firewall, Tools, VPN, and Status. The main content area is titled "Ether Switch Port Control" and contains the following text:

SMCD3GN3's ether switch allows users to control the enable/disable, auto-negotiation enable/disable, line speed and mode if auto-negotiation is disabled. Users could set the following table according to their need. For example, if they want to setup port 1 for 10Mbps and half duplex, they could just leave the checkboxes of the Auto, Speed and Mode to be blank for port 1. If they want to set for 100Mbps and full duplex, they need to leave the Auto checkbox to be blank and check the checkboxes of Speed and Mode for port 1. If they want the auto-negotiation, just check the the Auto checkbox.

Switch Port	Auto	Speed(10/100/1000)			Mode(H/F)	Enable
1	<input checked="" type="checkbox"/>	<input type="radio"/> 10Mbps	<input type="radio"/> 100Mbps	<input type="radio"/> 1000Mbps	<input checked="" type="checkbox"/> Full	<input checked="" type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="radio"/> 10Mbps	<input type="radio"/> 100Mbps	<input type="radio"/> 1000Mbps	<input checked="" type="checkbox"/> Full	<input checked="" type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input type="radio"/> 10Mbps	<input type="radio"/> 100Mbps	<input type="radio"/> 1000Mbps	<input checked="" type="checkbox"/> Full	<input checked="" type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input type="radio"/> 10Mbps	<input type="radio"/> 100Mbps	<input type="radio"/> 1000Mbps	<input checked="" type="checkbox"/> Full	<input checked="" type="checkbox"/>

At the bottom right of the main content area, there are three circular buttons: HELP (with a question mark), APPLY (with a checkmark), and CANCEL (with a red X).

Figure 25. Ether Switch Port Control Menu

The following procedure describes how to change the settings in the Ether Switch Port Control menu.

1. To change a port from auto-negotiation to a fixed speed and duplex setting:
 - a. Uncheck the **Auto** check box for the port.
 - b. Under **Speed (10/100/1000)**, click the radio that corresponds to the fixed speed you want to use for that port.
 - c. Under the **Mode H/F** column, leave the check mark for full-duplex mode or uncheck it for half-duplex mode.
2. To disable a port, regardless of the auto-negotiation and duplex settings, uncheck **Enable** for the port.
3. Click **Apply**.

LAN Access Control Menu

Using the LAN Access Control menu, you can:

- Allow all EtherLAN client stations to access the Internet through the Gateway. This is the default setting.
- Allow certain trusted EtherLAN client stations to access the Internet through the Gateway. You use the add up to 16 trusted clients.
- Deny certain trusted EtherLAN client stations from accessing the Internet through the Gateway. You use the add up to 16 untrusted clients.

To access the LAN Access Control menu, click **LAN** in the menu bar and then click the **Ether Access Control** submenu in the menu bar. Figure 26 shows an example of the menu.

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

- System
- WAN
- LAN**
 - Ether Switch Control
 - Ether Access Control**
 - Additional Public Lan
 - Public IP Access Control
- QOS
- Routing
- Wireless
- NAT
- Firewall
- Tools
- VPN
- Status

LAN Access Control

The SMCD3GN3 can allow the Ether LAN client stations to connect to your SMCD3GN3 in any of these ways:

- All Ether LAN stations** Allow all Ether LAN stations to access the Internet through the SMCD3GN3
- Trusted PC list** Allow particular Ether LAN client stations to access the Internet through the SMCD3GN3. You can use the trusted table to add/delete the clients.
- Untrusted PC list** Disallow particular Ether LAN client stations to access the Internet through the SMCD3GN3. You can use the untrusted table to add/delete the clients.

Lan Trusted Table (up to 16 items)

#	Device Name	MAC Address
<input type="button" value="Delete"/>		

Lan Untrusted Table (up to 16 items)

#	Device Name	MAC Address
<input type="button" value="Delete"/>		

Auto-Learned Lan Devices

Device Name	MAC Address	Trusted?
		<input type="radio"/> Y <input type="radio"/> N

Manually-Added Lan Devices

Device Name	MAC Address	Trusted?
<input type="text"/>	<input type="text"/>	<input type="radio"/> Y <input type="radio"/> N
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

Figure 26. LAN Access Control Menu

Controlling LAN Access

By default, **All EtherLAN LAN stations** is selected at the top of the menu. This setting allows all client stations to access the Internet through the Gateway. To restrict LAN access, click one of the following radio buttons and click **Apply**:

- **Trusted PC List** = restricts Internet access through the Gateway to client stations in the Lan Trusted Table. To add client station to this table, see “Adding and Deleting Trusted Client Stations”, below.
- **Untrusted PC list** = prevents client stations in the Lan Untrusted Table from accessing the Internet through the Gateway. To add client stations to this table, see “Adding and Deleting Untrusted Client Stations” on page 57.

Adding and Deleting Trusted Client Stations

To restrict Internet access through the Gateway to certain trusted EtherLAN client stations, define the client stations as trusted clients. Using this procedure you can define up to 16 trusted client stations.

1. Click **Trusted PC list** at the top of the menu.
2. To add client stations that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned Lan Devices**:
 - a. Click a client station that the Gateway learned automatically.
 - b. Under **Trusted?**, click **Y**.
 - c. Click **Add**. The client station is added to the **Lan Trusted Table**.
 - d. To add more auto-learned client stations (up to 16), repeat steps 2a through 2c.
3. To manually add trusted client stations, perform the following steps under **Manually-Added Lan Devices**:
 - a. Under **Device Name**, enter a name for the device.
 - b. Under **MAC Address**, enter the MAC address of the device.
 - c. Under **Trusted?**, click **Y**.
 - d. Click **Add** to add the client station to the **Lan Trusted Table**.
 - e. To manually add more client stations (up to 16), repeat steps 3a through 3d.

4. To delete client stations from the **Lan Trusted Table**, click the radio button corresponding to the client station you want to delete and click the **Delete** button. A precautionary message does not appear before deleting a client station.
5. To enforce this policy, click **Trusted PC list** at the top of the menu.
6. When you finish, click **Apply**.

Adding and Deleting Untrusted Client Stations

To prevent certain trusted EtherLAN client stations from accessing the Internet through the Gateway, define the client stations as untrusted clients. Using this procedure you can define up to 16 untrusted client stations

1. Click **Untrusted PC list** at the top of the menu.
2. To add client stations that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned Lan Devices**:
 - a. Click a client station that the Gateway learned automatically.
 - b. Under **Trusted?**, click **N**.
 - c. Click **Add** to add the client station to the **Lan Untrusted Table**.
 - d. To add more auto-learned client stations, repeat steps 2a through 2c.
3. To manually add client stations, perform the following steps under **Manually-Added Lan Devices**:
 - a. Under **Device Name**, enter the name of the device.
 - b. Under **MAC Address**, enter the MAC address of the device.
 - c. Under **Trusted?**, click **N**.
 - d. Click **Add** to add the client station to the **Lan Untrusted Table**.
 - e. To add more client stations manually, repeat steps 3a through 3d.
4. To delete client stations from the untrusted list, in the **Lan Untrusted Table**, click the radio button corresponding to the client station you want to delete and click the **Delete** button. A precautionary message does not appear before deleting an untrusted client station.
5. To enforce this policy, click **Untrusted PC list** at the top of the menu.
6. When you finish, click **Apply**.

Additional Public Lan Menu

Using the Additional Public Lan menu, you can add more than one public subnet to the LAN interface.

To access the Additional Public Lan menu, click **LAN** in the menu bar and then click the **Additional Public Lan** submenu in the menu bar. Figure 27 shows an example of the menu.



Figure 27. Additional Public Lan Menu

Adding Public Subnets

Using the following procedure, you can add up to 5 public subnets to the LAN interface.

1. In the Additional Public LAN menu, click the **Add** button. The Adding Public Lan menu in Figure 28 appears.

The screenshot shows the SMC Networks Gateway Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN (expanded), QOS, Routing, Wireless, NAT, Firewall, Tools, VPN, and Status. Under the LAN menu, there are sub-items: Ether Switch Control, Ether Access Control, Additional Public Lan (highlighted), and Public IP Access Control. The main content area is titled 'Adding Public Lan' and includes the following text: 'In this page, users can specify the new gateway ip and subnet mask for the new public LAN subnet.' Below this text is a form with two rows: 'IP Address' and 'Subnet Mask', each with five input fields. Below the form are three buttons: 'Back', 'Apply', and 'Cancel'. A 'HELP' button is located in the bottom right corner of the main content area.

Figure 28. Adding Public Lan Menu

2. In the **IP Address** row, enter the IP address for the new public subnet.
3. In the **Subnet Mask** row, add the subnet mask for the new public subnet.
4. Click **Apply** to add the IP address and subnet. (Or click **Back** to return to the previous menu or **Cancel** to cancel the operation .) If you clicked **Apply**, the IP address and subnet mask are added to the **Additional Public Lan Table**.
5. By default the IP address and subnet you specified are active. To make them inactive, uncheck the check box below **Active**.
6. Click **Apply** in the Additional Public Lan menu to save your settings.
7. To add more public subnets (up to 5), repeat steps 1 through 6.

8. To change the settings for a subnet, click the radio button to the left of the subnet you want to change and click the **Edit** button. When the Adding Public Lan menu appears, edit the IP address and subnet mask as necessary and click **Apply**. Click **Apply** in the Additional Public Lan menu to save your settings.
9. To delete a subnet, click the radio button to the left of the subnet you want to delete and click the **Delete** button. No precautionary message appears before you delete a subnet. Click **Apply** in the Additional Public Lan menu to save your settings.

Public IP Access Control Menu

Using the Public IP Access Control menu, you can block specific public IP addresses from accessing the Internet.

To access the Public IP Access Control, click **LAN** in the menu bar and then click the **Public IP Access Control** submenu in the menu bar. Figure 29 shows an example of the menu and Table 10 describes the settings you can select.



Figure 29. Public IP Access Control Menu

Table 10. Public IP Access Control Menu Options

Option	Description
Enable Public IP Access Control	Check this check box to make the fields on this page available.
Single Address / Address Range	<p>From the first drop-down list, select whether you want to block a single IP address or a range of IP addresses.</p> <ul style="list-style-type: none">• If you select Single Address, type the four octets of the IP address you want to block. The second set of four fields is unavailable.• If you select Address Range, in the first four fields, type the first four octets of the IP address in the starting IP address range you want to block. In the last four fields, type the last four octets of the IP address in the ending IP address you want to block. The IP address or address range appears in the Deny IP Addresses list.
Delete	To remove an IP address or address range from the Deny IP Addresses list, click the IP address or address range and click Delete .

QoS Settings Menu

Quality of Service (QoS) refers to a collection of techniques for identifying data whose delivery across the network is time sensitive, and managing its delivery through both bandwidth allocation and prioritization schemes

Using the QoS Settings menu, you can enable the Gateway's QoS module to provide guarantees on the ability of the network to deliver predictable results. To access the QoS menu, click **QOS** in the menu bar. Figure 30 shows an example of the menu.

By default, QoS is enabled. To enable the Gateway's QoS module, check **Enable QOS Module** and click **Apply**. To disable the Gateway's QoS module, uncheck **Enable QOS Module** and click **Apply**.

If you enable the Gateway's QoS module, the following submenus appear under **QOS** in the menu bar:

- **Port** - lets you configure the priority queue to which the switch port is mapped. See page 64.
- **COS** - lets you define four queues to which the CoS is mapped. See page 65.
- **DSCP** - lets you define the QoS class queue to which the customized DSCP is mapped. See page 67.
- **Queue** - lets you specify whether QoS behavior runs with strict or weighted priority. See page 69.
- **DSCP Remarking** - lets you define the DSCP remarking action and mode. See page 71.

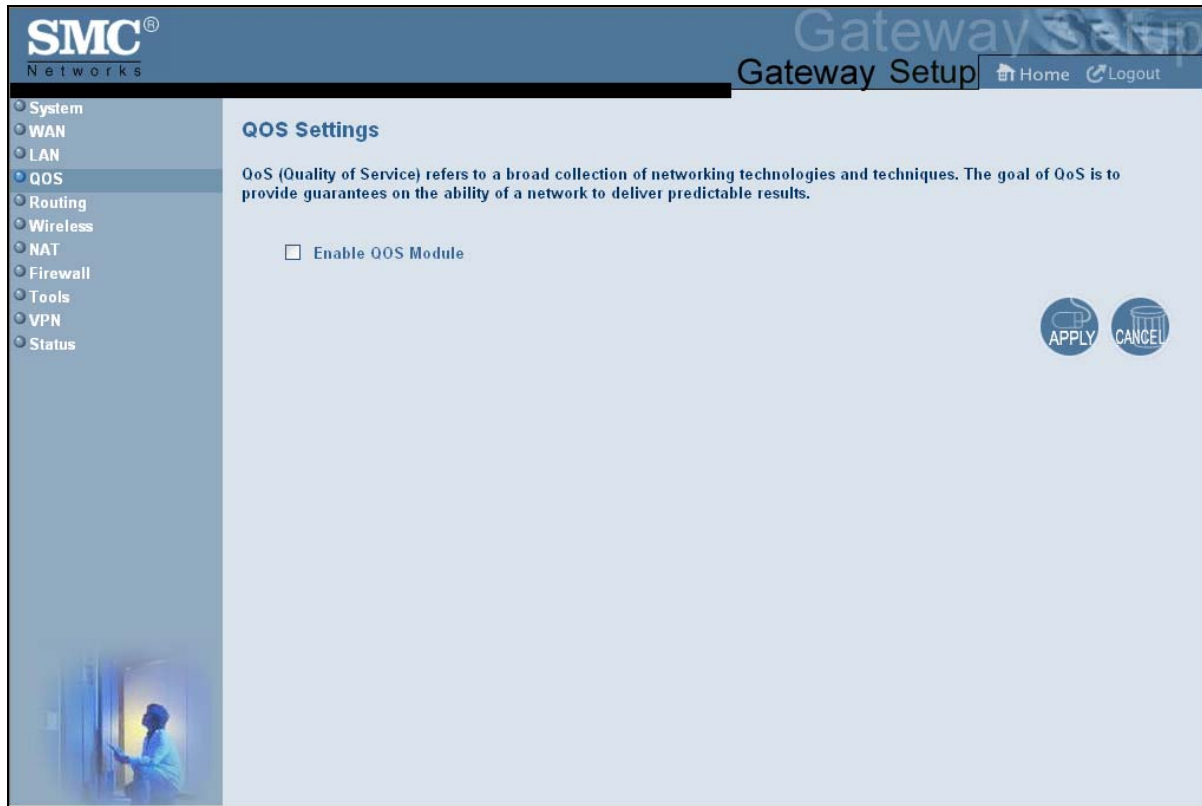


Figure 30. QoS Settings Menu

Port Based QoS Menu

The Port Based QoS menu lets you prioritize performance of the four Gateway LAN ports. To access the Port Based QoS menu, click **QoS** in the menu bar and then click the **Port** submenu in the menu bar. Figure 31 shows an example of the menu.



Note: The **Port** submenu is not available in the menu bar if **Enable QoS Module** is not checked in the QoS Settings menu (see page 62).

The screenshot shows the SMC Networks Gateway Setup interface. The left sidebar contains a navigation menu with categories: System, WAN, LAN, QoS, Routing, Wireless, NAT, Firewall, Tools, VPN, and Status. The QoS category is expanded, showing sub-items: Port, COS, DSCP, Queue, and DSCP Remarking. The 'Port' sub-item is selected. The main content area is titled 'Port Based QoS' and contains the following text: 'This page defines the Priority Queue to which the switch port mapped. Higher priority values are evaluated as of higher importance'. Below this text is a checkbox labeled 'Enable Port Based QoS'. Underneath the checkbox is a table with two columns: 'Port' and 'Queue'. The table has four rows, each representing a port and its corresponding queue number. The 'Queue' column contains dropdown menus with values 0, 1, 2, and 3. At the bottom right of the page are three circular buttons: HELP, APPLY, and CANCEL.

Port	Queue
1	0
2	1
3	2
4	3

Figure 31. Port Based QoS Menu

To define port-based QoS settings:

1. Check **Enable Port Based QoS**.
2. For each port, select a priority queue number from 0 to 3. Higher priority values are evaluated as being of higher importance than lower priority values.
3. Click **Apply**.

CoS Settings Menu

Given that there will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity, it is important to move traffic on the basis of relative importance. Without CoS prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. For example, without CoS, most traffic received by the Gateway is forwarded with the same priority it had upon entering the Gateway. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your requirements. CoS helps to keep the most important network traffic moving at an acceptable speed, regardless of current bandwidth usage. This means you can manage available bandwidth so that the switch transmits the most important traffic first.

The CoS Settings menu lets you configure a CoS priority of 0 through 7 for an outbound packet. When the packet is then sent to a port, the CoS priority determines which outbound queue the packet uses. After configuring CoS priority for outbound packets, use this menu to map the classes of service to the Gateway’s four ports.

To access the CoS Settings menu, click **QOS** in the menu bar and then click the **CoS** submenu in the menu bar. Figure 32 shows an example of the menu.



Note: The **COS** submenu is not available in the menu bar if **Enable QOS Module** is not checked in the QoS Settings menu (see page 62).

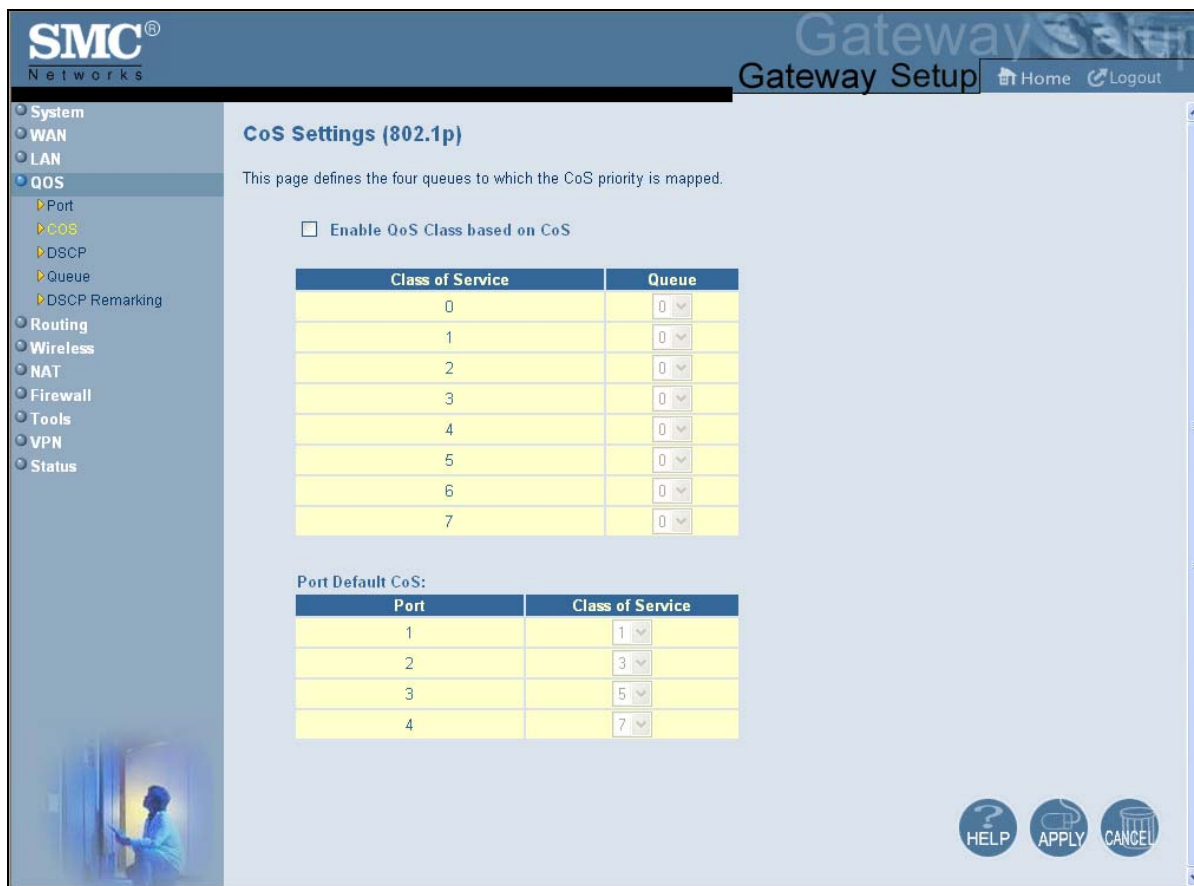


Figure 32. CoS Settings Menu

To define CoS settings:

1. Check **Enable QoS Class based on CoS**.
2. For each class of service, assign a queue number from 0 to 3. Higher priority values are evaluated as being of higher importance than lower priority values.
3. Under **Port Default CoS**, map the Gateway's four ports to the classes of service you defined in the previous step.
 - CoS setting from 0 to 3 = normal priority. Packets in this queue leave the port after the high-priority queue is emptied.
 - CoS setting from 4 to 7 = high priority. Packets in this queue leave the port first.
4. Click **Apply**.

DSCP Based QoS Menu

The DSCP Based QoS menu lets you classify and prioritize traffic using DSCP tags. DSCP allows the Gateway to determine how traffic classes should be prioritized. Using the DSCP Based QoS menu, you can use DSCP to provide different levels of service to conforming and non-conforming traffic by appropriately selecting the DSCP values in this menu. The Gateway uses the Hierarchical Token Bucket queuing algorithm, which divides the 64 possible DSCP code values into 8 queues.

Table 11 shows the actual queuing.

Table 11. Queuing for DSCP-Based QoS

Name	Precedence	DSCP Range	Priority
Routing (default)	000 (0)	000000(0) – 000111 (7)	8
Priority	001 (1)	001000 (8) – 001111 (15)	7
Immediate	010 (2)	010000 (16) – 010111 (23)	6
Flash	011 (3)	011000 (24) – 011111 (31)	5
Flash Override	100 (4)	100000 (32) – 100111 (39)	4
Critical	101 (5)	101000 (40) – 101111 (47)	3
Internetwork Control	110 (6)	111000 (48) – 110111 (55)	2
Network Control	111 (7)	111000 (56) – 111111 (63)	1

To access the DSCP Based QoS menu, click **QOS** in the menu bar and then click the **DSCP** submenu in the menu bar. Figure 33 shows an example of the menu.



Note: The **DSCP** submenu is not available in the menu bar if **Enable QoS Module** is not checked in the QoS Settings menu (see page 62).

The screenshot shows the SMC Networks Gateway Setup interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, QoS (selected), Port, COS, DSCP, Queue, DSCP Remarking, Routing, Wireless, NAT, Firewall, Tools, VPN, and Status. The main content area is titled "DSCP Based QoS" and includes the following text: "This page defines the QoS Class Queue to which the customized DSCP mapped." Below this text is a checkbox labeled "Enable DSCP Based QoS". A table with three columns: "Index", "DSCP Value (0-63)", and "Queue" is displayed. The table has 8 rows, with the last row labeled "Others". At the bottom right of the page are three circular buttons: HELP, APPLY, and CANCEL.

Index	DSCP Value (0-63)	Queue
0	<input type="text" value="0"/>	<input type="text" value="0"/>
1	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input type="text" value="0"/>	<input type="text" value="0"/>
5	<input type="text" value="0"/>	<input type="text" value="0"/>
6	<input type="text" value="0"/>	<input type="text" value="0"/>
7	Others	<input type="text" value="0"/>

Figure 33. DSCP Based QoS Menu

To define DSCP-based QoS settings:

1. Check **Enable DSCP Based QoS**.
2. For each index, select a DSCP value from 0 to 63.
3. Under **Queue**, select a queue (from 0 to 3) you want to map to this DSCP value. Higher priority values are evaluated as being of higher importance than lower priority values.
4. To define DSCP-based QoS values for other queues, repeat steps 2 and 3.
5. Click **Apply**.

Queue Settings Menu

The Queue Settings menu lets you configure QoS behavior as either strict priority or weighted priority.

- Strict priority – allows delay-sensitive data such as voice to be sent before packets in other queues.
- Weighted priority – lets you assign each queue with a certain weight indicating the amount of guaranteed capacity, with high priority packets served before any low priority packets.

To access the Queue Settings menu, click **QOS** in the menu bar and then click the **Queue** submenu in the menu bar. Figure 34 shows an example of the menu.



Note: The **Queue** submenu is not available in the menu bar if **Enable QOS Module** is not checked in the QoS Settings menu (see page 62).

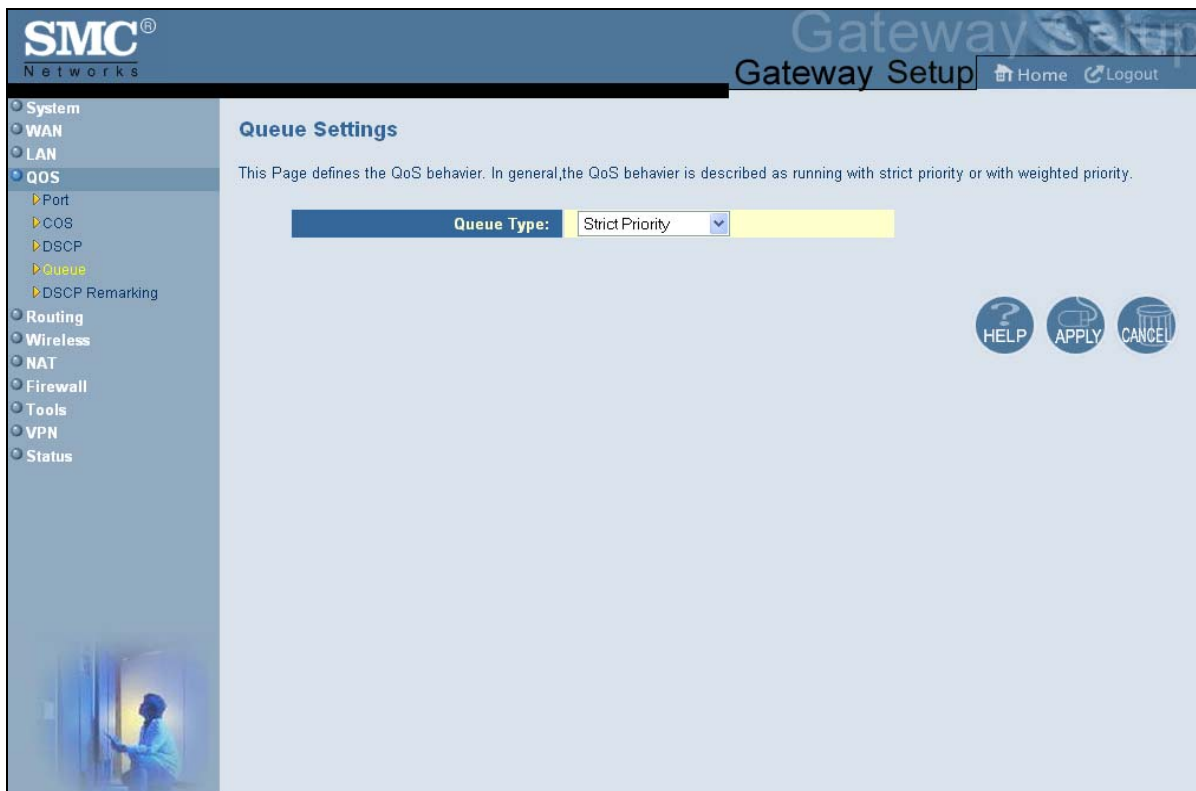


Figure 34. Queue Settings Menu

By default, the Gateway uses strict priority. To change to weighted priority:

1. For **Queue Type**, select **Weighted Priority**. The options in Figure 35 appear.

Queue Type: <input type="text" value="Weighted Priority"/>		
Weight Base: <input type="text" value="10"/>		
Queue	Weight (0-undefined)	% of Bandwidth
0	<input type="text" value="1"/>	10
1	<input type="text" value="2"/>	20
2	<input type="text" value="3"/>	30
3	<input type="text" value="4"/>	40

Figure 35. Weighted Priority Options

2. For **Weight Base**, select a queue weight to ensure that some sets of queues get higher thresholds than others. Queue weight directs the Gateway to set the queue thresholds proportionately. Choices are **8** or **10**. Queues with a weight of 10 are longer than those with a queue weight of 8.
3. For each Gateway queue, select a weight. Each weight corresponds to a percentage of consumed bandwidth, as shown in the **% of Bandwidth** column.
4. When you finish, click **Apply**.

DSCP Remarking Menu

The DSCP Remarking menu lets you configure the Gateway's DSCP remarking mode and actions.

To access the Queue Settings menu, click **QOS** in the menu bar and then click the **DSCP Remarking** submenu in the menu bar. Figure 36 shows an example of the menu.



Note: The **DSCP Remarking** submenu is not available in the menu bar if **Enable QOS Module** is not checked in the QoS Settings menu (see page 62).

SMC Networks Gateway Setup Home Logout

DSCP Remarking

This pages defines the DSCP remarking action and mode. The four internal priorities mapping mode:
 1. Map to AF code points: 0:AF12, 1:AF22, 2:AF32, 3:AF42
 2. Map to CS code points: 0:000000b, 1:001000b, 2:010000b, 3:011000b

Enable DSCP Remarking

Dscp remarking mode:

Map frame priority to AF code points	<input checked="" type="radio"/>
Map frame priority to CS code points	<input type="radio"/>

Request a remarking action, when DSCP equals one of the following CPs:

Expedited Forwarding Code Point	<input type="checkbox"/>
Assured Forwarding Code Points	<input type="checkbox"/>
Class Selector Code Points	<input checked="" type="checkbox"/>
Zero	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>

HELP APPLY CANCEL

Figure 36. DSCP Remarking Menu

To configure DSCP remarking settings:

1. Check **Enable DSCP Remarking**.
2. Complete the options in the menu and refer to Table 12.
3. When you finish, click **Apply**.

Table 12. DSCP Remarking Options

Option	Description
Dscp remarking mode	<p>Lets you select the DSCP remarking mode that the Gateway is to use. Choices are:</p> <ul style="list-style-type: none"> • Map frame priority to AF code points = select this option for Quality of Service configurations that use assured forwarding (AF) code points to mark packets. AF guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. (<i>default</i>) • Map frame priority to CS code points = select this option for Quality of Service configurations that use class selector (CS) code points to mark packets. CS provides code points that can be used for backward compatibility with IP Precedence. IP Precedence is a legacy technology that the Gateway supports for backwards compatibility.
Request a remarking action when DSCP equals one of the following CPs	
Expedited Forwarding Code Point	Expedited forwarding provides a low-loss, low-latency, low-jitter, and assured bandwidth service. Applications such as VoIP, video, and other time sensitive applications require a robust network treatment like expedited forwarding. When checked, the Gateway requests a remarking action if DSCP equals an expedited forwarding code point. By default, this option is not checked.
Assured Forwarding Code Points	Assured forwarding defines a method by which packets can be given different forwarding assurances. Traffic can be divided into different classes and then each class given a certain percentage of bandwidth. For example, one class could have 50% of the available link bandwidth, another class could have 30%, and another 20% of the bandwidth. When checked, the Gateway requests a remarking action if DSCP equals an assured forwarding code point. By default, this option is not checked.
Class Selector Code Points	Class Selector code points are code points that can be used for backward compatibility with IP Precedence models. When checked, lets the Gateway request a remarking action if DSCP equals a class selector code point. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.
Zero	When checked, lets the Gateway request a remarking action if DSCP equals zero. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.
Others	When checked, lets the Gateway request a remarking action if DSCP equals a non-zero value. By default, this option is checked, but does not take effect until the OSPF Status changes to ENABLE.

Routing Menus

The Routing menu provides the following submenus for configuring Gateway routing:

- Static routes – lets you manually add static routes to create specific paths to desired destinations. See page 73.
- RIP control – lets you select how the Gateway adjusts to physical changes in the network's layout and exchange routing tables with other routers. See page 75.
- OSPF control – lets you control how the Gateway works with the OSPF protocol. See page 79.

Static Routes Menu

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Using the Static Routes menu, you can manually add static routes to create specific paths to desired destinations.

To access the Static Routes menu, click **Routing** in the menu bar and then click the **Static Routes** submenu. Figure 37 shows an example of the menu.

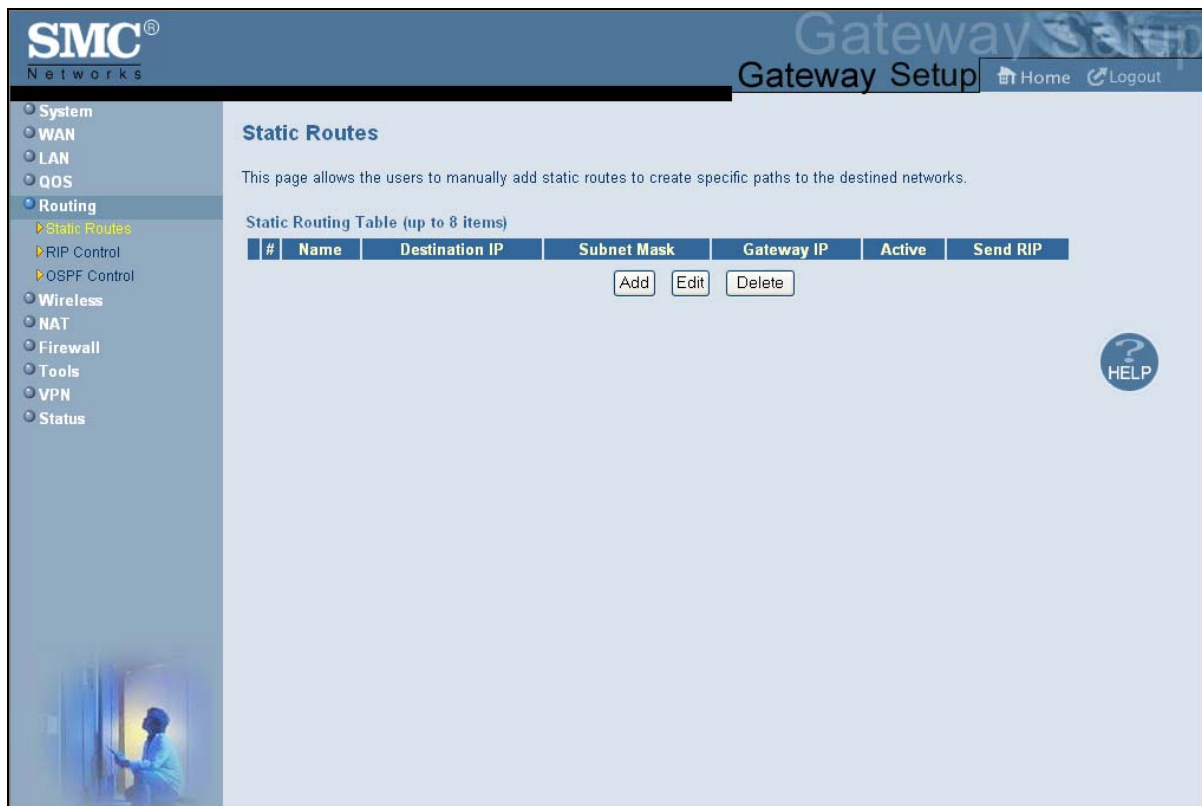


Figure 37. Static Routes Menu

Using the Static Routes menu, you can add up to eight static routes, containing different networks and subnets, to routers connected to the Gateway. The following example describes how to configure a static route. For example, assume that a router called **SMC** is connected to the Gateway with subnet address 111.222.33.0 attached to it. Also, assume that the router's IP address in the Gateway subnet is 192.168.100.33. In this example, you can add a static route named **SMC**, with a destination IP address of 111.222.33.0, a subnet mask of 255.255.255.0, and a gateway IP address of 192.168.100.33.

Adding Static Routes

To add static routes:

1. In the Static Routes menu, click **Add**. The Add Static Routes menu in Figure 38 appears.

SMC[®]
Networks

Gateway Setup Home Logout

Add Static Routes

In this page, users can add static routes to the routers connected to the SMCD3GN3, containing different networks and subnets. Users can specify a name for the route as a way to easily remember which entry is linked to which route. The Destination IP and its Subnet Mask are the network IP address of the destination network and its subnet mask. The Gateway IP is the locally-assigned IP address on the Gateway LAN network. For example, a router 'SMC' is connected to the SMCD3GN3, which has a subnet address '111.222.33.0' attached to it, and its IP in the SMCD3GN3 subnet is '192.168.100.33'. We can add a static route called 'SMC' and its destination IP is '111.222.33.0', subnet mask is '255.255.255.0' and its gateway IP is '192.168.100.33'.

Name	<input type="text"/>
Destination IP	<input type="text"/>
Subnet Mask	<input type="text"/>
Gateway IP	192 168 <input type="text"/>

Back Apply Cancel

HELP

Figure 38 Add Static Routes Menu

2. Complete the fields in the Add Static Routes menu (see Table 18).
3. Click **Apply**. (Or click **Back** to return to the Static Routes menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the static route is added to the **Static Routing Table**.
4. To define additional static routes (up to eight), repeat steps 1 through 3.
5. To change the settings for a static route, click the radio button to the left of the static route you want to change and click the **Edit** button. When the Add Static Routes menu appears, edit the settings as necessary (see Table 18) and click **Apply**.

- To delete a static route, click the radio button to the left of the static route you want to delete and click the **Delete** button. No precautionary message appears before you delete a static route.

Table 13. Add Static Routes Menu Options

Option	Description
Name	Name used to identify the route.
Destination IP	IP address of the destination network.
Subnet Mask	Subnet mask of the destination network. The subnet mask determines which part of the Destination IP address is the network portion and which part is the host portion.
Gateway IP	Locally assigned IP address on the Gateway that allows contact between the Gateway and the remote network or host.

RIP Control Menu

RIP sends routing-update messages at regular intervals. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

In general, when a router sends a routing update, the following authentication sequence occurs

- A router sends a routing update with a key and the corresponding key number to the neighbor router.
- The receiving (neighbor) router checks the received key against the same key stored in its own memory.
- If the two keys match, the receiving router accepts the routing update packet. If the two keys do not match, it rejects the routing update packet.

Using the RIP Control menu, you can configure the way how the Gateway adjusts to physical changes in the network's layout and exchange routing tables with other routers. To access the RIP Control menu, click **Routing** in the menu bar and then click the **RIP Control** submenu. Figure 46 shows an example of the menu and Table 21 describes the options.

SMC Networks Gateway Setup [Home](#) [Logout](#)

- System
- WAN
- LAN
- QOS
- Routing**
 - Static Routes
 - RIP Control**
 - OSPF Control
- Wireless
- NAT
- Firewall
- Tools
- VPN
- Status

RIP Control

This page allows the users to control the RIP protocol which could be used to exchange the routing information between routers. The routing information could be used to build up/modify/age out the routes dynamically.

RIP Control Table

Interface Name	Cable
RIP Send Version	Do Not Send
RIP Receive Version	Do Not Receive
Update Interval	30 sec
Default Metric	1
Authentication Type	No Authentication
Authentication Key & ID	Key: ***** ID: 0
Neighbor	

HELP APPLY CANCEL

Figure 39. RIP Control Menu

Table 14. RIP Control Menu Options

Option	Description
WPS Summary	
Interface Name	Select the name of the interface. Choices are <ul style="list-style-type: none"> • Cable (<i>default</i>) • CPE
RIP Send Version	Select the format and the broadcasting method of the RIP packets that the Gateway sends. Choices are: <ul style="list-style-type: none"> • Do Not Send (<i>default</i>) • RIP1 • RIP2 • RIP1/2 Your selection should match the version supported by other routers on your network.
RIP Receive Version	Select the format and the broadcasting method of the RIP packets that the Gateway receives. Choices are: <ul style="list-style-type: none"> • Do Not Receive (<i>default</i>) • RIP1 • RIP2 • RIP1/2 Your selection should match the version supported by other routers on your network.
Update Interval	How often, in seconds, the Gateway sends routing-update messages. Default is 30 seconds.
Default Metric	Number by which the metric value for the path increases when the Gateway receives a routing update that includes changes to an entry. Choices are 1 – 15. Default is 1.
Authentication Type	The authentication mechanism used, if any. Choices are: <ul style="list-style-type: none"> • No Authentication = no authentication is used. If you keep this default setting, the Authentication Key & ID fields are gray and unavailable. (<i>default</i>) • Simple Password = an authentication method where a clear text password is sent to participating neighbors on the network. This selection sends the authenticating password over the network, possibly making it available to individuals who can access packets off the network. Do not use this option as part of your security strategy. Rather, use it to avoid accidental changes to the routing infrastructure. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the password. • MD5 = an authentication method that works much like Simple Password authentication, except that MD5 does not send the key over the network. Instead, a router uses the MD5 algorithm to produce a message digest of the key (also called a hash). The router sends the message digest instead of the key itself, which ensures that no one can eavesdrop on the network and learn keys during transmission. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the key and the second field becomes available for entering the ID.
Authentication Key & ID	Specify the appropriate information based on the Authentication Type selected: <ul style="list-style-type: none"> • No Authentication – no entry required; fields are gray and unavailable. (<i>default</i>) • Simple Password = in the first field, enter the clear-text password to be used for authentication. The second field requires no entry, and is gray and unavailable. • MD5 = in the first field, enter the MD5-hash password. In the second field, enter the Key Identifier that identifies the key used to create the authentication data for this message.

錯誤! 尚未定義樣式。

Neighbor	Enter the IP address of the Gateway's RIP neighbor router.
----------	--

OSPF Control Menu

OSPF is a router protocol used in larger autonomous system networks in preference to RIP, an older routing protocol that is installed in many of today's corporate networks. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network, so that all have the same routing table information. Unlike RIP, in which the entire routing table is sent, the host using OSPF sends only the part that has changed. With RIP, the routing table is sent to a neighbor host at a pre-determined interval. OSPF multicasts the updated information only when a change has taken place.

Using the OSPF Control menu, you can control how the Gateway uses OSPF. You can also add more than one OSPF area to the cable interface.

To access the OSPF Control menu, click **Routing** in the menu bar and then click the **OSPF Control** submenu. Figure 40 shows an example of the menu and Table 15 describes the options.

SMC Networks Gateway Setup

OSPF Control

This page allows the users to control the OSPF protocol which could be used to exchange the routing information between routers. The routing information could be used to build up/modify/age out the routes dynamically.

OSPF Control Table

Interface Name	Cable
OSPF Status	DISABLE
Network Type	Broadcast
Router Dead Interval	40 sec
Interface Cost	1 From 1 to 65535
Authentication Type	No Authentication
Authentication Key & ID	Key: [] ID: 1
Area ID for Cable	[][][][]

This table allows the users to add more than one Ospf area information to the cable interface

Additional OSPF area Table (up to 5 items)

#	Area ID	IP address	Subnet Mask	Default Cost for Area
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

HELP APPLY CANCEL

Figure 40. OSPF Control Menu

Table 15. OSPF Control Menu Options

Option	Description
Interface Name	A read-only field that shows the name of the interface.
OSPF Status	Enables or disables OSPF. <ul style="list-style-type: none"> • ENABLE = OSPF is enabled and the remaining fields on this menu, except Interface Name, become available. • DISABLE = OSPF is disabled. (<i>default</i>)
Network Type	The type of network on which OSPF will be used if OSPF is enabled. Choices are: <ul style="list-style-type: none"> • Broadcast = broadcast network. (<i>default</i>) • Not Broadcast = not broadcast network. • Point-to-Multipoint = point-to-multipoint network. • Point-to-Point = point-to-point network.
Router Dead Interval	Interval, in seconds, during which at least one hello packet must be received from a neighbor before the Gateway declares that a neighbor is down. Default is 40 seconds.
Interface Cost	Cost of sending a packet on an OSPF interface. Range is 1 – 65535. Default is 1.
Authentication Type	The authentication mechanism used, if any. Choices are: <ul style="list-style-type: none"> • No Authentication – no authentication is used. If you keep this default setting, the Authentication Key & ID fields are gray and unavailable. (<i>default</i>) • Simple Password = an authentication method where a clear text password is sent to participating neighbors on the network. This selection sends the authenticating password over the network, possibly making it available to individuals who can access packets off the network. Do not use this option as part of your security strategy. Rather, use it to avoid accidental changes to the routing infrastructure. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the password. • MD5 = an authentication method that works much like Simple Password authentication, except that MD5 does not send the key over the network. Instead, a router uses the MD5 algorithm to produce a message digest of the key (also called a hash). The router sends the message digest instead of the key itself, which ensures that no one can eavesdrop on the network and learn keys during transmission. If you select this setting, the first field in the Authentication Key & ID option becomes available for entering the key and the second field becomes available for entering the ID.
Authentication Key & ID	Specify the appropriate information based on the Authentication Type selected: <ul style="list-style-type: none"> • No Authentication – no entry required; fields are gray and unavailable. (<i>default</i>) • Simple Password = in the first field, enter the clear-text password to be used for authentication. The second field requires no entry, and is gray and unavailable. • MD5 = in the first field, enter the MD5-hash password. In the second field, enter the Key Identifier that identifies the key used to create the authentication data for this message.
Area ID for Cable	OSPF supports two-level hierarchical routing by using OSPF areas. This approach allows the routing table size, memory and CPU demands to be kept to a manageable levels. Each area is identified by 32-bit Area ID. This field allows the Gateway to associate packets to the appropriate OSPF area.

Adding OSPF Areas to the Cable Interface

To add OSPF areas to the cable interface:

1. In the OSPF Control menu, be sure **OSPF Status** is set to **ENABLE**. Otherwise, you will not be able to add OSPF areas to the cable interface.
2. Click the **Add** button below the **Additional OSPF area Table**. The Adding OSPF Area menu appears (see Figure 41).
3. Complete the fields in the Adding OSPF Area menu (see Table 16).
4. Click **Apply**. (Or click **Back** to return to the OSPF Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the OSPF area is added to the **Additional OSPF area Table**.
5. To configure additional OSPF area (up to 5), repeat steps 1 through 4. When you finish, click **Apply** in the OSPF Control menu to save your settings.
6. To change the settings for an OSPF area, click the radio button to the left of the OSPF area you want to change and click the **Edit** button. When the Adding OSPF Area menu appears, edit the settings as necessary (see Table 16) and click **Apply**.
7. To delete a predefined service, click the radio button to the left of the OSPF area you want to delete and click the **Delete** button. No precautionary message appears before you delete an OSPF area.
8. Click **Apply** on the OSPF Control menu.

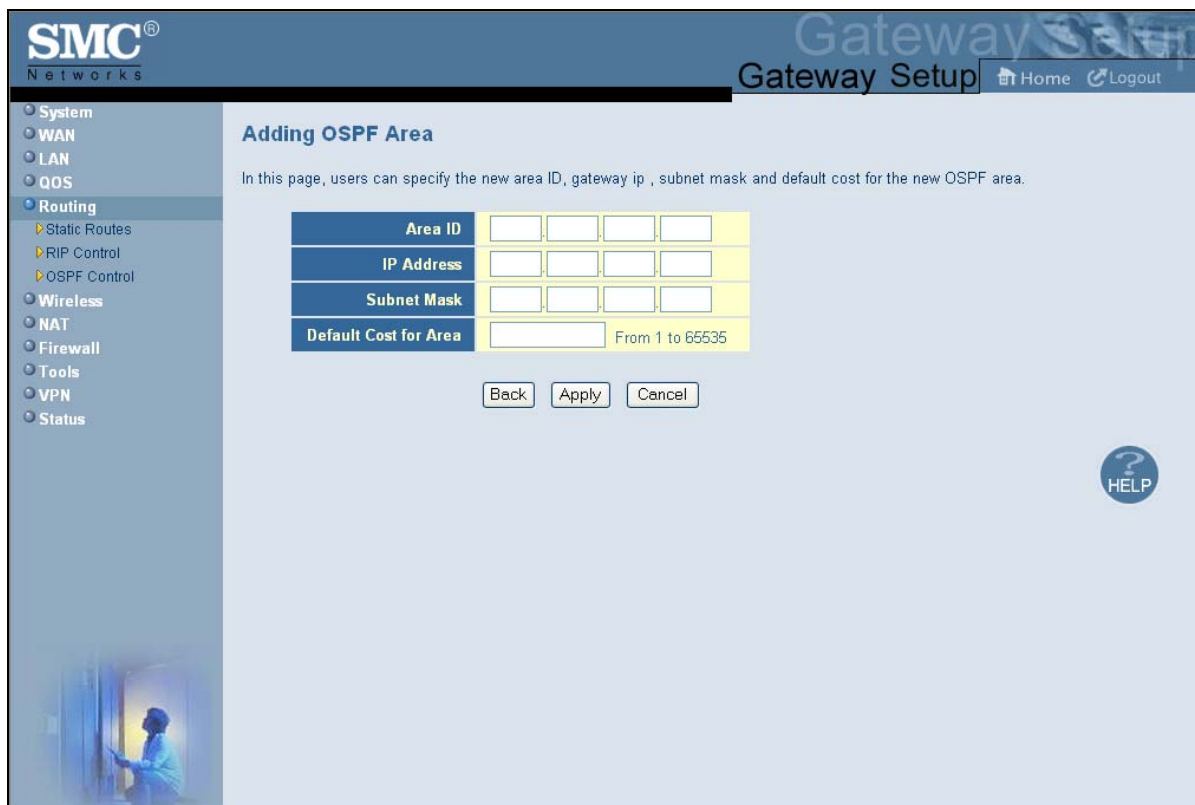


Figure 41. Adding OSPF Area Menu

Table 16. Adding OSPF Area Menu Options

Option	Description
Area ID	Area ID associated with the OSPF interface.
IP Address	IP address associated with the OSPF interface.
Subnet Mask	Subnet mask associated with the OSPF interface.
Default Cost for Area	Cost for sending a packet on the OSPF interface.

Wireless Basic Settings Menu

The Wireless Basic Settings menu lets you configure basic wireless settings, such as:

- Enabling or disabling the Gateway's wireless operation
- Selecting a wireless mode
- Configuring primary and multiple SSIDs
- Configuring channel settings

To access the Wireless Basic Settings menu, click **Wireless** in the menu bar. Figure 42 shows an example of the menu and Table 17 describes the settings you can select.

Wireless Basic Settings

The gateway can be quickly configured as a wireless access point for roaming clients by setting the access identifier and channel number. It also supports data encryption and client filtering. Users could also choose which mode would be run for this access point. There are 11b, 11g, 11n, or mixed mode. If necessary, users can also disable the wireless module by choosing from the **Wireless ON/OFF** drop-down menu.

Wireless ON/OFF	DISABLE			
Wireless Mode	11B/G/N Mixed			
SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID	SMCD3GN2-TWCE0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(2)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(3)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(4)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(5)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(6)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(7)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Multiple SSID(8)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Channel	11			

HELP APPLY CANCEL

Figure 42. Wireless Basic Settings Menu

Table 17. Wireless Basic Settings Menu Options

Option	Description
Wireless ON/OFF	<p>Enables or disables the Gateway's wireless operation.</p> <ul style="list-style-type: none"> • ENABLE = Gateway's wireless operation is active. Selecting this option activates the options in this menu. Clicking Apply displays the submenus below the Wireless menu. • DISABLE = Gateway's wireless operation is not active. Selecting this option deactivates the options in this menu. Clicking Apply hides the submenus below the Wireless menu. (<i>default</i>)
Wireless Mode	<p>If wireless operation is enabled for the Gateway, this option selects the wireless mode used by the Gateway. Choices are:</p> <ul style="list-style-type: none"> • 11B/G Mixed = use this setting if you have a combination of IEEE 802.11b and IEEE 802.11g devices on your network. • 11B Only = use this setting if you have only IEEE 802.11b devices on your network or want to limit your network to IEEE 802.11b devices. • 11G Only = use this setting if you have only IEEE 802.11g devices on your network or want to limit your network to IEEE 802.11g devices. • 11N Only = use this setting if you have only IEEE 802.11n devices on your network or want to limit your network to IEEE 802.11n devices. • 11G/N Mixed = use this setting if you have a combination of IEEE 802.11g and IEEE 802.11n devices on your network. • 11B/G/N Mixed = use this setting if you have a combination of IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n devices on your network. (<i>default</i>)
Primary/Multiple SSID settings	<p>SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alpha-numeric characters, which may be any keyboard character. Be sure these settings are the same for all devices in your wireless network. You can set up a primary SSID and seven additional SSIDs, designated Multiple SSID(2) through Multiple SSID(8). Each SSID can be hidden or configured for Wi-Fi Multimedia (WMM) mode. Each SSID, except the primary SSID, can also be configured to be in or out of service.</p> <ul style="list-style-type: none"> • Hidden = when checked, hides the SSID. Use this setting to block illegal connections. Users cannot reconnect automatically or manually to a wireless network that uses a hidden SSID. The wireless network that uses a hidden SSID does not appear in the Microsoft Windows Wireless Network Connection window. • In-service = when checked, broadcasts the Gateway's SSID. • WMM Mode = when checked, enables WMM. Enabling WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
Channel	<p>Select the appropriate channel from the list provided to correspond with your network settings, between 1 and 11 (in North America). Default is Auto, which selects the appropriate channel automatically. All devices in your wireless network must use the same channel to work properly.</p>

Wireless Encryption Settings Menu

Using the Wireless Encryption Settings menu, you can protect the data transmitted across your wireless network. The same encryption keys you specify here must also be configured on your other wireless client devices on your wireless network.

To access the Wireless Encryption Settings menu, click **Wireless** in the menu bar and then click the **Encryption** submenu. Figure 43 shows an example of the menu and Table 18 describes the settings you can select.



Note: The **Encryption** submenu is not available in the menu bar if wireless operation is disabled in the Wireless Basic Settings menu (see page 83).

SMC[®] Networks Gateway Setup Home Logout

Wireless Encryption Settings

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Commercial Wireless Gateway and wireless client devices to use encryption.

SSID	B2FFD0
Security Mode	WPA-Personal

WPA_Personal

WPA Mode	Auto (WPA-PSK or WPA2-PSK)
Cipher type	TKIP and AES
Group Key Update Interval	3600 (seconds)
Pre-shared Key	H2112516A961
Pre-Authentication	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

HELP APPLY CANCEL

Figure 43. Wireless Encryption Settings Menu

Table 18. Wireless Encryption Settings Menu Options

Option	Description
SSID	Network name of the primary wireless carrier. This field can be changed by administrators, but not by users.
Security Mode	<p>Selects the security mode used to protect transmissions across the wireless network.</p> <ul style="list-style-type: none"> • None = no security is used over the wireless network. • WEP = Wired Equivalency Privacy encryption is used over the wireless network. Select this option if your wireless adapters support WEP but not WPA-Personal. WEP provides basic security, but is not as secure as WPA-Personal. If you select WEP, select the options in Figure 44 and Table 19. • WPA-Personal = select this option if your wireless adapters support WPA-Personal. This encryption method is superior to WEP and offers two cipher types, TKIP and AES, with dynamic encryption keys. If you select WPA-Personal, select the options in <div data-bbox="537 653 1403 1230" style="border: 1px solid #ccc; padding: 10px;"> <h3 style="margin: 0;">Wireless Encryption Settings</h3> <p style="margin: 5px 0 0 20px;">Encryption transmits your data securely over the wireless network. Matching encryption keys must be configured on the Wireless Gateway and wireless client devices to use encryption.</p> <div style="margin: 10px 0 0 20px;"> <p>SSID <input type="text" value="B2FFD0"/></p> <p>Security Mode <input type="text" value="WPA-Personal"/></p> <h4 style="margin: 10px 0 0 20px;">WPA_Personal</h4> <p>WPA Mode <input type="text" value="Auto (WPA-PSK or WPA2-PSK)"/></p> <p>Cipher type <input type="text" value="TKIP and AES"/></p> <p>Group Key Update Interval <input type="text" value="3600"/> (seconds)</p> <p>Pre-shared Key <input type="text" value="H2112516A961"/></p> <p>Pre-Authentication <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> </div> </div> <ul style="list-style-type: none"> • Figure 45 and Table 20. (<i>default</i>)

Wireless Encryption Settings

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Commercial Wireless Gateway and wireless client devices to use encryption.

SSID	B2FFD0
Security Mode	WEP

WEP

WEP Key Length	64 bit (10 hex digits)	(length applies to all keys)
WEP Key 1	0000000000	
WEP Key 2	0000000000	
WEP Key 3	0000000000	
WEP Key 4	0000000000	
Default WEP Key	WEP Key 1	
Authentication	Open System	
Passphrase		<input type="button" value="Generate Keys"/>

Figure 44. WEP Options

Table 19. WEP Options

Option	Description
WEP Key Length	Level of WEP encryption applied to all WEP keys. Choices are 64-bit (10 hex digits) and 128-bit (26 hex digits).
WEP Key 1 – WEP Key 4	Fields for entering up to four WEP keys manually. Alternatively, you can click the Generate Keys button to generate these keys automatically.
Default WEP Key	Specifies which of the four WEP keys the Gateway is to use as its default.
Authentication	Authentication used. Choices are: <ul style="list-style-type: none"> • Open System = clients can only associate to the wireless access point using Open Option. (<i>default</i>) • Shared Key = all wireless stations share the same secret key. • Automatic = clients can associate to the wireless access point using Open System or Shared Key.
Passphrase	A sequence of words or text that can be used to automatically generate WEP keys. A passphrase can consist of from 8 to 63 ASCII characters. You can use upper-case, lower-case, and numeric characters to form your passphrase. A Generate Keys button next to this field lets the Gateway generate a passphrase based on the characters typed in this field.

Wireless Encryption Settings

Encryption transmits your data securely over the wireless network. Matching encryption keys must be setup on your Commercial Wireless Gateway and wireless client devices to use encryption.

SSID

Security Mode

WPA_Personal

WPA Mode

Cipher type

Group Key Update Interval (seconds)

Pre-shared Key

Pre-Authentication Disable Enable

Figure 45. WPA_Personal Options

Table 20. WPA_Personal Options

Option	Description
WPA Mode	Lets administrators select the WPA mode they want to use. Choices are: <ul style="list-style-type: none"> • WPA-PSK = select this setting if your access points and wireless clients support WPA-Pre-Shared Key (PSK) Authentication. • WPA2-PSK = select this setting if your access points and wireless clients support WPA2-PSK Authentication. • Auto (WPA-PSK or PWA2-PSK) = select this setting if your access points and wireless clients support either WPA-PSK or WPA2-PSK. <i>(default)</i>
Cipher type	Algorithm encryption to be used. Choices are: <ul style="list-style-type: none"> • TKIP = automatic encryption with WPA-PSK; requires pre-shared key. • AES = automatic encryption with WPA2-PSK; requires pre-shared key. • TKIP and AES = uses both TKIP and AES cipher types; requires pre-shared key. <i>(default)</i>
Group Key Update Interval	Number of seconds that instructs the Gateway how often it should change the encryption keys. Usually the security level is higher if you set the period shorter to change encryption keys more often. Default value is 3600 seconds (6 minutes). Type 0 to disable group key update interval.
Pre-shared Key	Shared secret between the Gateway and access points and wireless clients. Please check whether a default pre-shared key is required.
Pre-Authentication	Enables secure fast roaming, without noticeable signal latency. By default, this option is disabled.

WPS Setup

Using the WPS Setup menu, you can enable or disable WPS. WPS is a standard for easy and secure wireless network set up and connections.

The advantages of WPS are:

- WPS automatically configures the network name (SSID) and WPA security key for the Gateway and for the access point and wireless devices that join the network.
- You do not need to know the network name and security keys or passphrases to use WPS to join a wireless network.
- No one can guess your security keys or passphrase because they are generated randomly.
- WPS uses the Extensible Authentication Protocol (EAP), which is a strong authentication protocol used in WPA2.

The disadvantages of WPS are:

- Unless all the Wi-Fi devices on the network are WPS-compatible, you cannot take advantage of the ease of securing the network.
- Not all wireless equipment supports WPS.

- If your wireless devices do not support WPS, it can be hard to join a network that was set up with WPS because the wireless network name and security key are random sequences of letters and numbers.

To access the WPS Setup menu, click **Wireless** in the menu bar and then click the **WPS** submenu. Figure 46 shows an example of the menu. Using the **WPS Config** drop-down list, select the appropriate option to enable or disable WPS setup.

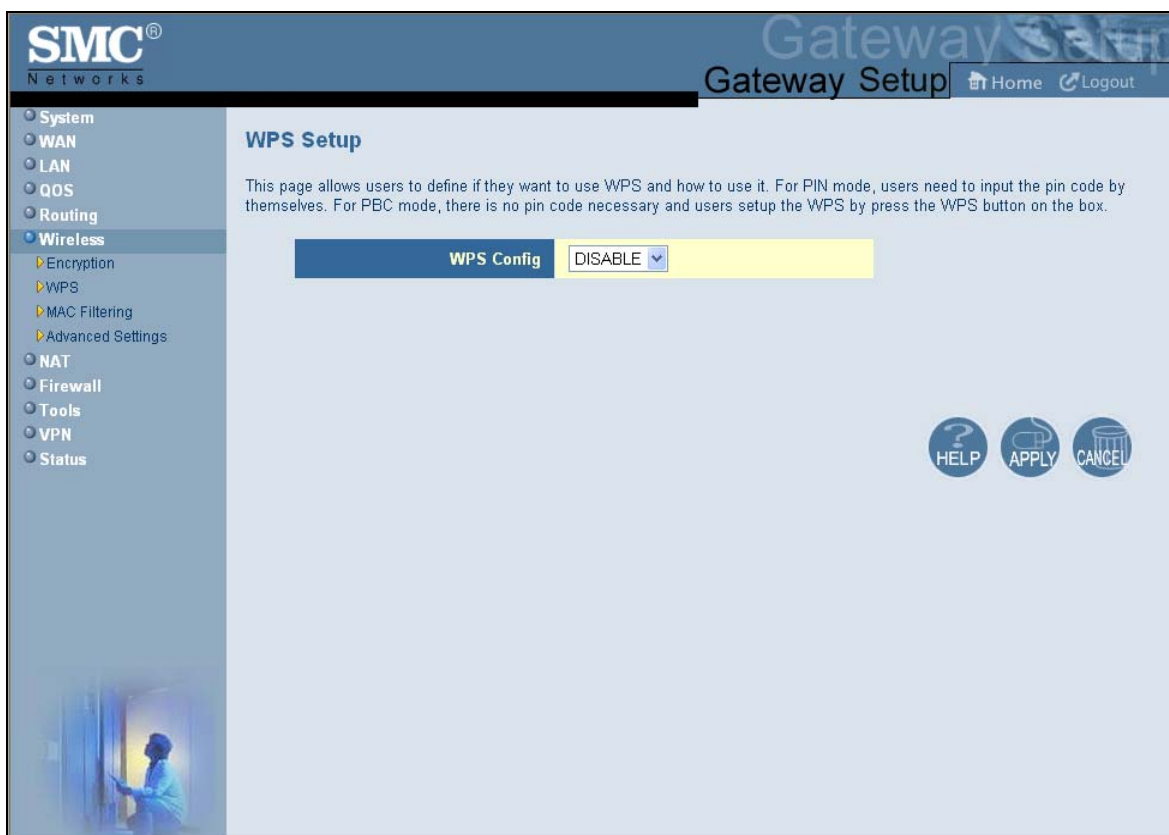


Figure 46. WPS Setup Menu

By default, WPS is disabled. If you select ENABLE and click Apply, the options in

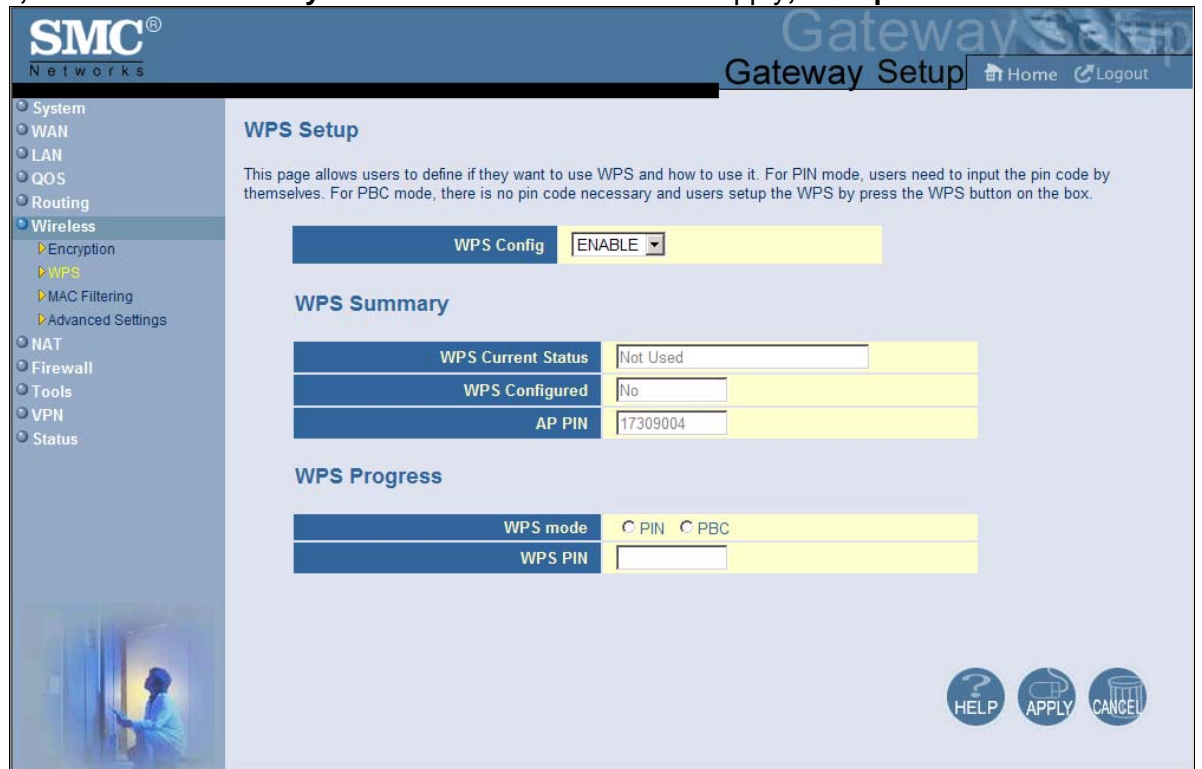


Figure 47 are displayed. Table 21 describes the options shown.

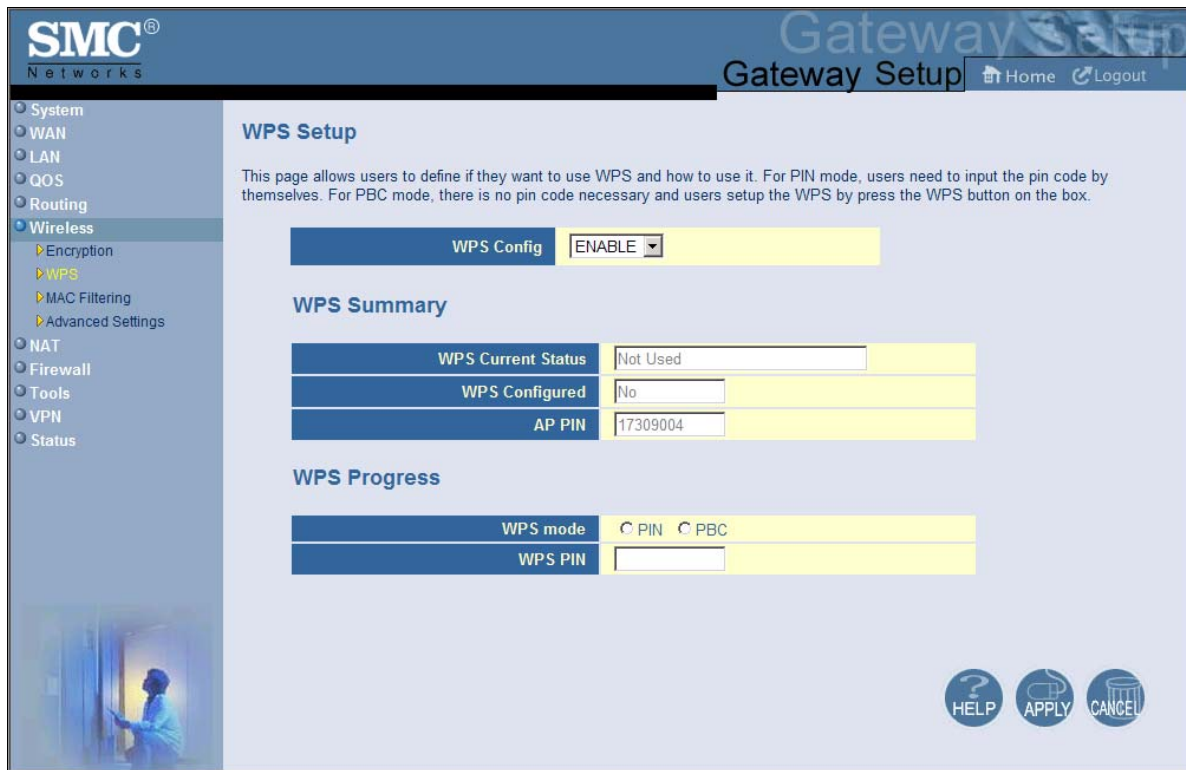


Figure 47. WPS Setup Menu with WPS Config Enabled

Table 21. WPS Summary and WPS Progress Options

Option	Description
WPS Config	Enables or disables the Gateway's WPS setup. <ul style="list-style-type: none"> • ENABLE = Gateway's WPS setup is available. (<i>default</i>) • DISABLE = Gateway's WPS setup is unavailable.
WPS Summary	
WPS Current Status	A read-only field that shows whether WPS is currently being used.
WPS Configured	A read-only field that whether WPS has been configured.
AP PIN	A read-only field that shows the personal identification number (PIN) for the access point.
WPS Progress	
WPS mode	Determines whether WPS can be configured using a PIN or the WPS button on the front panel of the Gateway. <ul style="list-style-type: none"> • PIN = requires users to enter a PIN in the WPS Setup menu to configure WPS. • PBC = Push Button Configuration. Allows users to use the WPS button on the front panel of the Gateway to configure WPS.
WPS PIN	If PIN was selected for WPS mode, enter the PIN that users must enter to enable WPS. The PIN must be 8 alpha-numeric characters long.

MAC Filtering

The MAC Filtering menu allows wireless client stations to connect over a wireless connection in two ways:

- By allowing all wireless station access.
- By allowing only trusted PCs.

To access the **MAC Filtering** menu, click **Wireless** in the menu bar and then click the **MAC Filtering** submenu.

The screenshot shows the SMC Networks Gateway Setup interface. The sidebar menu on the left includes System, WAN, LAN, QOS, Routing, Wireless (selected), NAT, Firewall, Tools, VPN, and Status. The 'Wireless' submenu is expanded, showing Encryption, WPS, MAC Filtering (selected), and Advanced Settings. The main content area is titled 'MAC Filtering' and contains the following elements:

- A header: 'The SMCD3GN3 can allow the wireless client stations to connect to your SMCD3GN3 in any of these ways:'
- Two dropdown menus: 'SSID' (set to B2FFD0) and 'MAC Filtering Mode' (set to Allow-All).
- A section titled 'Wireless Control List (up to 16 items)' with a table:

#	Device Name	MAC Address
Delete		
- A section titled 'Auto-Learned Wireless Devices' with a table:

Device Name	MAC Address
- A section titled 'Manually-Added Wireless Devices' with a table:

Device Name	MAC Address

 Below the table are 'Add' and 'Cancel' buttons.
- At the bottom right, there are three circular icons: HELP, APPLY, and CANCEL.

Figure 48 shows an example of the menu and Table 22 describes the settings you can select.



Note: The **MAC Filtering** submenu is not available in the menu bar if wireless operation is disabled in the Wireless Basic Settings menu (see page 83).

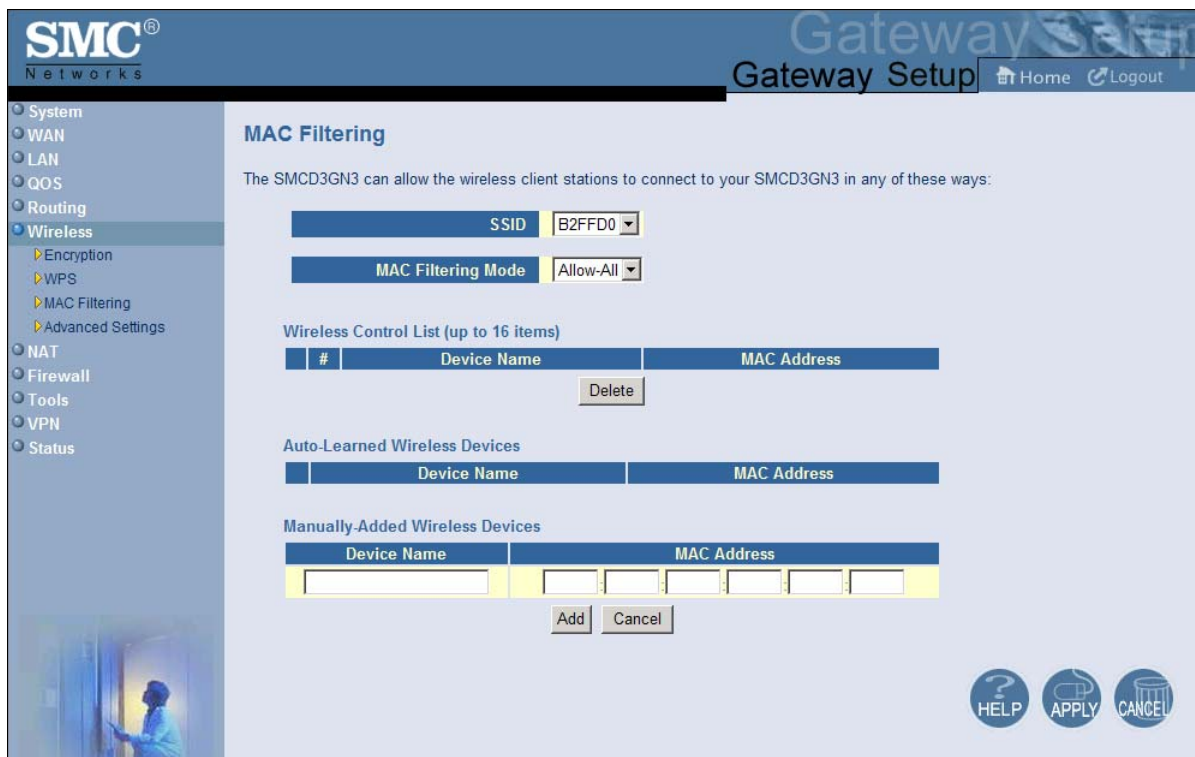


Figure 48. MAC Filtering Menu

Table 22. MAC Filtering Options

Option	Description
SSID	Network name of the primary wireless carrier.
MAC Filtering Mode	Determines which wireless client stations can connect to the Gateway. The choices are: <ul style="list-style-type: none"> • Allow- All = all wireless client stations can connect to the Gateway. (<i>default</i>) • Allow = allow only the wireless client stations in the MAC filter table to connect to the Gateway. • Deny = no wireless client stations can connect to the Gateway.
Wireless Control List	Shows the device name and MAC address of up to 16 devices that you manually added to the MAC filter table. To delete a device, click the radio button to the left of the device you want to delete and click the Delete button. A precautionary message does not appear before deleting the MAC address, so be sure you do not need the MAC address before deleting it.
Auto-Learned Wireless Devices	Shows the wireless devices whose presence the Gateway has automatically learned.
Manually-Added Wireless Devices	Enter a unique name and MAC address of the wireless devices that you want to manually add to the Wireless Control List (MAC filter table). Click Add to add the device to the Wireless Control List.

Adding and Deleting Wireless Client Stations

To allow wireless client stations to access the Internet through the Gateway, use the following procedure to define up to 16 wireless client stations.

- To add wireless client stations that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned Lan Devices**:
 - Click a wireless client station that the Gateway learned automatically.
 - Click **Add**. The wireless client station is added to the **Wireless Control List**.
 - To add more auto-learned wireless client stations (up to 16), repeat steps 1a and 1b.
- To manually add wireless client stations, perform the following steps under **Manually-Added Wireless Devices**:
 - Under **Device Name**, enter a unique name for the device (that is, a name that does not already appear in the **Wireless Control List**).
 - Under **MAC Address**, enter the MAC address of the device.
 - Click **Add** to add the wireless client station to the **Wireless Control List**.
 - To manually add more wireless client stations (up to 16), repeat steps 2a through 2c.
- To delete wireless client stations from the **Wireless Control List**, click the radio button corresponding to the wireless client station you want to delete and click the **Delete** button. A precautionary message does not appear before deleting a wireless client station.
- When you finish, click **Apply**.

Advanced Wireless Settings Menu

Using the Advanced Wireless Settings Filtering menu, you can configure advanced wireless settings for the Gateway.

To access the Advanced Wireless Settings menu, click Wireless in the menu bar and then click the Advanced Wireless Settings submenu.

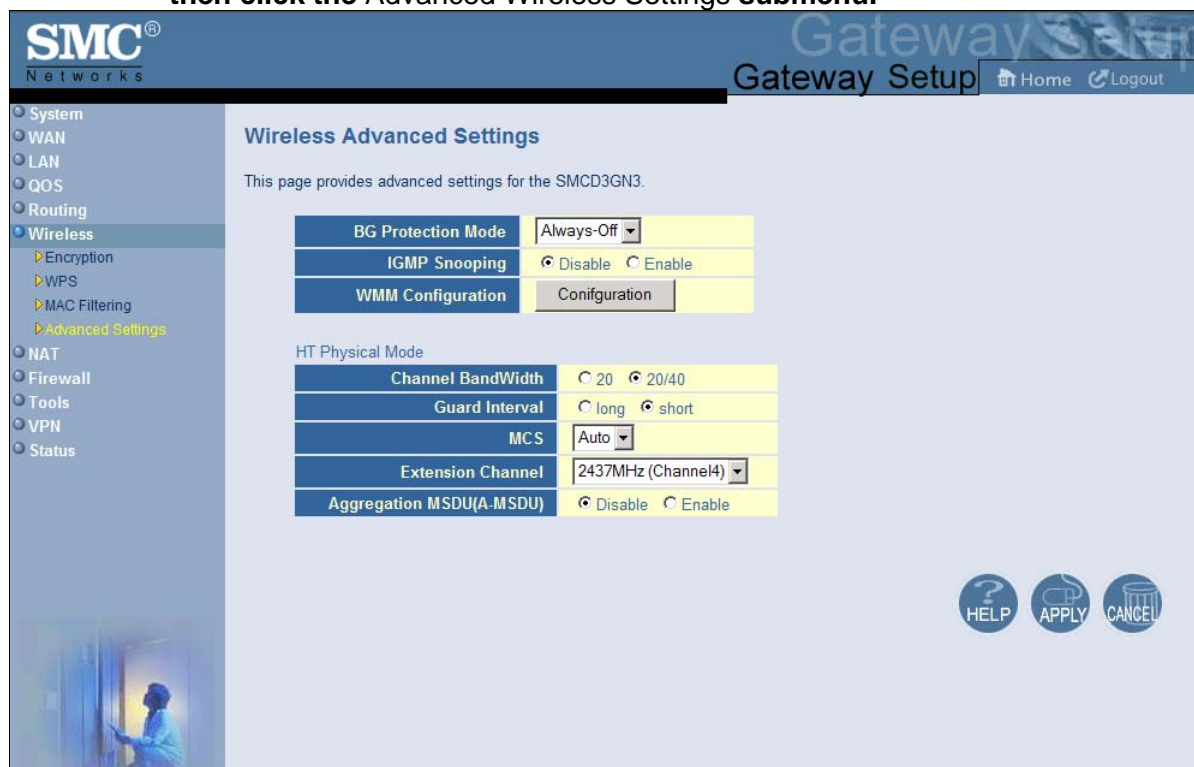


Figure 49 shows an example of the menu and Table 23 describes the settings you can select.



Note: The **Advanced Wireless Settings** submenu is not available in the menu bar if wireless operation is disabled in the Wireless Basic Settings menu (see page 83).

The screenshot displays the SMC Networks Gateway Setup web interface. The top navigation bar includes the SMC Networks logo, the title "Gateway Setup", and links for "Home" and "Logout". A left-hand sidebar menu lists various system settings: System, WAN, LAN, QOS, Routing, Wireless (selected), NAT, Firewall, Tools, VPN, and Status. The "Wireless" section is expanded to show sub-options: Encryption, WPS, MAC Filtering, and Advanced Settings (highlighted in yellow). The main content area is titled "Wireless Advanced Settings" and contains the following configuration options:

- BG Protection Mode:** Always-Off (dropdown)
- IGMP Snooping:** Disable Enable
- WMM Configuration:** Configuration (button)
- HT Physical Mode:**
 - Channel BandWidth:** 20 20/40
 - Guard Interval:** long short
 - MCS:** Auto (dropdown)
 - Extension Channel:** 2437MHz (Channel4) (dropdown)
 - Aggregation MSDU(A-MSDU):** Disable Enable

At the bottom right of the settings area, there are three circular buttons: HELP (with a question mark icon), APPLY (with a refresh icon), and CANCEL (with a trash can icon). A small image of a person in a white lab coat is visible in the bottom left corner of the interface.

Figure 49. Wireless Advanced Settings Menu

Table 23. Wireless Advanced Settings Options

Option	Description
BG Protection Mode	This mode is a protection mechanism that prevents collisions among 802.11b/g modes. Choices are: <ul style="list-style-type: none"> • Auto = BG protection mode goes on or off automatically as needed. • Always-On = BG protection mode is always on. • Always-Off = BG protection mode is always off. (<i>default</i>)
IGMP Snooping	Enables or disables the Gateway from forwarding multicast traffic intelligently. <ul style="list-style-type: none"> • Enable = Gateway listens to IGMP membership reports, queries, and leave messages to identify the Gateway ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group or groups. • Disable = Gateway does not analyze all IGMP packets. (<i>default</i>)
WMM Configuration	Displays a screen for selecting WMM settings for your wireless access point(s).
HT Physical Mode	
Operating Mode	Lets you select between Mixed Mode and Green Field. <ul style="list-style-type: none"> • Mixed Mode = provides backward compatibility with IEEE 802.11n/a/g/b devices. (<i>default</i>) • Green Field = used for pure network of 802.11n access points and clients, taking full advantage of the high-throughput capabilities of the 11n MIMO architecture
Channel BandWidth	Select a channel bandwidth of 20 or 20/40. <ul style="list-style-type: none"> • 20 = allows only single-channel operation (e.g., 20 MHz). • 20/40 = allows both single channel operation (20 MHz) and the wider bandwidth operation (40 MHz) by using two or more adjacent (contiguous channels). A 20/40 BSS is a wireless network that allows a wider bandwidth operation mode. (<i>default</i>)
Guard Interval	The guard interval is the period in nanoseconds that the Gateway listens between packets. Choices are: <ul style="list-style-type: none"> • Long = 800 ns guard interval. • Short = 400 ns guard interval (<i>default</i>)
MCS	Modulation Coding Scheme (MCS) is a specification of PHY parameters consisting of modulation order (BPSK, QPSK, 16-QAM, 64-QAM) and FEC code rate (1/2, 2/3, 3/4, 5/6). MCS is used in the Gateway to define 32 symmetrical settings. MCS provides for potentially greater throughput. High throughput data rates are a function of MCS, bandwidth, and guard interval. Default is auto.
Extension Channel	Defines a second 20-MHz channel. 40-MHz stations can use this channel in addition to using the control channel simultaneously.
Aggregation MSDU(A_MSDU)	Enables or disables aggregation of multiple MSDUs in one MPDU. Default is disable.

NAT Settings

Using the NAT Settings menu, you can enable the Gateway's Network Address Translation (NAT) table and allow multiple users at your local site to access the Internet. To access the NAT Settings menu, click **NAT** in the menu bar. Figure 50 shows an example of the menu. By default, the Gateway's NAT module is enabled. To disable it, uncheck **Enable NAT Module** and click **Apply**. To enable it, check **Enable NAT Module** and click **Apply**.

If you enable the Gateway's NAT module, the following submenus appear under **NAT** in the menu bar:

- **Port Forwarding** - lets you configure the Gateway to provide port-forwarding services that let Internet users access predefined services. See page 96.
- **1-to-1 Mapping** - lets you use the NAT to perform 1-to-1 mapping between global IP addresses on the cable modem WAN interface and the private IP address on the LAN. See page 102.



Note: If you change this setting, the Gateway reboots automatically.

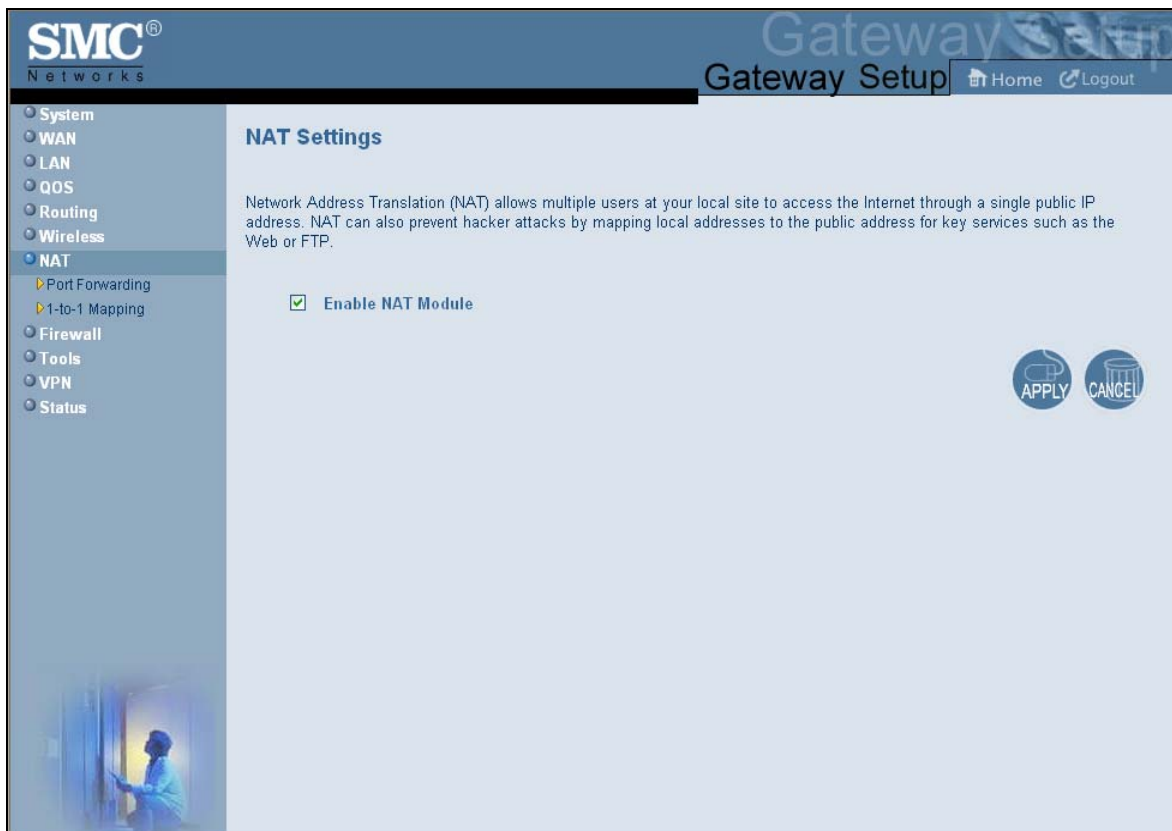


Figure 50. NAT Settings Menu

Port Forwarding Menu

The Port Forwarding menu lets you configure the Gateway to provide port-forwarding services that let Internet users access predefined services such as HTTP (80), FTP (20/21), and AIM/ICQ (5190) as well as custom-defined services. You perform port forwarding by redirecting the WAN IP address and the service port to the local IP address and service port. You can configure a maximum of 100 predefined and custom-defined services.

To access the Port Forwarding menu, click **NAT** in the menu bar and then click the **Port Forwarding** submenu in the menu bar. Figure 51 shows an example of the menu.

SMC Networks Gateway Setup Home Logout

Port Forwarding

Users can configure the SMCD3GN3 to provide the port forwarding services which allow the Internet users to access local services such as the Web server or FTP server at your local site. This is done by redirecting the combination of the WAN IP address and the service port to the local private IP and its service port. The maximum total number allowed for predefined and customer-defined services is 100.

Disable Port Forwarding Function

Predefined Service Table

#	Service Name	LAN Server IP	Remote IPs	Active
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

Customer Defined Service Table

#	Service Name	Type	LAN Server IP	Remote IPs	Public Port	Private Port	Active
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

Figure 51. Port Forwarding Menu

Adding Predefined Services

Using the following procedure, you can select well-known services and specify the LAN host IP address(es) that will provide the service to the Internet.

1. In the Port Forwarding menu, be sure **Disable Port Forwarding Function** is not checked (unchecked is the default setting).
2. Click the **Add** button below the **Predefined Service Table**. The Predefined Service menu appears (see Figure 52).
3. Complete the fields in the Predefined Service menu (see Table 24).
4. Click **Apply**. (Or click **Back** to return to the Port Forwarding menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the predefined service is added to the **Predefined Service Table**.
5. To configure additional predefined services (up to 100, including customer-defined services), repeat steps 1 through 3.
6. To change the settings for a predefined service, click the radio button to the left of the service you want to change and click the **Edit** button. When the Predefined Service menu appears, edit the settings as necessary (see Table 24) and click **Apply**.
7. To delete a predefined service, click the radio button to the left of the service you want to delete and click the **Delete** button. No precautionary message appears before you delete a predefined service.

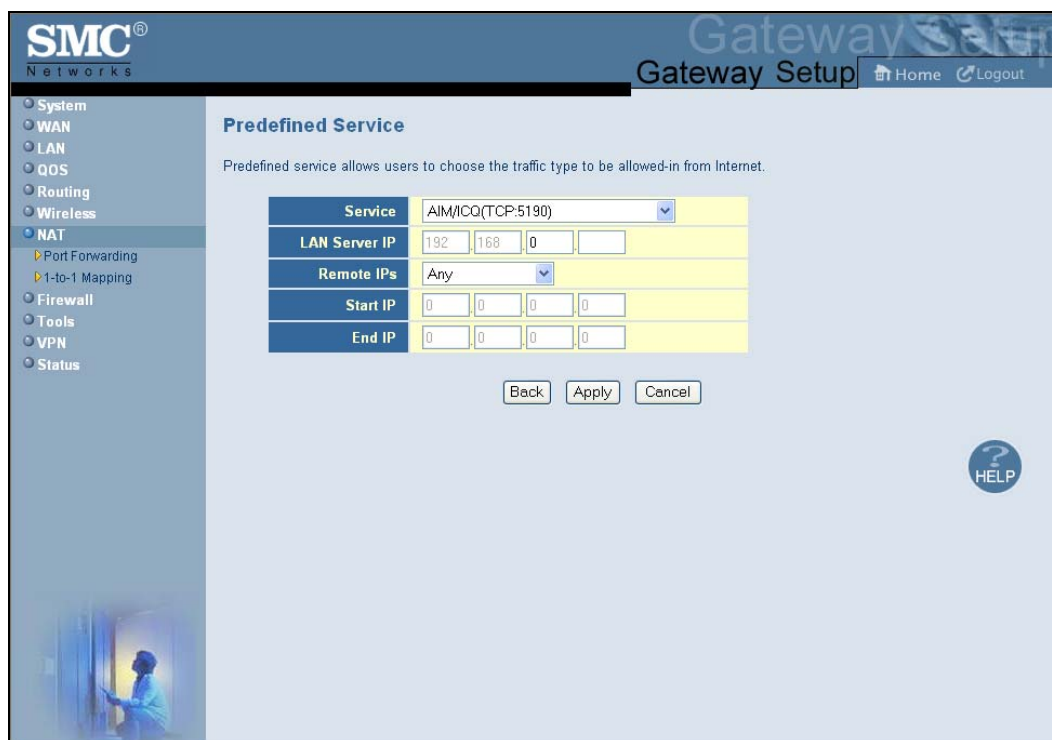


Figure 52. Predefined Service Menu

Table 24. Predefined Service Menu Options

Option	Description
Service	List of predefined services from which you can choose.
LAN Server IP	IP address of the LAN PC or server that is running the service.
Remote IPs	Forwards the service to any remote IP address, one remote IP address, or a range of remote IP addresses. <ul style="list-style-type: none"> • If you select one remote IP address, enter the IP address in the Start IP field. • If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To forward to: <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any remote IP addresses.
End IP	Enter the ending IP address in the remote IP address range. This field is unavailable if the Gateway is configured for any remote IP addresses or for a single remote IP address.

Adding Customer-Defined Services

Using the following procedure, you can define special application services you want to provide to the Internet. The following example shows how to set port forwarding for a Web server on an Internet connection, where port 80 is blocked from the WAN side, but port 8000 is available.

Name:	Web Server
Type:	TCP
LAN Server IP:	192.168.0.100
Remote IPs:	Any (allow access to any public IP)
Public Port:	8000
Private Port:	80

With this configuration, all HTTP (Web) TCP traffic on port 8000 from any IP address on the WAN side is redirected through the firewall to the Internal Server with the IP address 192.168.0.100 on port 80.

To create your own customized services:

1. In the Port Forwarding menu, be sure **Disable Port Forwarding Function** is not checked (unchecked is the default setting).
2. Click the **Add** button below the **Customer Defined Service Table**. The Customer Defined Service menu appears (see Figure 53).
3. Complete the fields in the Customer Defined Service menu (see Table 25).
4. Click **Apply**. (Or click **Back** to return to the Port Forwarding menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the customer-defined service is added to the **Customer Defined Service Table**.
5. To configure additional customer-defined services (up to 100, including predefined services), repeat steps 1 through 3.
6. To change the settings for a customer-defined service, click the radio button to the left of the service you want to change and click the **Edit** button. When the Customer Defined Service menu appears, edit the settings as necessary (see Table 25) and click **Apply**.
7. To delete a customer-defined service, click the radio button to the left of the service you want to delete and click the **Delete** button. No precautionary message appears before you delete a customized service.



Figure 53. Customer Defined Service Menu

Table 25. Customer Defined Service Page Options

Option	Description
Name	Name for identifying the custom service. The name is for reference purposes only.
Type	The type of protocol. Choices are TCP, UDP, and TCP/UDP. Default is TCP.
LAN Server IP	IP address of the LAN PC or server that is running the service.
Remote IPs	Forwards the service to any remote IP address, one remote IP address, or a range of remote IP addresses. <ul style="list-style-type: none"> If you select one remote IP address, enter the IP address in the Start IP field. If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To specify: <ul style="list-style-type: none"> A single remote IP address, enter the remote IP address. A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any remote IP addresses.
End IP	Ending IP address in the remote IP address range. This field is unavailable if the Gateway is configured for any remote IP addresses or a single remote IP address.
Public IP Ports	A single public IP port or a range of public IP ports on which the service is provided. If necessary, contact the application vendor for this information. <ul style="list-style-type: none"> If you select a single public port, enter the port number in the Start Public Port field. If you select a range of public ports, enter the starting port number in the Start Public Port field and the ending port number in the End Public Port field.
Start Public Port	Starting number of the port on which the service is provided.
End Public Port	Ending number of the port on which the service is provided. This field is unavailable if the Gateway is configured for a single public IP port.
Private Ports	Numbers of the ports whose traffic the Gateway forwards to the LAN. If there is a range of ports, enter the starting private port here and check Enable Port Range . The Gateway automatically calculates the end private port. The LAN PC server listens for traffic/data on this port (or these ports).

1-to-1 Mapping Menu

Using the 1-to-1 Mapping menu, you can use the NAT to perform 1-to-1 mapping between global IP addresses on the cable modem WAN interface and the private IP address on the LAN.

To access the 1-to-1 Mapping menu, click NAT in the menu bar and then click the 1-to-1 Mapping submenu.

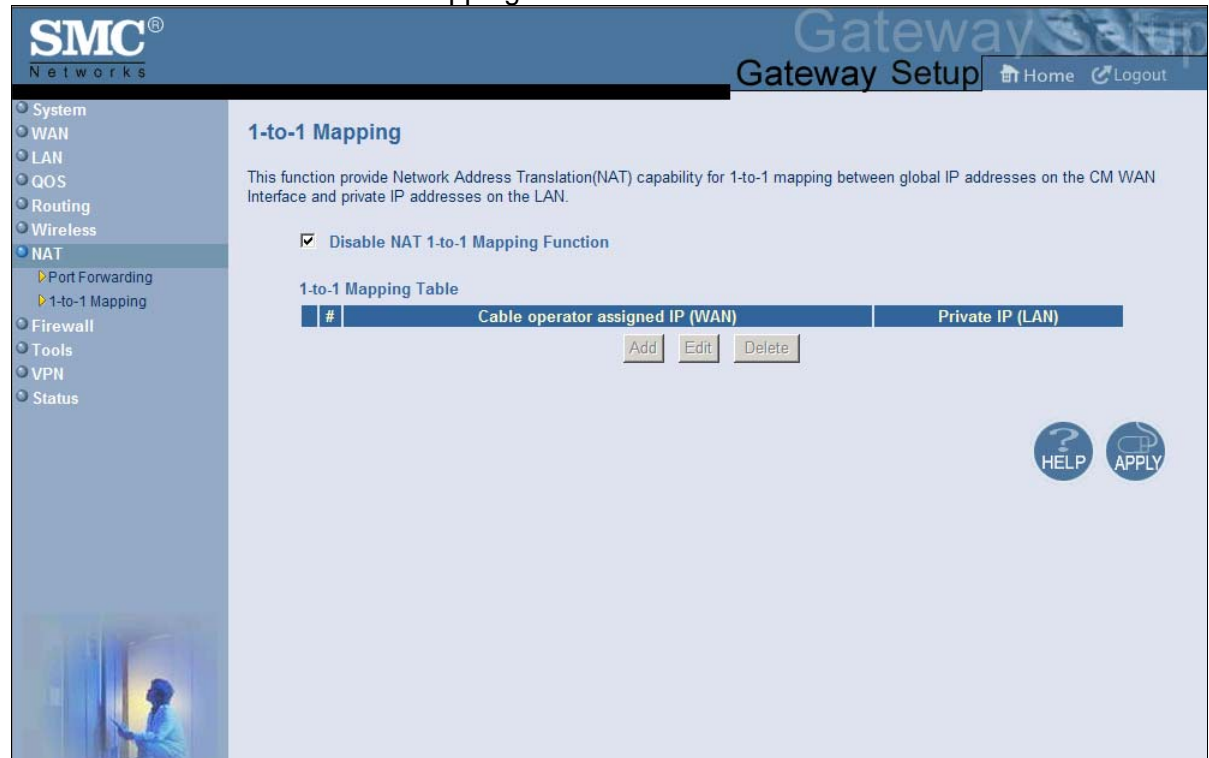


Figure 54 shows an example of the menu. By default, 1-to-1 mapping is disabled. To enable it, uncheck **Disable NAT 1-to-1 Mapping Function** and click **Apply**. To disable it, check **Disable NAT 1-to-1 Mapping Function** and click **Apply**.



Note: The **1-to-1 Mapping** submenu is not available in the menu bar if **Enable NAT Module** is not checked in the NAT Settings menu (see page 91).



Figure 54. 1-to-1 Mapping Menu

If you enable (uncheck) NAT 1-to-1 mapping, use the following procedure to define the mapping between global IP addresses on the cable modem WAN interface and the private IP address on the LAN.

1. In the 1-to-1 Mapping menu, uncheck **Disable NAT 1-to-1 Mapping Function** if it is selected.
2. Click the **Add** button below **1-to-1 Mapping Table**. The Adding NAT 1-to-1 Mapping Entry menu appears (see Figure 55).
3. Complete the fields in the Predefined Service menu (see Table 26).
4. Click **Apply**. (Or click **Back** to return to the 1-to-1 Mapping menu or click **Cancel** to cancel any selections you made.) If you clicked **Apply**, the mapping is added to the **1-to-1 Mapping Table**.
5. To configure additional mappings, repeat steps 1 through 3. When you finish, click **Apply** in the 1-to-1 Mapping menu to save your settings.
6. To change the settings for a mapping, click the radio button to the left of the mapping you want to change and click the **Edit** button. When the Adding NAT 1-to-1 Mapping Entry

menu appears, edit the settings as necessary (see Table 26) and click **Apply**. Click **Apply** in the 1-to-1 Mapping menu to save your settings.

7. To delete a mapping, click the radio button to the left of the mapping you want to delete and click the **Delete** button. No precautionary message appears before you delete a mapping.
8. Click **Apply** in the 1-to-1 Mapping menu to save your settings.

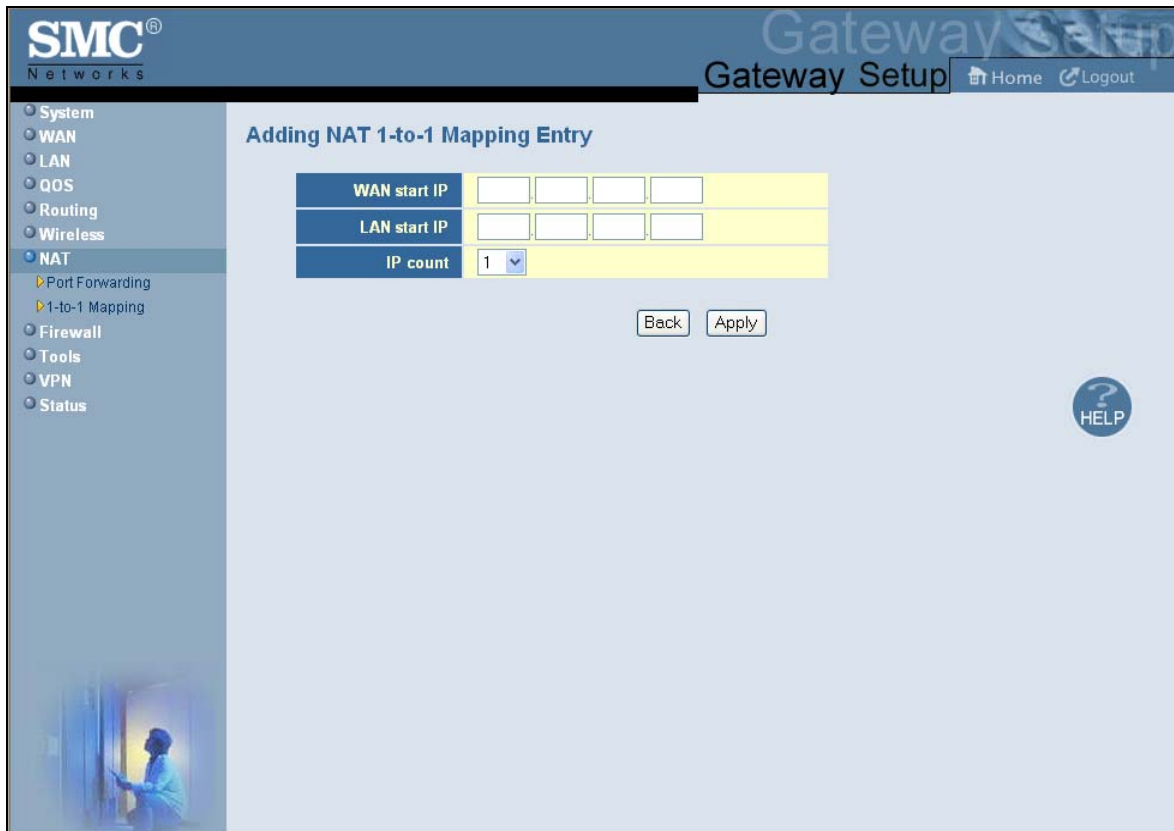


Figure 55. Adding NAT 1-to-1 Mapping Entry

Table 26. Adding NAT 1-to-1 Mapping Entry Options

Option	Description
WAN start IP	Starting range of the IP addresses on the WAN that are to be mapped.
LAN start IP	Starting range of the IP addresses on the LAN that are to be mapped.
IP count	Count of the IP addresses to be mapped. Default is 1.

Security Settings (Firewall) Menu

The Security Settings (Firewall) menu lets you enable or disable the Gateway's firewall.

If you enable the Gateway firewall module, the following submenus appear in the menu bar:

- Configure access control settings — see page 107
- Configure the Gateway for special applications — see page 108
- Set up URL blocking — see page 122
- Schedule routes — see page 124
- Receive email or syslog alert notifications — see page 125
- Configure a local client computer as a local DMZ for unrestricted two-way Internet access — see page 129

Enabling or Disabling Firewall

The Security Settings (Firewall) menu provides an option for enabling or disabling the Gateway's firewall setting. To access the Security Settings (Firewall) menu, click Firewall in the menu bar.



Figure 56 shows an example of the menu.

By default, the Gateway's firewall settings are enabled. To disable the firewall, uncheck **Enable Firewall Module** and click **Apply**. Disabling the firewall hides the submenus below the **Firewall** menu.

The Security Settings (Firewall) menu also provides an option for enabling or disabling the Session Initiation Protocol (SIP) application-layer gateway service on the Gateway firewall. This option allows SIP signaling requests to traverse directly through the Gateway to the destination device.



Figure 56. Security Settings (Firewall) Menu

Configuring Access Control

The Access Control menu lets you enable access control to block traffic at the Gateway's LAN interfaces from accessing the Internet.

To access the Access Control menu, click **Firewall** in the menu bar and then click the **Access Control** submenu in the menu bar.



Note: The **Access Control** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).

By default, the Gateway does not block attempts to access the LAN from the Internet. To enable access control, check **Enable Access Control** if it is unchecked and click **Apply**. When Access Control is enabled, you can configure up to 35 predefined and customer-defined filtering tables.

SMC Networks Gateway Setup

System
WAN
LAN
QOS
Routing
Wireless
NAT
Firewall
 Access Control
 Special Application
 URL Blocking
 Schedule Rule
 Email/Syslog Alert
 DMZ
Tools
VPN
Status

Access Control

By default all access attempts from the Internet to the LAN are blocked. In the NAT section, port forwarding rules can be setup to allow access from the Internet to the Private LAN. Here in this Service Table section, access rules can be setup to allow access from the Internet to the Public LAN. The maximum total number allowed for predefined and customer defined access rules is 35.

Enable Access Control

Predefined Service Table

#	Service Name	Remote IPs	Local IPs	Allowed
Add Edit Delete				

Customer Defined Service Table

#	Service Name	Type	Remote IPs	Local IPs	Port	Allowed
Add Edit Delete						

The following two Filtering Tables allow users to define the traffic type not permitted from LAN to the Internet. The maximum total number allowed for predefined and customer defined filters is 35.

Predefined Filtering Table

#	Service Name	LAN IPs	Blocked
Add Edit Delete			

Customer Defined Filtering Table

#	Service Name	Type	Remote IPs	Local IPs	Port	Allowed
Add Edit Delete						

The following two Filtering Tables allow users to define the traffic type not permitted from LAN to the Internet. The maximum total number allowed for predefined and customer defined filters is 35.

Predefined Filtering Table

#	Service Name	LAN IPs	Blocked
Add Edit Delete			

Customer Defined Filtering Table

#	Service Name	Type	Remote IPs	Local IPs	Port	Blocked
Add Edit Delete						

Respond to Ping on Internet WAN Port

Respond to Ping on Public LAN Port

HELP APPLY CANCEL

Figure 57. Access Control Menu

Adding Predefined Access Rules

Using the following procedure, you can select a well-known service and specify whether to block all LAN hosts, a single LAN host, or a range of LAN hosts.

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Predefined Service Table**, click the **Add** button. The Predefined Access Rules menu appears (see Figure 58).
3. Complete the fields in the Predefined Access Rules menu (see Table 27).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the rule for the predefined access rule is added to the **Predefined Service Table**.
5. To configure additional access control rules for predefined services (up to 35, including access rules for customer-defined services), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the rule for a predefined rule, click the radio button to the left of the rule you want to change and click the **Edit** button. When the Predefined Access Rules menu appears, edit the settings as necessary (see Table 27) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a predefined rule, click the radio button to the left of the rule you want to delete and click the **Delete** button. No precautionary message appears before you delete a rule. Click **Apply** in the Access Control menu to save your settings.

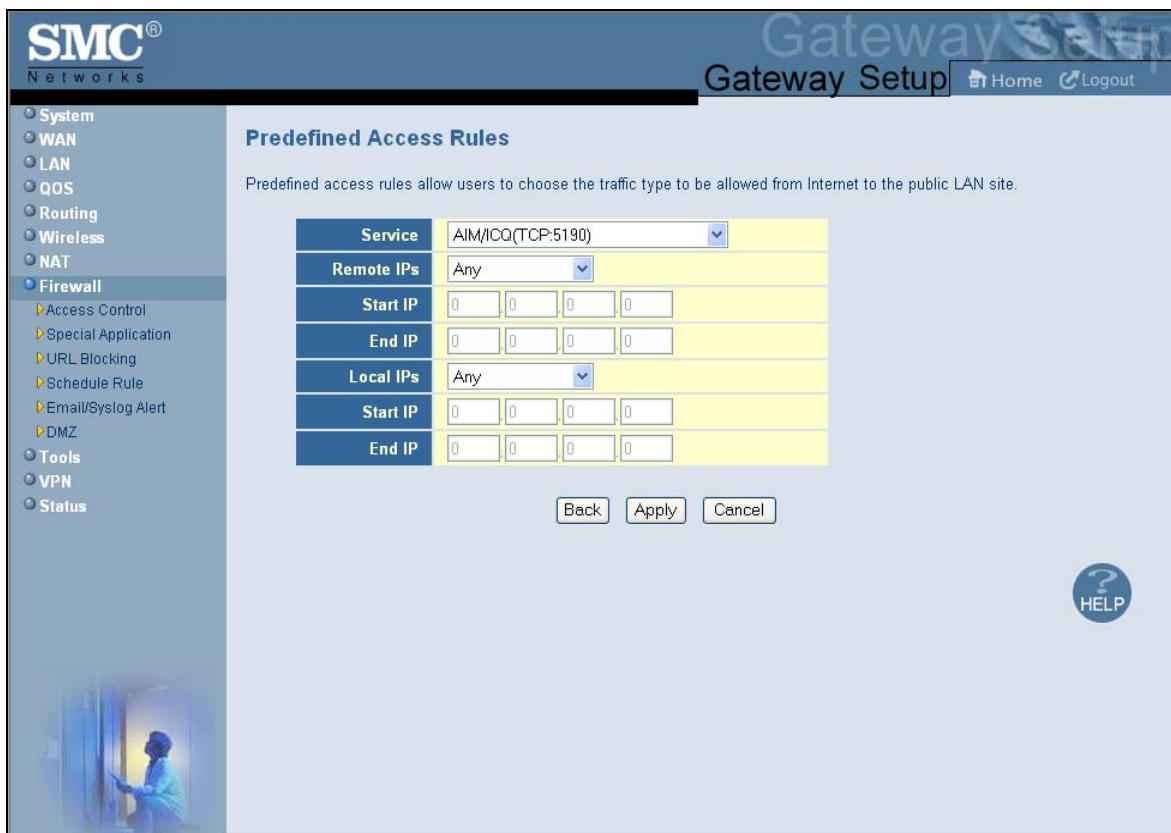


Figure 58. Predefined Access Rules Menu

Table 27. Predefined Access Rules Menu Options

Option	Description
Service	List of predefined services from which you can choose.
Remote IPs	<p>Allows access to any remote IP address, one remote IP address, or a range of remote IP addresses.</p> <ul style="list-style-type: none"> • If you select one remote IP address, enter the IP address in the Start IP field. • If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To forward to:</p> <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if the Gateway is configured for any remote IP addresses.</p>
End IP	Enter the ending IP address in the remote IP address range. This field is unavailable if the Gateway is configured for any remote IP addresses or for a single remote IP address.
Local IPs	<p>Lets you specify any local IP addresses, a single local IP address, or a range of local IP addresses to which the access rule is applied.</p> <ul style="list-style-type: none"> • If you select one local IP address, enter the IP address in the Start IP field. • If you select a range of local IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	<p>To apply the predefined access rule to:</p> <ul style="list-style-type: none"> • A single local IP address, enter the local IP address. • A range of local IP addresses, enter the starting IP address here and the ending IP address range in the next field. <p>This field is unavailable if the Gateway is configured for any local IP addresses.</p>
End IP	Ending IP address in the local IP address range to which the access rule will be applied. This field is unavailable if the Gateway is configured for any local IP address or a single local IP address.

Adding Customer-Defined Access Rules

Using the following procedure, you can define your own rules regarding the type of traffic allowed from the Internet to the public LAN site.

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Customer Defined Service Table**, click the **Add** button. The Customer Defined Access Rules menu appears (see Figure 59).
3. Complete the fields in the Customer Defined Access Rules menu (see Table 28).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the rule for the customer-defined rule is added to the **Customer Defined Service Table**.
5. To configure additional access control rules for customer-defined services (up to 35, including access rules for predefined services), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the rule for a customer-defined service, click the radio button to the left of the rule you want to change and click the **Edit** button. When the Customer-Defined Access Rules menu appears, edit the settings as necessary (see Table 28) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a customer-defined rule, click the radio button to the left of the rule you want to delete and click the **Delete** button. No precautionary message appears before you delete a rule. Click **Apply** in the Access Control menu to save your settings.

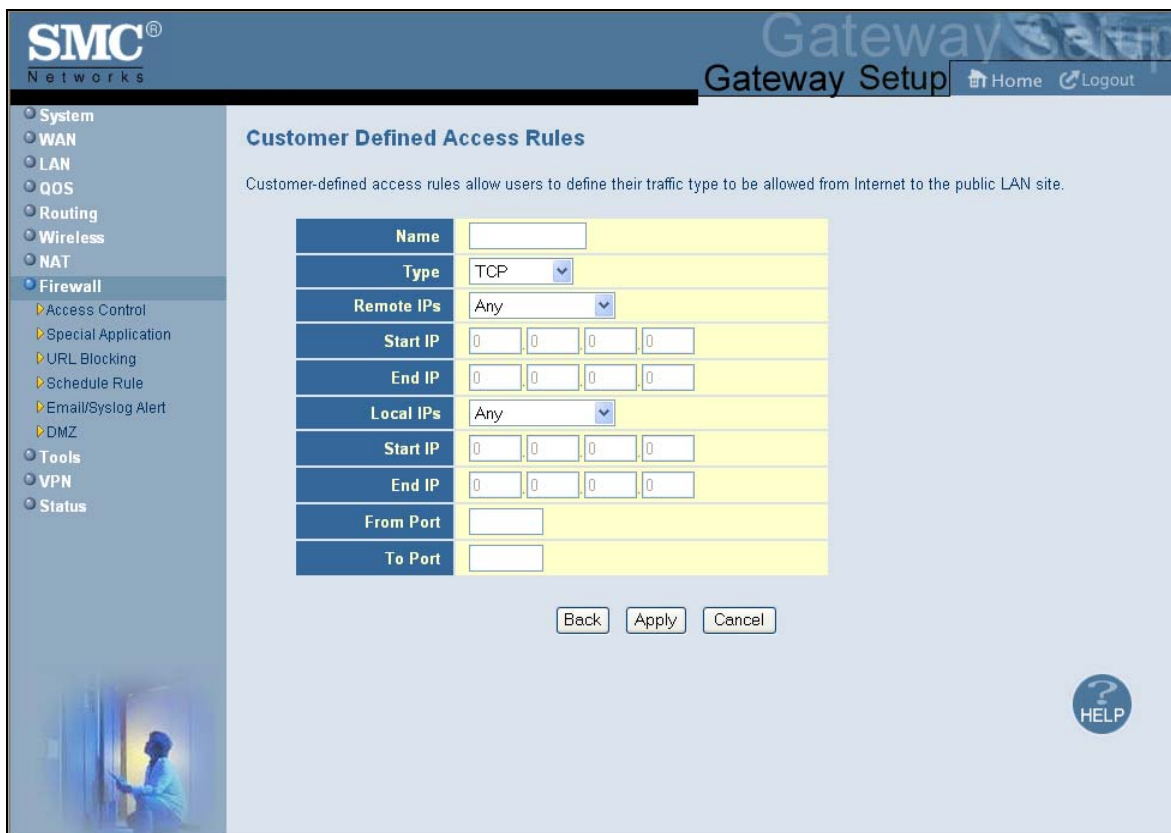


Figure 59. Customer Defined Access Rules Menu

Table 28. Customer Defined Access Rules Menu Options

Option	Description
Name	Name for identifying the custom service. The name is for reference purposes only.
Type	The type of protocol you want to access rule. Choices are TCP, UDP, and TCP/UDP. Default is TCP.
Remote IPs	Lets you apply the access rule to any remote IP addresses, a single remote IP address, or a range of remote IP addresses. <ul style="list-style-type: none"> • If you select one remote IP address, enter the IP address in the Start IP field. • If you select a range of remote IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To specify: <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any remote IP addresses.
End IP	Ending IP address in the LAN IP address range to which the access rule will be applied. This field is unavailable if the Gateway is configured for any LAN IP address or a single LAN IP address.
Local IPs	Lets you specify any local IP addresses, a single local IP address, or a range of local IP addresses to which the access rule is applied. <ul style="list-style-type: none"> • If you select one local IP address, enter the IP address in the Start IP field. • If you select a range of local IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To apply the predefined access rule to: <ul style="list-style-type: none"> • A single local IP address, enter the local IP address. • A range of local IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any local IP addresses.
End IP	Ending IP address in the local IP address range to which the access rule will be applied. This field is unavailable if the Gateway is configured for any local IP address or a single local IP address.
From Port	Starting port number on which the access rule will be applied. If necessary, contact the application vendor for this information.
To Port	Ending port number on which the access rule will be applied. If necessary, contact the application vendor for this information.

Adding Predefined Filters

Using the following procedure, you can add predefined filters that block certain types of traffic from the LAN side of the Gateway to the Internet side of the Gateway .

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Predefined Filtering Table**, click the **Add** button. The Predefined Filter menu appears (see Figure 60).
3. Complete the fields in the Predefined Filter menu (see Table 29).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the predefined filter is added to the **Predefined Filtering Table**.
5. To define additional filters for access control (up to 35, including customer-defined filters), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the settings for a predefined filter, click the radio button to the left of the service you want to change and click the **Edit** button. When the Predefined Filter menu appears, edit the settings as necessary (see Table 29) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a predefined filter, click the radio button to the left of the filter you want to delete and click the **Delete** button. No precautionary message appears before you delete a predefined filter. Click **Apply** in the Access Control menu to save your settings.

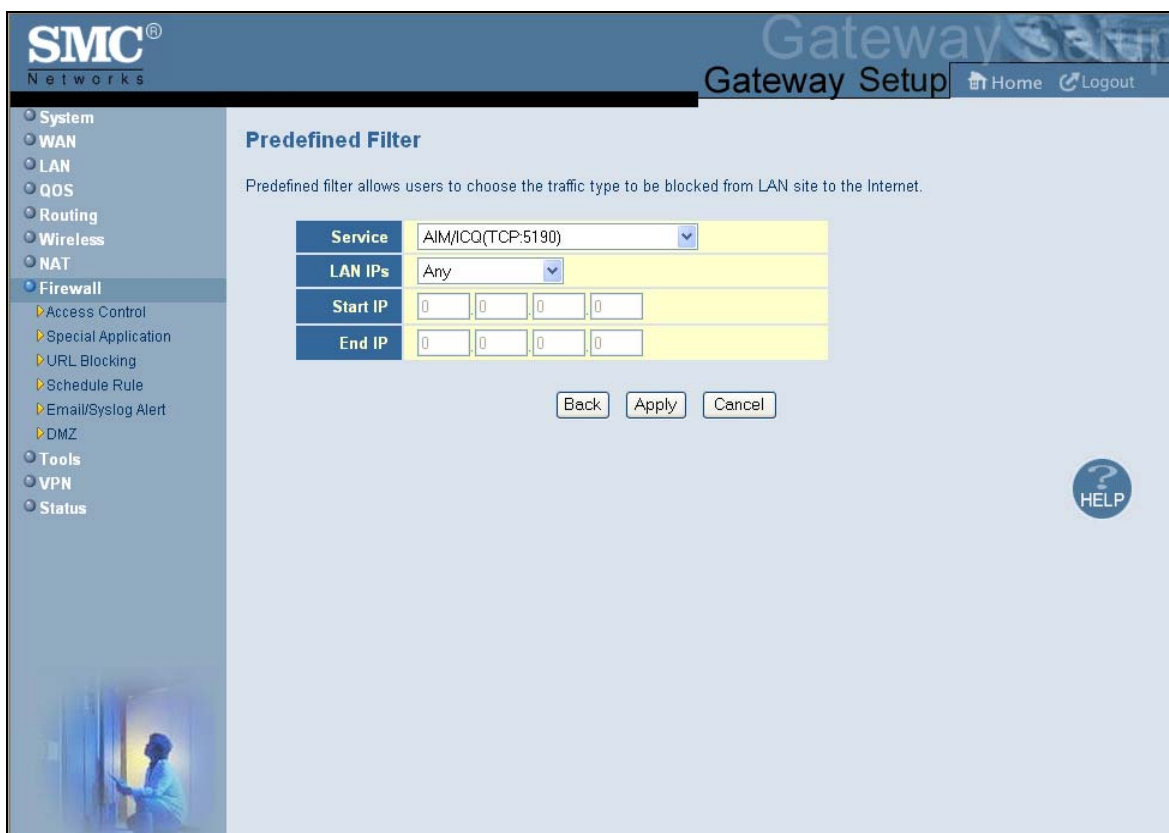


Figure 60. Predefined Filter Menu

Table 29. Predefined Filter Menu Options

Option	Description
Service	List of predefined services from which you can choose.
LAN IPs	Lets you apply the filter to any LAN IP addresses, a single LAN IP address, or a range of LAN IP addresses. <ul style="list-style-type: none"> • If you select one LAN IP address, enter the IP address in the Start IP field. • If you select a range of LAN IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To apply the predefined filter to: <ul style="list-style-type: none"> • A single local IP address, enter the local IP address. • A range of local IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any local IP addresses.
End IP	Ending IP address in the local IP address range to which the filter will be applied. This field is unavailable if the Gateway is configured for any local IP address or a single local IP address.

Adding Customer-Defined Filters

Using the following procedure, you can add customer-defined filters that block certain types of traffic from the LAN side of the Gateway to the Internet side of the Gateway.

1. In the Access Control menu, check **Enable Access Control** if it is not checked and click the **Apply** button. The remaining fields in the menu become available.
2. Under **Customer Defined Filtering Table**, click the **Add** button. The Customer Defined Filter menu appears (see Figure 61).
3. Complete the fields in the Customer Defined Filter menu (see Table 30).
4. Click **Apply**. (Or click **Back** to return to the Access Control menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the customer-defined filter is added to the **Customer Defined Filtering Table**.
5. To define additional filters for access control (up to 35, including predefined filters), repeat steps 1 through 4. When you finish, click **Apply** in the Access Control menu to save your settings.
6. To change the settings for a customer-defined filter, click the radio button to the left of the filter you want to change and click the **Edit** button. When the Customer Defined Filter menu appears, edit the settings as necessary (see Table 30) and click **Apply**. Click **Apply** in the Access Control menu to save your settings.
7. To delete a customer-defined filter, click the radio button to the left of the filter you want to delete and click the **Delete** button. No precautionary message appears before you delete a customer-defined filter. Click **Apply** in the Access Control menu to save your settings.



Figure 61. Customer Defined Filter Menu

Table 30. Customer Defined Filter Menu Options

Option	Description
Name	Name for identifying the custom service. The name is for reference purposes only.
Type	The type of protocol you want to filter. Choices are TCP, UDP, and TCP/UDP. Default is TCP.
LAN IPs	Lets you apply the filter to any LAN IP addresses, a single LAN IP address, or a range of LAN IP addresses. <ul style="list-style-type: none"> • If you select one LAN IP address, enter the IP address in the Start IP field. • If you select a range of LAN IP addresses, enter the starting IP address in the Start IP field and the ending IP address in the End IP field.
Start IP	To specify: <ul style="list-style-type: none"> • A single remote IP address, enter the remote IP address. • A range of remote IP addresses, enter the starting IP address here and the ending IP address range in the next field. This field is unavailable if the Gateway is configured for any remote IP addresses.
End IP	Ending IP address in the LAN IP address range to which the filter will be applied. This field is unavailable if the Gateway is configured for any LAN IP address or a single LAN IP address.
From Port	Starting port number on which the filter will be applied. If necessary, contact the application vendor for this information.
To Port	Ending port number on which the filter will be applied. If necessary, contact the application vendor for this information.

Responding to or Ignoring Pings

When the Gateway firewall module is enabled, the Gateway can respond to pings sent to its WAN port from an external IP over the Internet and sent to its public LAN port.

To have the WAN port of the Gateway ignore ping requests from the Internet that are sent to the Gateway's WAN IP address, uncheck **Respond to Ping on Internet WAN Port** at the bottom of the Access Control menu and click **Apply**.

To have the public LAN port of the Gateway ignore ping requests from the Internet that are sent to the Gateway's WAN IP address, uncheck **Respond to Ping on Public LAN Port** at the bottom of the Access Control menu and click **Apply**.

Configuring Special Applications

Using the Special Application menu, you can configure the Gateway to detect port triggers for detect multiple-session applications and allow them to pass the firewall. For special applications, besides the initial communication session, there are multiple related sessions created during the protocol communications. Normally, a normal treats the triggered sessions as independent sessions and blocks them. However, the Gateway can co-relate the triggered sessions with the initial session and group them together in the NAT session table. As a result, you need only specify which protocol type and port number you want to track, as well as some other related parameters. In this way, the Gateway can pass the special applications according to the supplied information.

Assume, for example, that to use H.323 in a Net Meeting application, a local client starts a session A to a remote host. The remote host uses session A to communicate with the local host, but it also could initiate another session B back to the local host. Since there is only session A recorded in the NAT session table when the local host starts the communication, session B is treated as an illegal access from the outside and is blocked. Using the Special Application menu, you can configure the Gateway to co-relate sessions A and B and automatically open the port for the incoming session B.

To display the Special Applications menu, click **Firewall** in the menu bar and then click the **Special Application** submenu. Figure 62 shows an example of the menu.

The maximum allowed triggers is 50. To enable the special application function, check the **Enable Triggering** checkbox and click **Apply**. To disable it, uncheck the **Enable Triggering** checkbox and click **Apply**.



Note: The **Special Application** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).

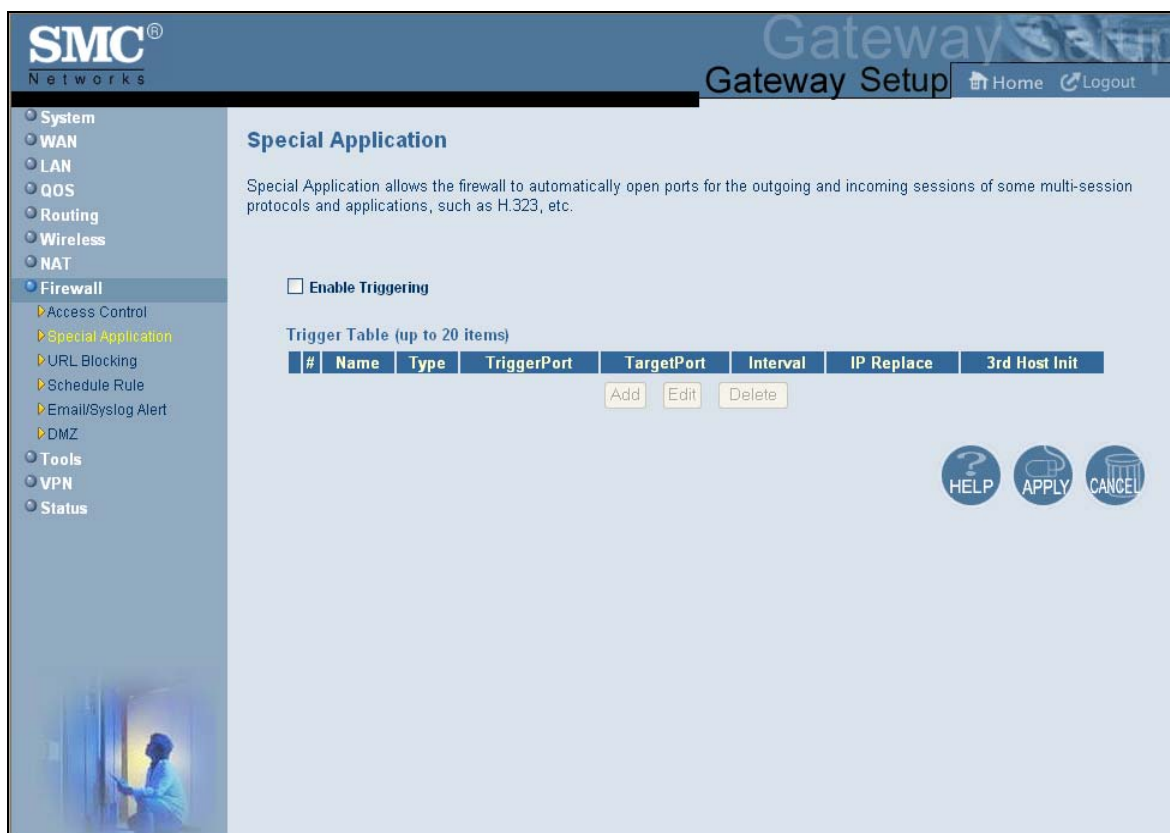


Figure 62. Special Application Menu

To enable port triggering:

1. In the Special Application menu, check **Enable Triggering** if it is unchecked and click the **Apply** button. The Trigger Table becomes available.
2. Click the **Add** button below **Trigger Table**. The Trigger menu appears (see Figure 63).
3. Complete the fields in fields Trigger menu (see Table 31).
4. Click **Apply**. (Or click **Back** to return to the Trigger menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the trigger is added to the **Trigger Table**.
5. To configure additional triggers (up to 20), repeat steps 1 through 4. When you finish, click **Apply** in the Special Applications menu to save your settings.
6. To change the settings for a trigger, click the radio button to the left of the trigger you want to change and click the **Edit** button. When the Trigger menu appears, edit the settings as necessary (see Table 31) and click **Apply**. Click **Apply** in the Special Application menu to save your settings.
7. To delete a trigger, click the radio button to the left of the trigger you want to delete and click the **Delete** button. No precautionary message appears before you delete a trigger. Click **Apply** in the Special Application menu to save your settings.



Figure 63. Trigger Menu

Table 31. Trigger Menu Options

Option	Description
Name	Name for identifying the trigger. The name is for reference purposes only.
Type	The type of protocol you want to use with the trigger. Choices are TCP and UDP. Default is TCP. For example, to track the H.323 protocol, the protocol type should be TCP.
Trigger Port	From and To port ranges of the special application. For example, to track the H.323 protocol, the From and To ports should be 1720.
Target Port	From and To port ranges for the target port listening for the special application.
Interval	Specify the interval between 50 and 30000 between two continuous sessions. If the interval exceeds this time interval setting, the sessions are considered to be unrelated.
IP Replacement	Select the IP replacement according to the application. Some applications embed the source host's IP in the datagram and normal NAT would not translate the IP address in the datagram. To make sure the network address translation is complete, IP replacement is necessary for these special applications, such as H.323.
Allow sessions initiated from/to the 3 rd host	Decide whether the sessions can start from/to a third host. To prevent hacker attacks from a third host, this feature usually is not allowed. However, for some special applications, such as MGCP in a VOIP application, a session initiated from a third host is permitted. For example, assume Client A is trying to make a phone call to a host B. Client A tries to communicate with the Media Gateway Controller (MGC) first and provides host B's number to MGC. Then MGC checks its own database to find B and communicate with B to provide B the information about A. B uses this information to communicate directly to A. So initially, A is talking to MGC, but the final step has B initiating a session to A. If the third-party host-initiated session is not allowed in this example, the whole communication fails.

Configuring URL Blocking

Using the URL Blocking menu, you can configure the Gateway to block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. The Gateway examines all the HTTP packets to block the access to those particular sites. This feature can be used to protect children from accessing inappropriate Web sites. You can block up to 50 sites.

Using URL blocking, you can also make up to 10 computers exempt from URL blocking and have full access to all Web sites at any time.

To display the URL Blocking menu, click **Firewall** in the menu bar and then click the **URL Blocking** submenu. Figure 64 shows an example of the menu.



Note: The **URL Blocking** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).



Tip: The Gateway provides a Schedule Rules feature that lets you configure URL blocking for certain days, if desired. For more information, see “Configuring Schedule Rules” on page 124.

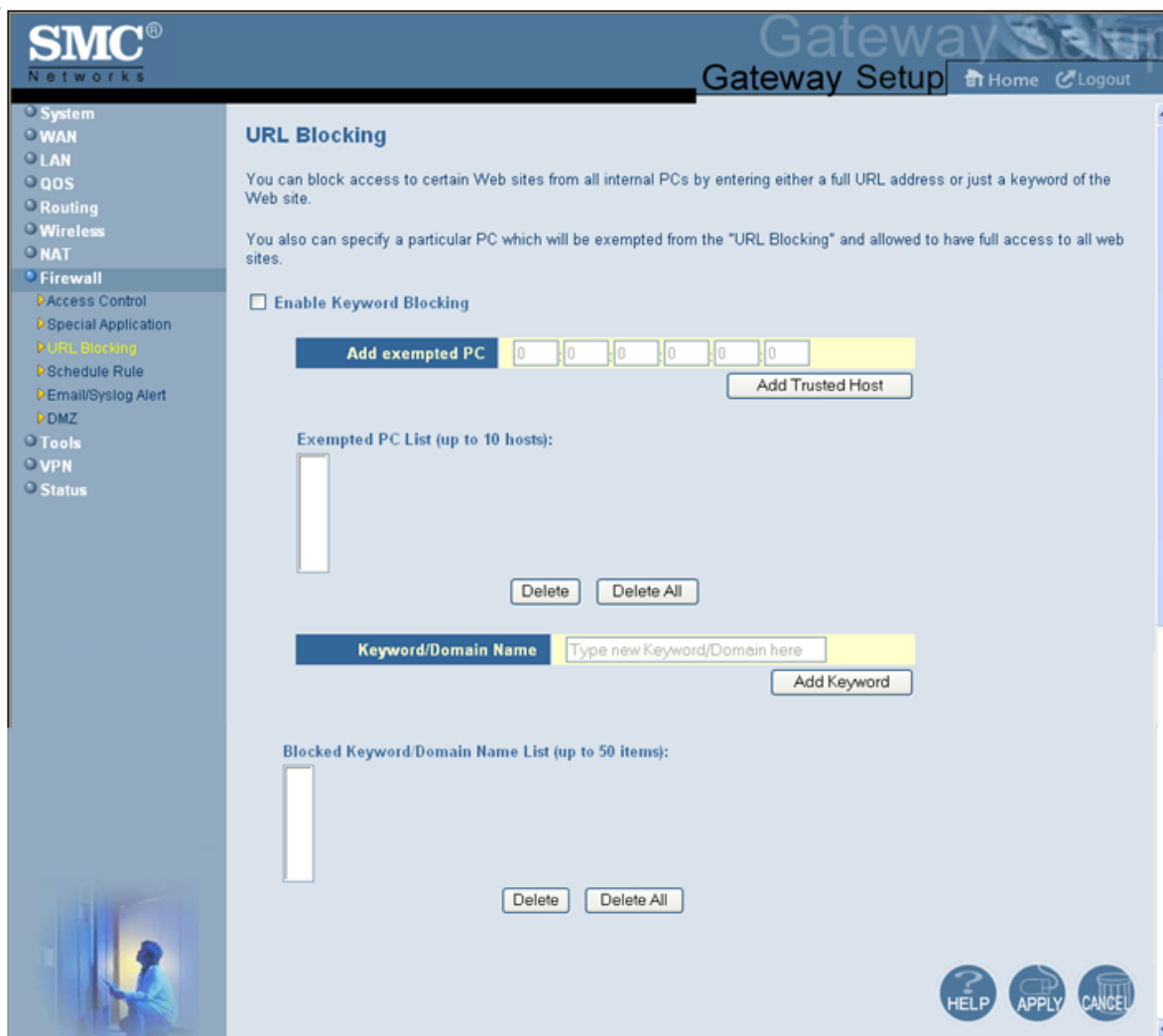


Figure 64. URL Blocking Menu

To enable URL blocking:

1. In the URL Blocking menu, check **Enable Keyword Blocking** if it is not checked and click **Apply**.
2. To exempt a computer from URL blocking, enter the computer's MAC address in the **Add exempted PC** field and click the **Add Trusted Host** button. The MAC address you entered appears in the **Exempted PC List**.
 - Repeat this step for each additional computer (up to 10) you want to make exempt from URL blocking.
 - To remove a computer from being exempted, use the **Delete** or **Delete All** buttons next to the field to delete selected or all MAC addresses.

3. To block a site, click in the **Keyword/Domain Name** field, enter keyword or domain name of the site you want to block, and click **Add Keyword**. The keyword or domain appears in the **Blocked Keyword/Domain List**.
 - Repeat this step for each additional keyword or domain (up to 50) you want to make exempt from URL blocking.
 - To remove a site from being blocked by a keyword or domain name, use the **Delete** or **Delete All** buttons next to the field to delete selected or all keywords and/or domains.
4. Click **Apply**.

Configuring Schedule Rules

Schedule rules work with the Gateway's URL blocking feature (described on page 122) to tell the Gateway when to perform URL blocking.

To access the Schedule Rule menu, click **Firewall** in the menu bar and then click the **Schedule Rule** submenu in the menu bar. Figure 65 shows an example of the menu.



Note: The **Schedule Rule** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).

SMC Networks Gateway Setup Gateway Setup Home Logout

Schedule Rule

This page defines the schedule rule you want to use with the "URL Blocking" page.

	Week Day
<input checked="" type="checkbox"/>	Every Day
<input checked="" type="checkbox"/>	Sunday
<input checked="" type="checkbox"/>	Monday
<input checked="" type="checkbox"/>	Tuesday
<input checked="" type="checkbox"/>	Wednesday
<input checked="" type="checkbox"/>	Thursday
<input checked="" type="checkbox"/>	Friday
<input checked="" type="checkbox"/>	Saturday

All Day

Start Time: 12 (hour) 0 (min) AM

End Time: 12 (hour) 0 (min) AM

HELP APPLY CANCEL

Figure 65. Schedule Rule Menu

By default, the Gateway is configured to apply schedule rules to URL blocking 24 hours every day. To change these settings:

1. To change the days when schedule rules are applied to URL blocking, uncheck **Every Day** under **Week Day**. Then check the days when you want to apply schedule rules to URL blocking.
2. To change the hours when schedule rules are applied to URL blocking, uncheck **All Day**. Then specify the start and end times when you want to apply schedule rules to URL blocking. Select **AM** or **PM**, where AM refers to times from Midnight to Noon and PM refers to times from Noon to Midnight.
3. Click **Apply**.

Configuring Email and Syslog Alerts

The Gateway inspects packets at the application layer, and stores TCP and UDP session information, including timeouts and number of active sessions. This information is helpful when detecting and preventing Denial of Service (DoS) and other network attacks.

If you enabled the Gateway's firewall or content-filtering feature, you can use the Email/Syslog Alert menu to configure the Gateway to send email notifications or add entries to the syslog when:

- Traffic is blocked
- Attempts are made to intrude onto the network
- Local computers try to access block URLs

You can configure the Gateway to generate email notifications or syslog entries immediately or at a preconfigured time.

To access the Email/Syslog Alert menu, click **Firewall** in the menu bar and then click the **Email/Syslog Alert** submenu in the menu bar.

The screenshot shows the SMC Networks Gateway Setup interface. The left sidebar contains a menu with the following items: System, WAN, LAN, QOS, Routing, Wireless, NAT, Firewall (selected), Access Control, Special Application, URL Blocking, Schedule Rule, Email/Syslog Alert (highlighted), DMZ, Tools, VPN, and Status. The main content area is titled "Email/Syslog Alert" and contains the following sections:

- Mail Server Configuration:** Includes fields for SMTP Server Address and Sender's E-mail Address.
- Mail Server Authentication:** Includes fields for User Name and Password.
- Recipient list (up to 4 items):** A table with columns for Name and Email Address, and buttons for Add, Edit, and Delete.
- Syslog Server Configuration:** Includes a field for Syslog Server Address.
- Alert Options:** A table with columns for Send Email and Send Syslog, and a row for "When intrusion is detected" with checkboxes for both.

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

Figure 66 shows an example of the menu. The menu has three sections:

- The top area lets you configure the Gateway to send email notifications.
- The middle area lets you add syslog entries.
- The bottom area lets you define the alerting schedule.



Note: The **Email/Syslog Alert** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).

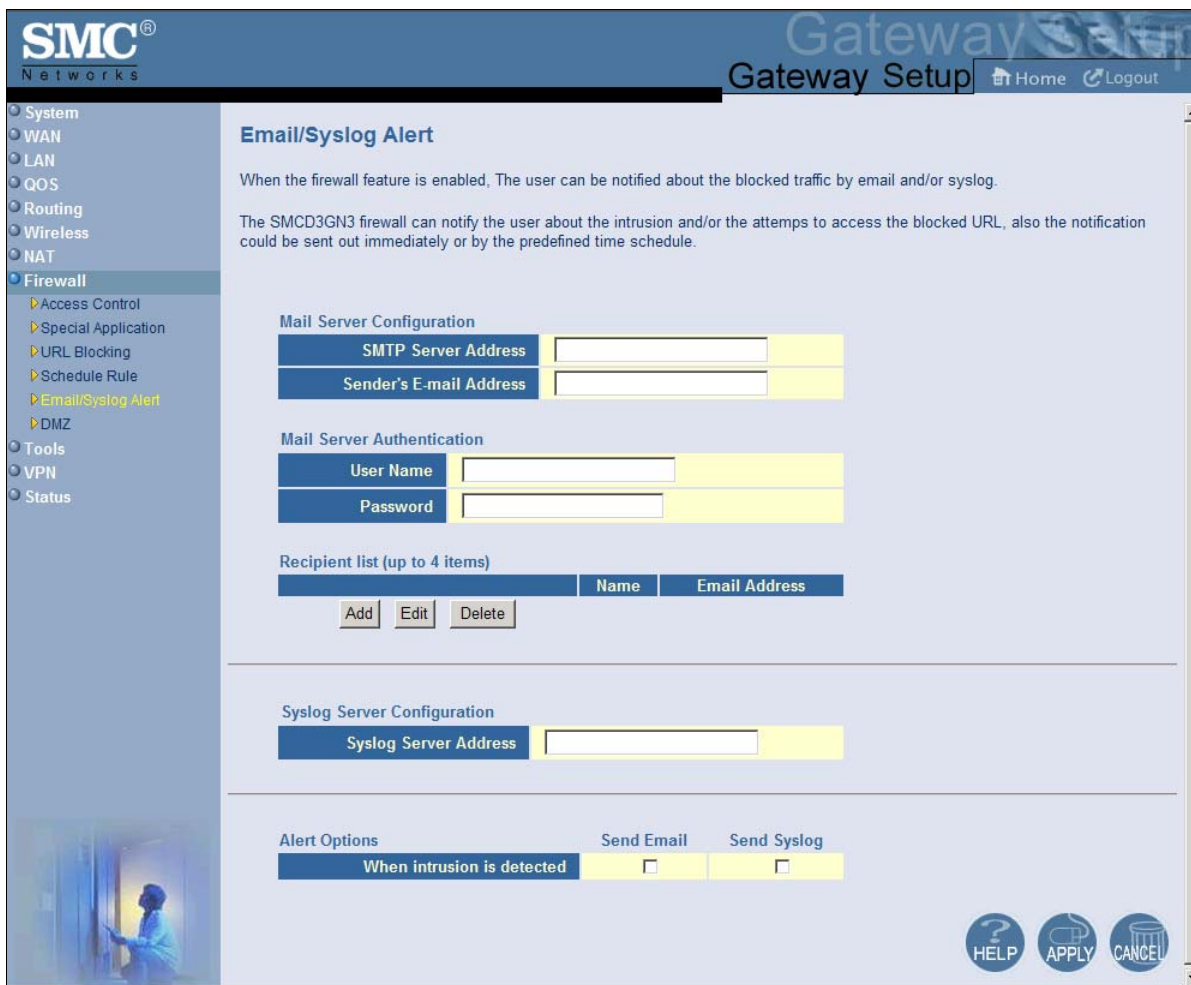


Figure 66. Email/Syslog Alert Menu

Configuring Email Alerts

The following procedure describes how to configure the Gateway to send email notifications. This procedure assumes that your mail server is working properly.

1. In the Email/Syslog Alert menu, under **Mail Server Configuration**, enter the following information:
 - **SMTP Server Address** = IP address of the SMTP server that will forward the email notification to recipients.
 - **Sender's Email Address** = name that will appear as the sender in the email notifications.
2. Under **Mail Server Authentication**, enter the following information:
 - **User Name** = your email name.
 - **Password** = your email password.
3. Under **Recipient list**, click **Add**. When the Recipient Adding menu appears (see Figure 67), enter the name of the person who will receive email notifications and the person's email address, and then click **Apply**. (Or click **Back** to return to the Email/Syslog Alert menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the email account is added to the **Recipient list**. To send email to additional email accounts (up to 4), repeat this step.
4. To change the settings for an email recipient, click the radio button to the left of the recipient you want to change and click the **Edit** button. When the Recipient Adding menu appears, edit the settings as necessary and click **Apply**.
5. To delete an email recipient, click the radio button to the left of the recipient and click **Delete**. No precautionary message appears before you delete the email recipient.
6. Click **Apply**.

Recipient Adding

Users could input and edit the email alert recipient list here.

Name	<input type="text"/>
Recipient's Email Address	<input type="text"/>

Figure 67. Recipient Adding Menu

Configuring Syslog Entries

To have the Gateway add a syslog entry when traffic is blocked, attempts are made to intrude onto the network, or local computers try to access block URLs:

1. In the Email/Syslog Alert menu, under **Syslog Server Configuration**, enter the syslog server address.
2. Click **Apply**.

Configuring Alert Options

Using the options in the **Alert Options** area, you can configure the Gateway to send an email to recipients you define in this menu and/or send entries to a syslog defined in this menu if the Gateway detects an intrusion.

To configure the Gateway to send an email to the configured email addresses if it detects an intrusion:

1. Perform steps 1 through 3 under “Configuring Email Alerts” on page 127.
2. Under **Alert Options**, check **Send Email** next to **When intrusion is detected**.
3. Click **Apply**.

To configure the Gateway to send an entry to a syslog if it detects an intrusion:

1. Perform step 1 under “Configuring Syslog Entries” on page 128.
2. Under **Alert Options**, check **Send Syslog** next to **When intrusion is detected**.
3. Click **Apply**.

Configuring DMZ Settings

If you have a local client computer that cannot run an Internet application properly behind the NAT firewall, you can configure it for unrestricted two-way Internet access by defining it as a Virtual Demilitarized Zone (DMZ) host. Adding a client to the DMZ may expose your local network to various security risks because the client in the DMZ is not protected by the firewall.

To access the DMZ (Demilitarized Zone) menu, click **Firewall** in the menu bar and then click the **DMZ** submenu in the menu bar. Figure 68 shows an example of the menu.



Note: The **DMZ** submenu is not available in the menu bar if **Enable Firewall Module** is disabled in the Security Settings (Firewall) menu (see page 105).

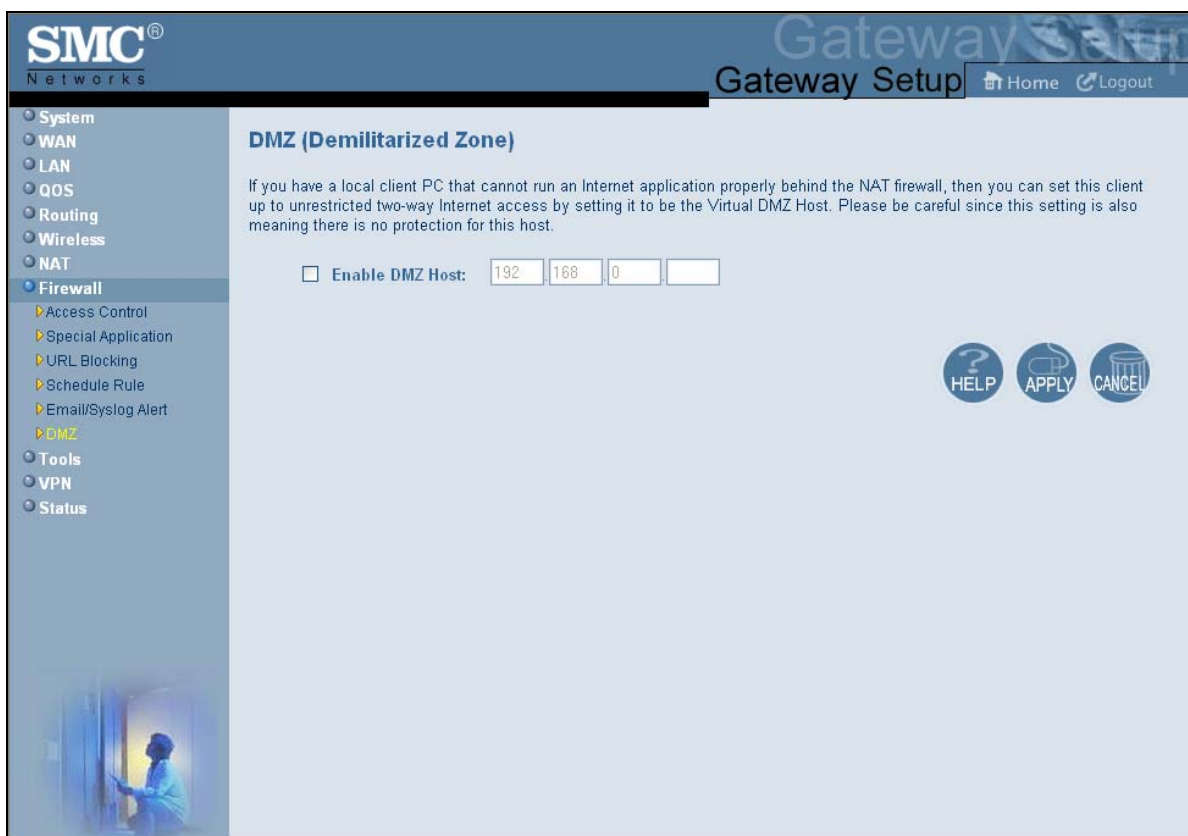


Figure 68. DMZ (Demilitarized Zone) Menu

To configure DMZ settings:

1. In the DMZ (Demilitarized Zone) menu, check **Enable DMZ Host**. The 2 rightmost fields next to this option become available.
2. Enter the last two octets in the IP addresses of the computer to be used as the DMZ server.
3. Click **Apply**.

Using the Configuration Tools Menu

Gateways often get upgraded or swapped out for a number of reasons. There also times when a Gateway might fail. In such cases, having a backup file containing your configuration settings allows you to restore a configuration by importing the configuration settings back into the Gateway.

Using the **Configuration Tools** menu, you can:

- Switch working scripts. See page 132.
- Back up the Gateway's current configuration settings locally. See page 132.
- Restore the configuration settings locally from a back-up copy. See page 133.
- Remotely back up the current configuration settings over the WAN. See page 134.
- Remotely restore the configuration settings from a backup copy over the WAN. See page 135.
- Restore the Gateway's factory default settings. See page 136.

To access the Configuration Tools menu, click Tools in the menu bar and then click the Configuration Tools submenu in the menu bar.

SMC Networks Gateway Setup [Home](#) [Logout](#)

Configuration Tools

Use the "Backup" tool to save the SMCD3GN3 current configuration to a file named "smc.cfg" on your local PC. You can then use the "Restore" tool to restore the saved configuration to the SMCD3GN3. Alternatively, if you want to backup or restore the SMCD3GN3 configuration remotely, you can use the "Remotely backup/restore Gateway settings" tool. To use this tool, you need to fill in the remote TFTP server address and Gateway config filename manually. Then press "Restore" button to retrieve the file from the TFTP server, or "Backup" to save the file to the TFTP server. Also, you can use the "Restore to Factory Defaults" tool to force the SMCD3GN3 to perform a power reset and restore the original factory settings.

- Configuration file settings**

#	Update Time	Length	
Script0	Thu Aug 11 13:54:30 2011	0 Bytes	running
Script1	Thu Jan 1 00:00:12 1970	0 Bytes	backup
- Locally backup current settings**

Script0 (running) Script1
- Locally restore saved settings from file**

Script0 (running) Script1
- Remotely backup/restore Gateway settings**

TFTP Server Address

Gateway Config Filename

Script0 (running) Script1

Script0 (running) Script1
- Restore to Factory Defaults**

Figure 69 shows an example of the menu.

SMC Networks Gateway Setup Home Logout

Configuration Tools

Use the "Backup" tool to save the SMCD3GN3 current configuration to a file named "smc.cfg" on your local PC. You can then use the "Restore" tool to restore the saved configuration to the SMCD3GN3. Alternatively, if you want to backup or restore the SMCD3GN3 configuration remotely, you can use the "Remotely backup/restore Gateway settings" tool. To use this tool, you need to fill in the remote TFTP server address and Gateway config filename manually. Then press "Restore" button to retrieve the file from the TFTP server, or "Backup" to save the file to the TFTP server. Also, you can use the "Restore to Factory Defaults" tool to force the SMCD3GN3 to perform a power reset and restore the original factory settings.

- Configuration file settings**

#	Update Time	Length	
Script0	Thu Aug 11 13:54:30 2011	0 Bytes	running
Script1	Thu Jan 1 00:00:12 1970	0 Bytes	backup

Switch Working Script
- Locally backup current settings**

Script0 (running) Script1
- Locally restore saved settings from file**

Script0 (running) Script1
- Remotely backup/restore Gateway settings**

TFTP Server Address

Gateway Config Filename

Script0 (running) Script1

Script0 (running) Script1
- Restore to Factory Defaults**

HELP CANCEL

Figure 69. Configuration Tools Menu

Switching Working Scripts

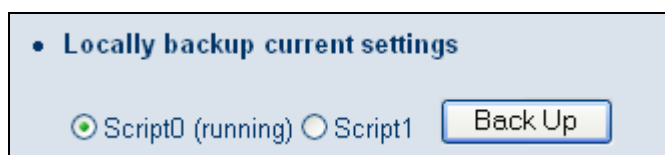
If more than one working script appears below **Configuration file settings**, you can switch to another working script.

1. Under Configuration file settings, click the Switch Working Script button.
2. When a prompt asks whether you want to switch scripts, click **OK** to switch or **Cancel** to keep the current working script.

Backing Up the Gateway's Current Configuration Locally

To back up the Gateway's current configuration locally:

1. If one or more scripts appear to the left of the **Back Up** button under **Locally backup current settings**, click the script you want to back up. **(running)** appears next to the script that is currently running.
2. Click the **Back Up** button.



3. When the File Download dialog box appears (see Figure 70), click **Save**. (Or click **Open** to view the file prior to saving it. If you open the file, you will have to repeat steps 1 and 2 to save it.)
4. When the Save As dialog box appears, go to the location where you want to save the configuration file and click the **Save** button. The file is saved as `smc.cfg`.
5. When the save operation is complete, the Download complete dialog box appears (see Figure 71). Click **Open** to open the configuration file, **Open Folder** to open the folder containing the configuration file, or **Close** to close the dialog box.



Tip: If you click **Open** and a message tells you that an application could not be found to open the configuration file, open the file in a text editor such as WordPad.

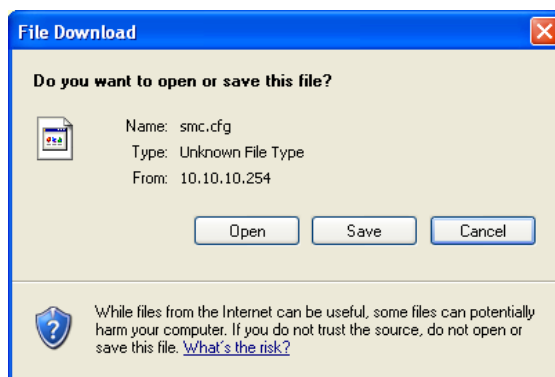


Figure 70. File Download Dialog Box

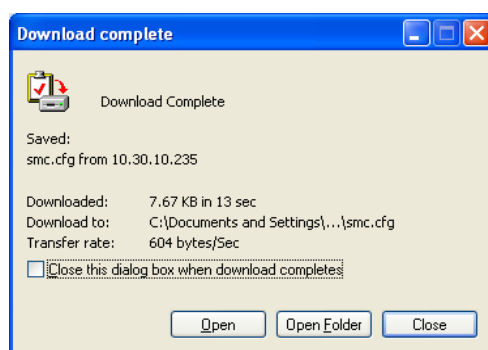


Figure 71. Download Complete Dialog Box

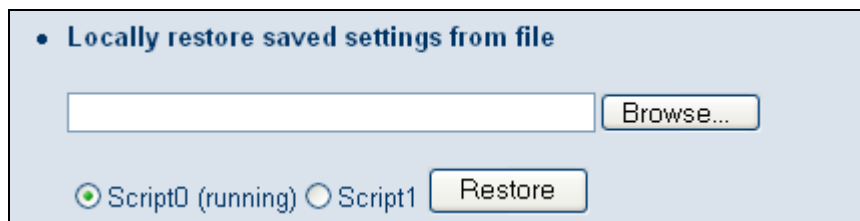
Restoring the Gateway's Current Configuration Locally

If you backed up the Gateway's configuration settings locally, use the following procedure to restore the settings locally.



Note: Restoring the Gateway's settings from a configuration file erases all of the Gateway's current settings.

1. If one or more scripts appear to the left of the **Restore** button under **Locally restore saved settings from file**, click the script you want to restore. **(running)** appears next to the script that is currently running.
2. Click the **Browse** button.



- When the Choose File dialog box appears, go to the location where you saved the `smc.cfg` file. Then either double-click the file, or click it and click the **Open** button. The file path and name appear to the left of the **Browse** button.
- Click the **Restore** button. The message in Figure 72 appears.
- Click **OK** to override the Gateway's current configuration with the one in the configuration file or click **Cancel** to not restore the configuration from the file.

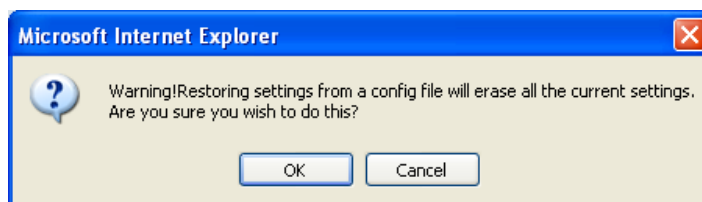
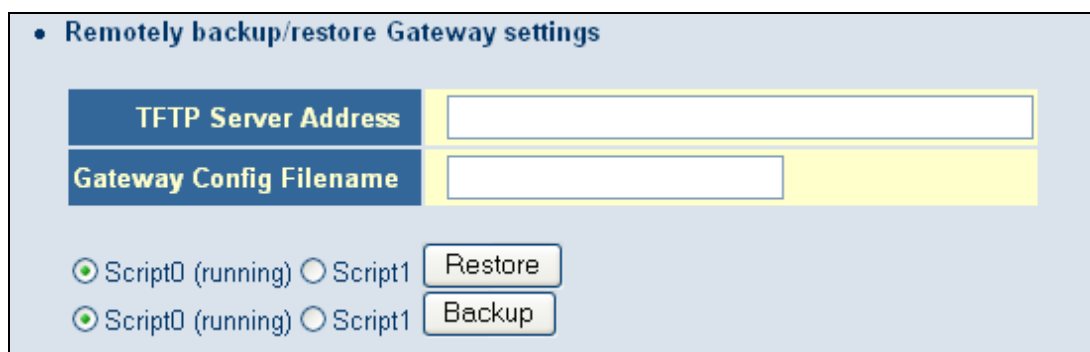


Figure 72. Warning Message when Restoring from a Configuration File

Backing Up the Gateway's Current Configuration Remotely

You can back up the Gateway's current configuration remotely by uploading the `smc.cfg` file to a TFTP server.

- Under **Remotely backup/restore Gateway settings**, enter the IP address of the TFTP server in the **TFTP Server Address** field.



- In the **Gateway Config Filename** field, enter the name of the configuration file.
- If one or more scripts appear to the left of the **Backup** button, select the script you want to restore. **(running)** appears next to the script that is currently running.
- Click the **Backup** button.

Restoring the Gateway's Current Configuration Remotely

If you backed up the Gateway's configuration settings to a TFTP server, use the following procedure to restore the settings remotely.



Note: Restoring the Gateway's settings from a configuration file erases all of the Gateway's current settings.

1. Under **Remotely backup/restore Gateway settings**, enter the IP address of the TFTP server in the **TFTP Server Address** field.

• Remotely backup/restore Gateway settings

TFTP Server Address

Gateway Config Filename

Script0 (running) Script1

Script0 (running) Script1

2. In the **Gateway Config Filename** field, enter the name of the configuration file.
3. If one or more scripts appear to the left of the **Restore** button, select the script you want to restore. **(running)** appears next to the script that is currently running.
4. Click the **Restore** button. The message in Figure 72 appears.
5. Click **OK** to override the Gateway's current configuration with the one in the configuration file or click **No** to not restore the configuration from the file.

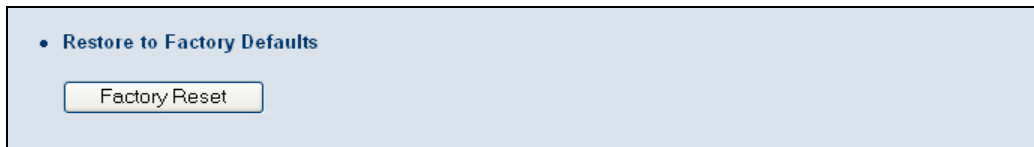
Restoring Factory Defaults

One way to restore the Gateway's factory default settings is by using the Reset switch on the Gateway's rear panel (see "Restoring Factory Defaults" on page 15). Another way is to use the Configuration Tools menu to power-cycle the Gateway.



Note: Rebooting the Gateway removes any customized overrides you made to the default settings. To reboot the Gateway and retain any customized settings, use the Reboot menu (see "Using the Reboot Menu to Reboot the Gateway" on page 137).

1. Under **Restore to Factory Defaults**, click **Factory Reset**. The warning message in Figure 73 appears.



2. Click **OK** to restore the Gateway's factory default settings or click **Cancel** to retain the Gateway's current settings.

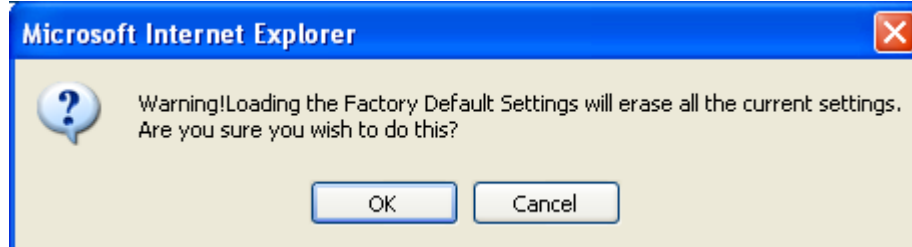


Figure 73. Warning Message when Restoring Factory Defaults

Using the Reboot Menu to Reboot the Gateway

Using the Reboot menu, you can reset the Gateway and retain all changes that have been made to the Gateway's factory default settings. To access the Reboot menu, click **Tools** in the menu bar and then click the **Reboot** submenu in the menu bar. Figure 74 shows an example of the menu.

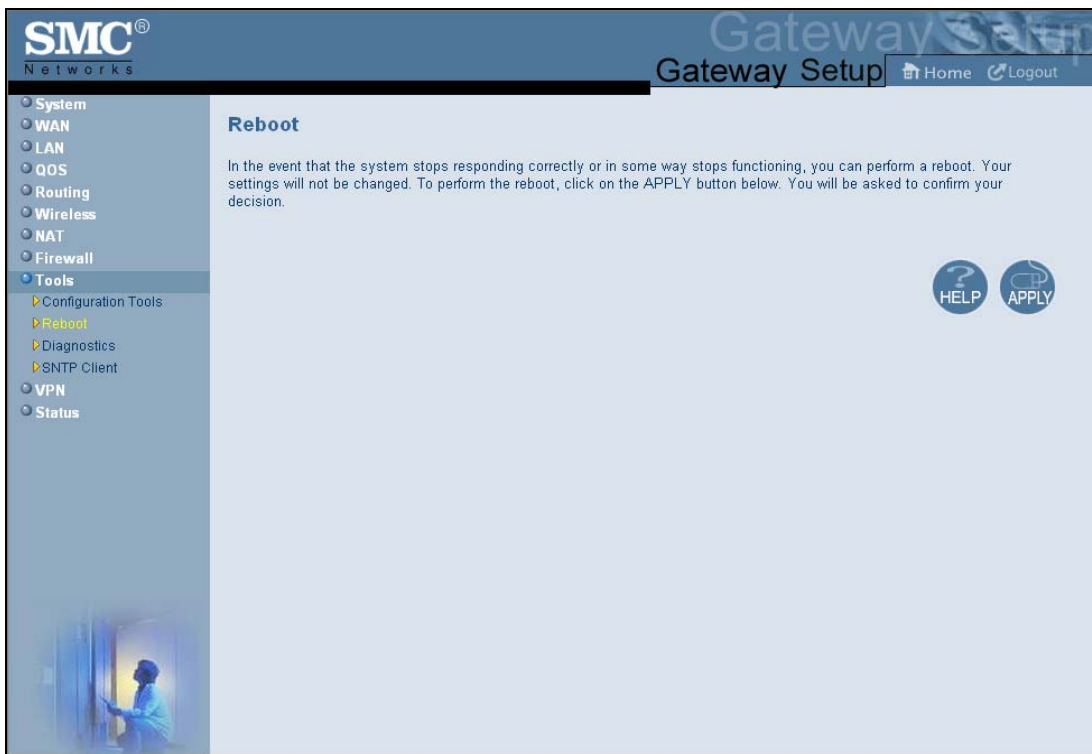


Figure 74. Reboot Menu

To reboot the Gateway and retain all changes made to its factory default settings:

1. In the Reboot menu, click **Apply**. The precautionary message in Figure 75 appears.
2. Click **OK** to reboot the Gateway or click **Cancel** to not reboot it. If you clicked **OK**, the reboot is complete when the **POWER** LED stops blinking and you will need to log in to the Web interface again.

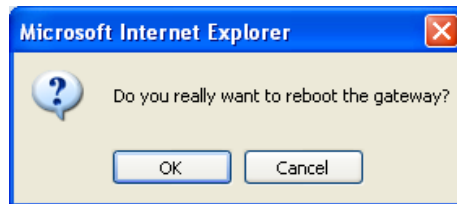


Figure 75. Precautionary Message When Rebooting the Gateway

Using the Diagnostics Menu

The Diagnostics menu lets you use “traceroute” to trace the routing path from the Gateway to the destination and router, and use ping to ascertain whether the destination is available. This menu also lets you specify the IP address for a log server, and the sniffing time to record the upstream and downstream traffic.

To access the Diagnostics menu, click **Tools** in the menu bar and then click the **Diagnostics** submenu in the menu bar. Figure 76 shows an example of the menu.

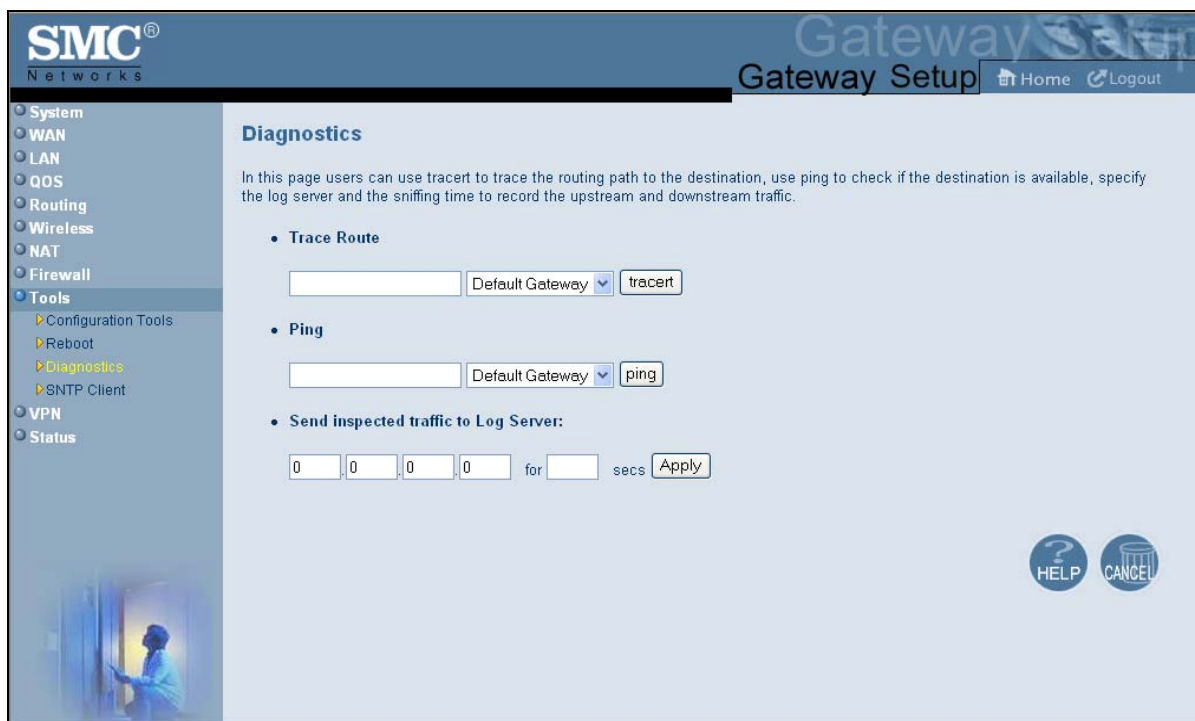


Figure 76. Diagnostics Menu

Using the Ping Tool

Using the ping tool, you can check the connectivity between the Gateway and another local or remote device. The Gateway provides a ping tool for conducting the ping with the default Gateway, across the RF interface, or across the WAN interface. This tool sends a small packet of data and then waits for a reply. When you ping a computer IP address and receive a reply, it confirms that the device is connected to the Gateway.

To perform ping activities, use the following procedure under **Ping** on the Diagnostics menu.

1. Enter the IP address or domain name of a target host in the **Ping** field.
2. In the drop-down list to the right of the IP address or domain name, select whether the ping is to be sent to the default Gateway, across the Gateway's RF interface, or across the Gateway's WAN interface.
3. Click the **ping** button. The results appear in the Diagnostics – Ping Results screen (see Figure 77 and Figure 78). The results screen may flash as the contents refresh during the ping.
4. To close the results screen, click the **Back** button.

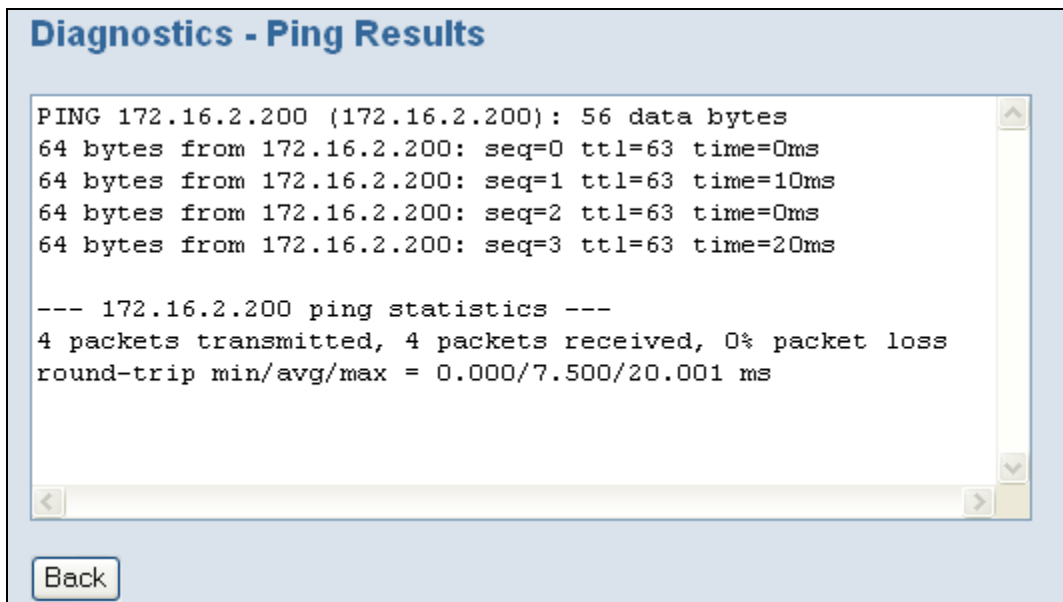


Figure 77. Example of Results for a Ping

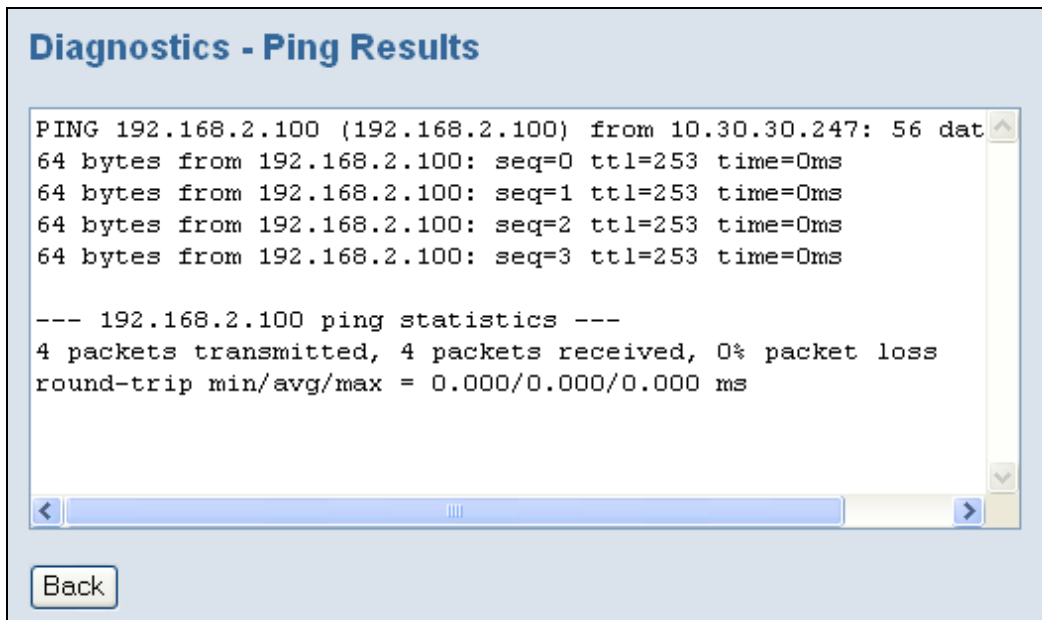


Figure 78. Example of Results for a WAN Ping

Using the Trace Route Tool

The Gateway provides a trace route tool for conducting the trace route with the default Gateway, across the RF interface, or across the WAN interface. This tool provides a supplemental role to the ping tool. While the ping tool confirms IP network reachability, you cannot pinpoint and improve some isolated problems.

Consider the following situations:

- When there are many hops (for example, gateways or routes) between the Gateway and the destination, and there seems to be a problem somewhere along the path. The destination system may have a problem, but you need to know where a packet is actually lost.
- The ping tools do not tell you the reasons for a lost packet.

The trace route tool can inform you where the packet is located and why the route is lost. Using the trace route tools, you can map the network path in real time from the Gateway to a local or public host.

To perform trace route activities, use the following procedure under **Trace Route** on the Diagnostics menu.

1. Enter the IP address or domain name of a target host in the **Trace Route** field.
2. In the drop-down list to the right of the IP address or domain name, select whether the trace route is to be sent to the default Gateway, across the Gateway's RF interface, or across the Gateway's WAN interface.
3. Click the **tracert** button. The trace route results appear in the Diagnostics – Trace Route Results screen, as the Gateway sends UDP packets to each device between the Gateway and the destination (see Figure 79 and Figure 80). It starts with the nearest device and expands the search by one hop until the destination is reached or the trace route times out. The results screen may flash as the contents refresh during the trace route operation.
4. To close the screen, click the **Back** button.

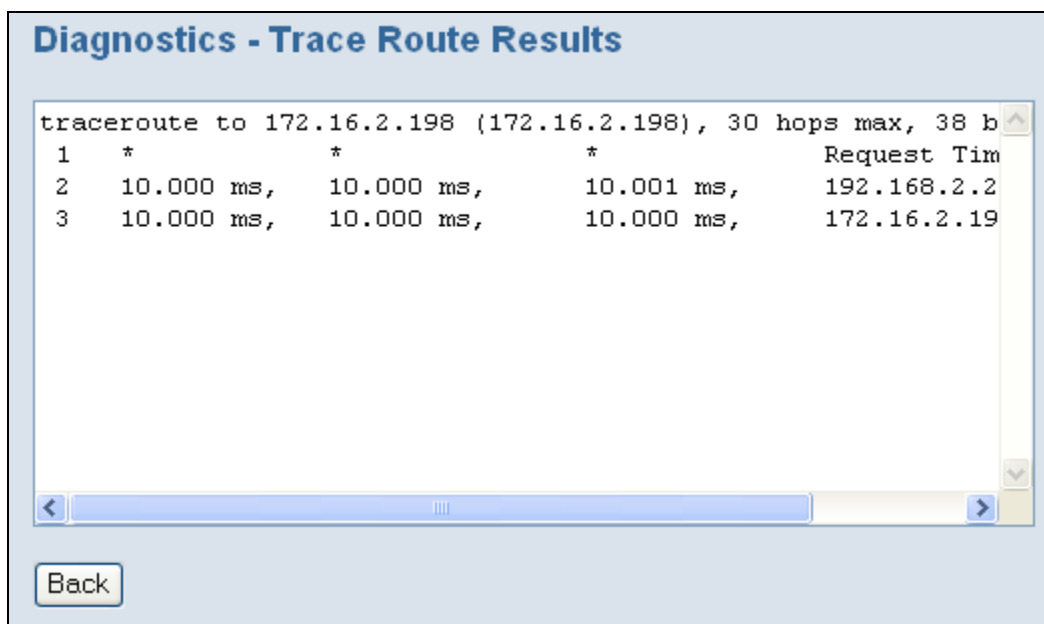


Figure 79. Example of Results for Trace Route

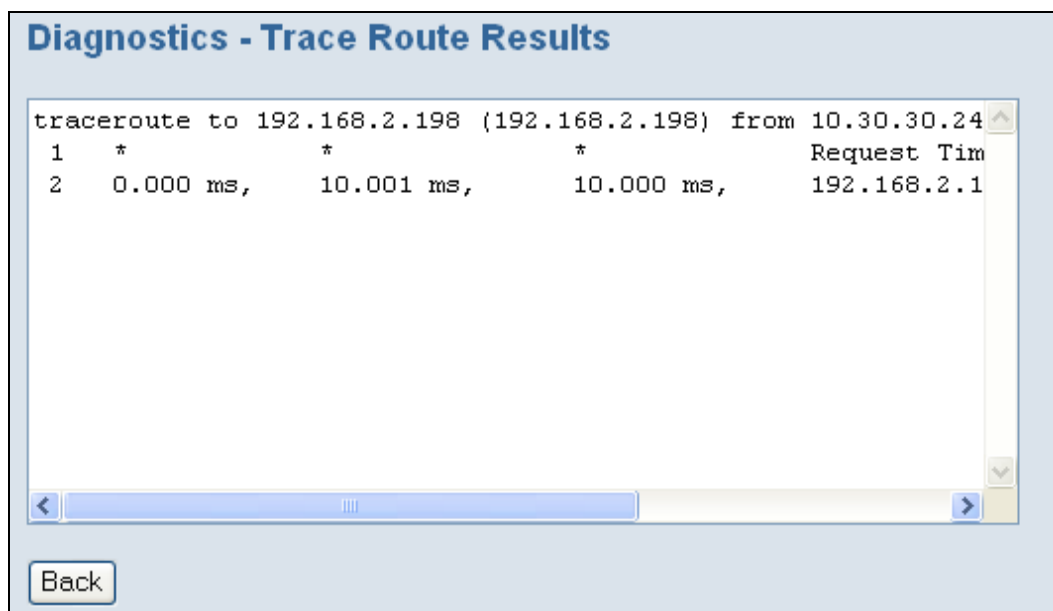


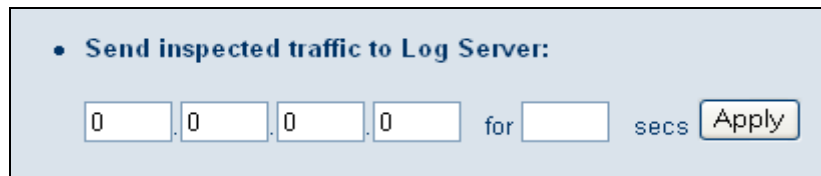
Figure 80. Example of Results for a WAN Trace Route

Sending Inspected Traffic to a Log Server

The Gateway can inspect upstream and downstream traffic, and log the results to the syslog server, where they can be further examined.

To send inspected traffic to a log server, perform the following procedure under **Send inspected traffic to Log Server** on the Diagnostics menu.

1. In the first four fields, enter the IP address of the log server.
2. In the **for** field, enter the number of seconds that inspected traffic is to be sent to the log server.



• **Send inspected traffic to Log Server:**

0 . 0 . 0 . 0 for [] secs

3. Click the **Apply** button.
4. The Gateway sniffs the traffic, logs the traffic to the syslog, and displays the message in Figure 81 when the number of seconds elapses.
5. Click **OK** to close the message.

You can now examine the sniffed traffic using appropriate syslog daemons and applications.



Figure 81. Sniffing Complete Message

Using the SNTP Menu

The SNTP Settings menu lets you configure the Gateway to act as an SNTP client. SNTP is a simplified, client-only version of NTP, a standard protocol used to synchronize system clocks on computer systems. SNTP can be enabled on the Gateway to keep the Gateway's time accurate up to fractions of a second. The service is constantly updating the Gateway's clock, and can be used as a master time source for other systems on your network.



Note: While SNTP typically provides time within 100 milliseconds of the accurate time, it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic. An SNTP client is more vulnerable to misbehaving servers than an NTP client, and should only be used in situations where strong authentication is not required.

To access the SNTP Settings menu, click **Tools** in the menu bar and then click the **SNTP Client** submenu in the menu bar. Figure 82 shows an example of the menu and Table 32 describes the options you can select.

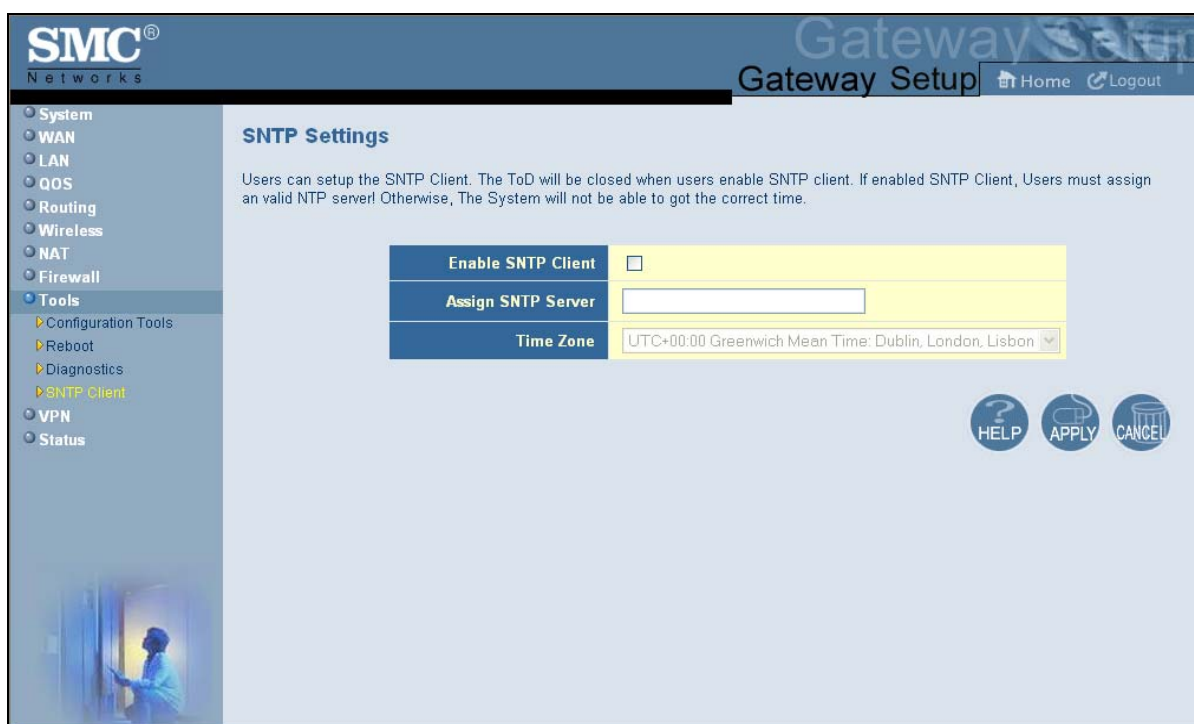


Figure 82. SNTP Settings Menu

Table 32. SNTP Settings Menu Options

Option	Description
Enable SNTP Client	Enables or disables the Gateway to be set up as an SNTP client. <ul style="list-style-type: none"> • Checked = Gateway can be set up as an SNTP client. The remaining fields in the menu become available. • Unchecked = Gateway cannot be set up as an SNTP client. The remaining fields in the menu remain gray and unavailable. (<i>default</i>)
Assign SNTP Server	IP address or host name of the SNTP server. This field is not available if Enable SNTP Client is not checked.
Time Zone	Time zone to be used for SNTP operations. This field is not available if Enable SNTP Client is not checked.

Configuring VPN Settings

A Virtual Private Network (VPN) is a technology designed to increase the security of information transferred over the Internet. A VPN creates a private encrypted tunnel from the user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

The Gateway supports the Internet Protocol Security (IPSec) to secure IP traffic. IPSec builds “virtual tunnels” between a local and remote subnet for secure communication between two networks. This connection is commonly known as a Virtual Private Network (VPN).

Alternatively, tunneling protocols such as L2TP and PPTP can be used to achieve a secure connection (such as to a corporate LAN) over the Internet. These tunneling protocols can optionally be secured themselves using IPSec.

Using the VPN menu, you can enable or disable the Gateway's VPN settings. If the VPN settings are enabled, you can use VPN submenus to:

- Allow PC clients behind the Gateway to access the IPSec VPN tunnel. See page 147.
- Define the VPN tunnel configuration. See page 148.

Using the VPN Menu

You can use the VPN menu to enable or disable the Gateway's VPN functions. By default, the Gateway's Virtual Private Network (VPN) settings are disabled.

To access the VPN menu, click **VPN** in the menu bar. Figure 83 shows an example of the menu and Table 33 describes the options you can select.

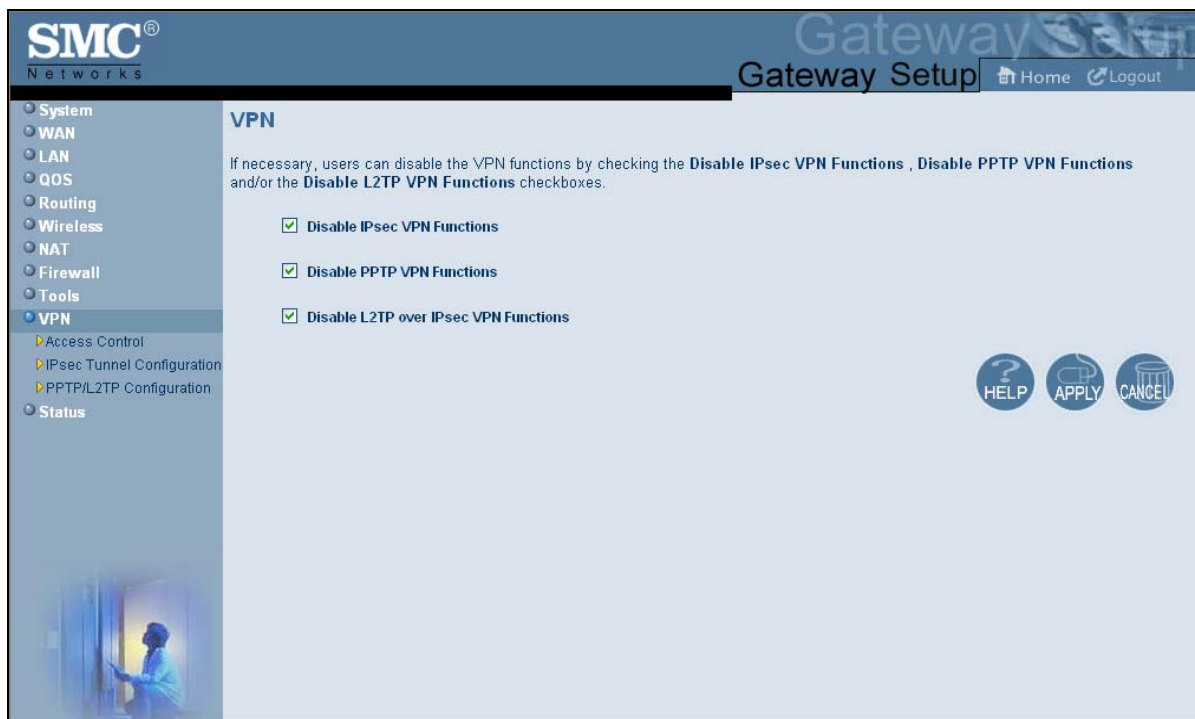


Figure 83. VPN Menu

Table 33. VPN Menu Options

Option	Description
Disable IPsec VPN Functions	<p>Lets you enable the Gateway's IPsec VPN functions. Select the option based on the type of Internet connection you will provide.</p> <ul style="list-style-type: none"> • Checked = functions are disabled. (<i>default</i>) • Unchecked = functioned are enabled.
Disable PPTP VPN Functions	<p>Lets you enable the Gateway's Point to Point Protocol (PPP) VPN functions. Select the option based on the type of Internet connection you will provide.</p> <ul style="list-style-type: none"> • Checked = functions are disabled. (<i>default</i>) • Unchecked = functioned are enabled.
Disable L2TP over IPsec VPN Functions	<p>Lets you enable the Gateway's LT2P VPN functions. Select the option based on the type of Internet connection you will provide.</p> <ul style="list-style-type: none"> • Checked = LT2P VPN functions are disabled. (<i>default</i>) • Unchecked = LT2P VPN functions are enabled.

Using the Access Control Menu to Allow CPEs to Access IPsec VPN Tunnel

You can use the Access Control menu to allow PC clients behind the Gateway to access the IPsec VPN tunnel.

To access the Access Control menu, click VPN in the menu bar and then click the Access Control submenu.

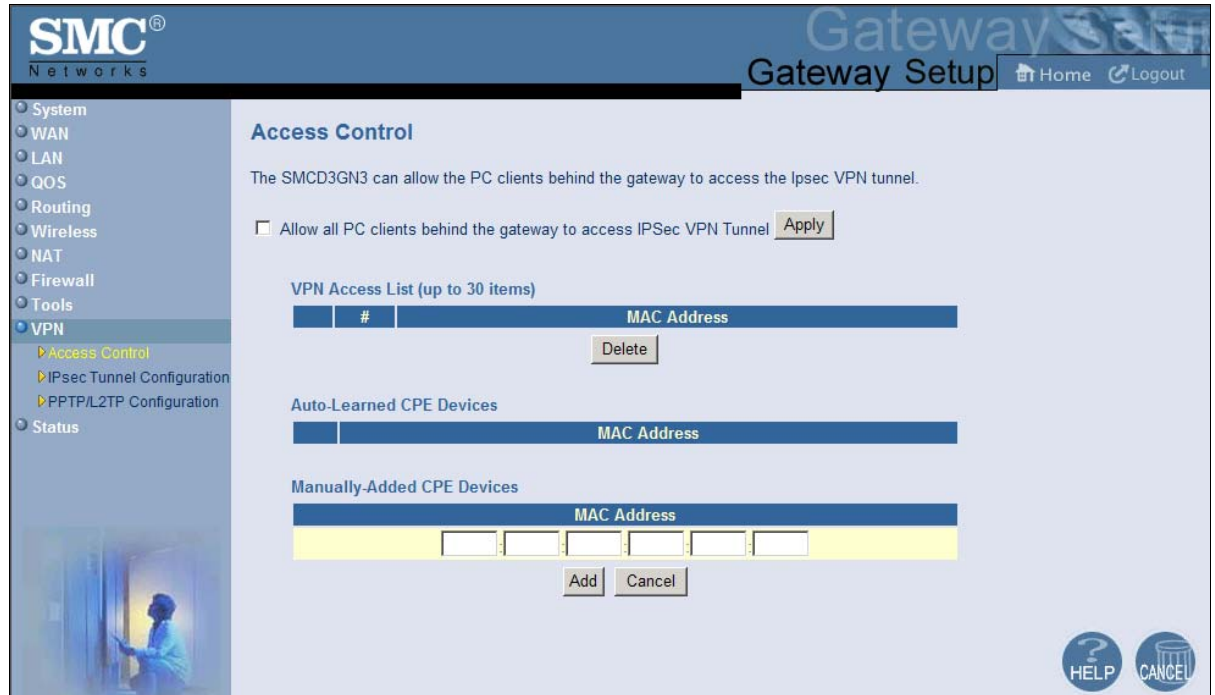


Figure 84 shows an example of the menu.

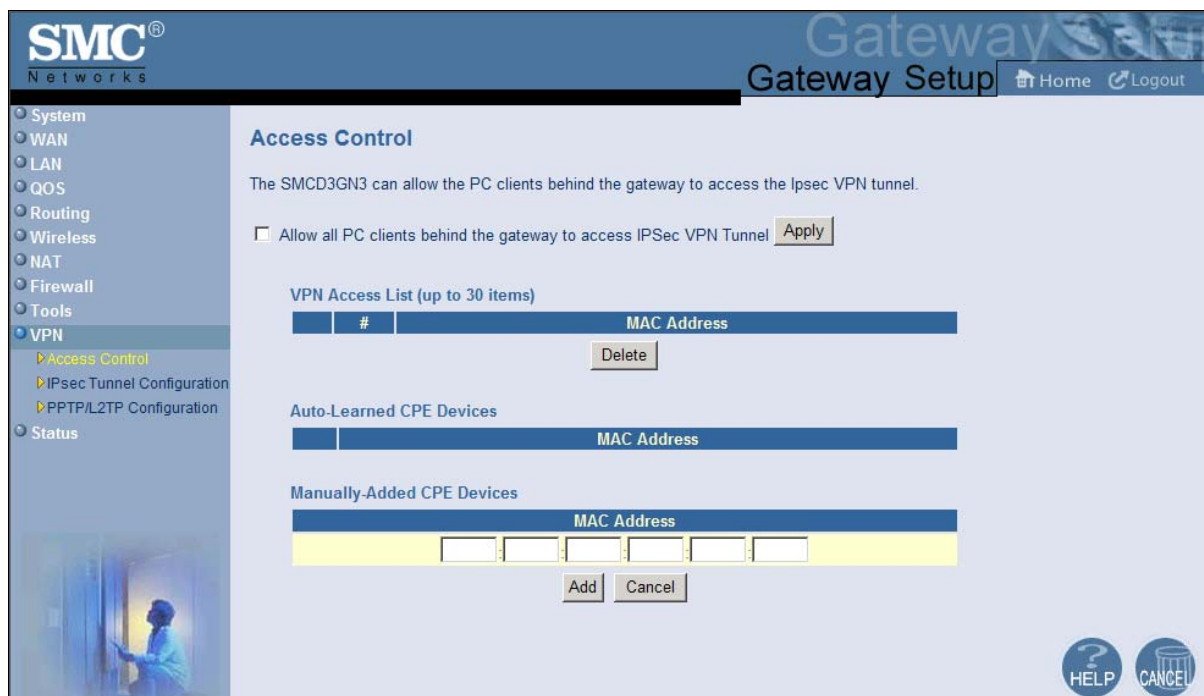


Figure 84. Access Control Menu

To allow PC clients behind the Gateway to access the IPSec VPN tunnel:

1. Click **VPN** in the menu bar.
2. On the VPN menu, uncheck **Disable IPsec VPN Functions** and click **Apply** (see Figure 83). Otherwise, the **Allow all PC clients behind the gateway to access IPSec VPN Tunnel** option in the Access Control menu will be unavailable.
3. In the menu bar, under **VPN**, click the **Access Control** submenu.
4. On the Access Control menu, click **Allow all PC clients behind the gateway to access IPSec VPN Tunnel** and click **Apply**. The fields in the menu become available.
5. To add customer premises equipment (CPE) that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned CPE Devices**:
 - a. Click a CPE that the Gateway learned automatically.
 - b. Click **Add** to add the CPE to the **VPN Access List**.
 - c. To add more auto-learned CPEs (up to 30), repeat steps 5a and 5b.
6. To manually add CPEs, perform the following steps under **Manually-Added CPE Devices**:
 - a. Under **MAC Address**, enter the MAC address of the device.
 - b. Click **Add** to add the CPE to the **VPN Access List**.
 - c. To manually add more CPEs (up to 30), repeat steps 6a and 6b.
7. To delete CPEs from access control, under **VPN Access List**, click the radio button corresponding to the CPE you want to delete and click the **Delete** button. A precautionary message does not appear before deleting a CPE.

Using the VPN – Tunnel Configuration Menu

You can use the VPN – Tunnel Configuration menu to define up to five tunnels. This menu also shows the VPN log and provides buttons for clearing, refreshing, and saving the log to a drive location.

To access the VPN – Tunnel Configuration menu, click VPN in the menu bar and then click the IPsec Tunnel Configuration submenu.

The screenshot displays the SMC Networks Gateway Setup web interface. The left sidebar contains a navigation menu with the following items: System, WAN, LAN, QoS, Routing, Wireless, NAT, Firewall, Tools, and VPN. The VPN menu is expanded, showing sub-items: Access Control, IPsec Tunnel Configuration, PPTP/L2TP Configuration, and Status. The main content area is titled "VPN - Tunnel Configuration" and features a "Tunnel Table (up to 5 items)" with columns for #, Remote IPsec ID, Remote Gateway IP, Status, Uptime & Count, and Active Type. Below the table are "Add", "Edit", and "Delete" buttons. A "VPN Log" section contains a scrollable text area with the following log entries:

```
Aug 10 16:42:55 Starting Pluto subsystem...
Aug 10 16:42:56 Unknown default RSA hostkey scheme, not generating a default
Aug 10 16:42:56 Starting Pluto (Openswan Version 2.4.12 PLUTO_SENDS_VENDORID
Aug 10 16:42:56 Setting NAT-Traversal port-4500 floating to on
Aug 10 16:42:56 port floating activation criteria nat_t=1/port_fload=1
Aug 10 16:42:56 including NAT-Traversal patch (Version 0.6c)
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC_SSH: Ok
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC: Ok (re
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_SERPENT_CBC: Ok (re
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_BLOWFISH_CBC: Ok (r
Aug 10 16:42:56 ike_alg_register_hash(): hash alg=6 has ctx_size=216 > hash_c
Aug 10 16:42:56 ike_alg_register_hash(): Activating <none>: FAILED (ret=-75)
Aug 10 16:42:56 starting up 1 cryptographic helpers
Aug 10 16:42:56 started helper pid=2248 (fd:5)
Aug 10 16:42:57 Using NETKEY IPsec interface code on 2.6.18_pro500
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/cacerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/aacerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/ocspcerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/crls'
```

At the bottom of the log window are "Clear", "Refresh", and "Send the Logs" buttons. A "HELP" icon is visible in the bottom right corner of the interface.

Figure 85 shows an example of the menu.

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

VPN - Tunnel Configuration

Tunnel Table (up to 5 items)

#	Remote IPsec ID	Remote Gateway IP	Status	Uptime & Count	Active Type
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					

VPN Log

```

Aug 10 16:42:55 Starting Pluto subsystem...
Aug 10 16:42:56 Unknown default RSA hostkey scheme, not generating a default
Aug 10 16:42:56 Starting Pluto (Openswan Version 2.4.12 PLUTO_SENDS_VENDORID
Aug 10 16:42:56 Setting NAT-Traversal port-4500 floating to on
Aug 10 16:42:56 port floating activation criteria nat_t=1/port_fload=1
Aug 10 16:42:56 including NAT-Traversal patch (Version 0.6c)
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC_SSH: Ok
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC: Ok (re
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_SERPENT_CBC: Ok (re
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
Aug 10 16:42:56 ike_alg_register_enc(): Activating OAKLEY_BLOWFISH_CBC: Ok (r
Aug 10 16:42:56 ike_alg_register_hash(): hash alg=6 has ctx_size=216 > hash_c
Aug 10 16:42:56 ike_alg_register_hash(): Activating <none>: FAILED (ret=-75)
Aug 10 16:42:56 starting up 1 cryptographic helpers
Aug 10 16:42:56 started helper pid=2248 (fd:5)
Aug 10 16:42:57 Using NETKEY IPsec interface code on 2.6.18_pro500
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/cacerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/aacerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/ocspcerts'
Aug 10 16:42:57 Could not change to directory '//etc/ipsec.d/crls'

```

[HELP](#)

Figure 85. VPN – Tunnel Configuration Menu

Defining VPN Tunnels

To define VPN tunnels:

1. Click **VPN** in the menu bar.
2. On the VPN menu, uncheck **Disable IPsec VPN Functions** and click **Apply** (see Figure 83). Otherwise, the buttons for adding, editing, and deleting VPN tunnels on the VPN - Tunnel Configuration menu will be unavailable.
3. In the menu bar, under **VPN**, click the **IPsec Tunnel Configuration** submenu.
4. On the VPN – Tunnel Configuration menu, click **Add**. The VPN – Adding VPN Tunnel menu in Figure 86 appears.

SMC Networks Gateway Setup Home Logout

VPN - Adding VPN Tunnel

Local Host Setting/Intranet Configuration

Local ID	<input type="text"/>
Intranet Address	<input type="text"/>
Intranet Subnet Mask	<input type="text"/>

Remote Gateway

Remote Gateway ID	<input type="text"/>
Remote Gateway Address	<input type="text"/>
Pre-shared Key	<input type="text"/>

Key Management/IKE

IKE Life Duration	<input type="text"/> (>IPSec Life Duration)
Authentication method	Preshared Key
IKE Hash	MD5
IKE Encryption	BLOWFISH

IPSec

IPSec Operation	ESP
ESP Transform	DES
ESP AUTH	MD5
AH	MD5
Tunnel Type	Public
IPSec Life Duration	<input type="text"/> (>= 60 sec)

Tunnel Remote Host Configuration

IP type : IP Subnet	
1	Subnet Mask
<input type="text"/>	<input type="text"/>

[HELP](#)

Figure 86 VPN – Adding VPN Tunnel Menu

- Complete the fields in the VPN - Adding VPN Tunnel menu (see Table 34).
- Click **Apply**. (Or click **Back** to return to the VPN – Tunnel Configuration menu or **Cancel** to cancel any selections you made.) If you clicked **Apply**, the tunnel is added to the **Tunnel Table**.
- To define additional tunnels (up to five), repeat steps 4 through 6.
- To change the settings for a tunnel, click the radio button to the left of the tunnel you want to change and click the **Edit** button. When the VPN – Adding VPN Tunnel menu appears, edit the settings as necessary (see Table 34) and click **Apply**.

9. To delete a tunnel, click the radio button to the left of the tunnel you want to delete and click the **Delete** button. No precautionary message appears before you delete a tunnel.

Table 34. VPN – Adding VPN Tunnel Menu Options

Option	Description
Local Host Setting Intranet Configuration	
Protect Private Lan button	Click this button to automatically populate the Intranet Address and Intranet Subnet Mask fields with unique private LAN values.
Protect Public Lan button	Click this button to automatically populate the Intranet Address and Intranet Subnet Mask fields with unique public LAN values.
Local ID	ID to identify and authenticate the local host.
Intranet Address	IP address of the local host. You can manually add this information, or use the Protect Private Lan or Protect Public Lan button to auto-assign a unique IP address for the private or public LAN, respectively.
Intranet Subnet Mask	Subnet mask of the local host. You can manually add this information, or use the Protect Private Lan or Protect Public Lan button to auto-assign a unique subnet mask for the private or public LAN, respectively.
Remote Gateway	
Remote Gateway ID	ID to identify and authenticate the remote gateway at the other end of the VPN tunnel.
Remote Gateway Address	IP address of the remote gateway at the other end of the VPN tunnel.
Pre-shared Key	A "pass code" that must be the same at both the local and the remote side. Both ends of the tunnel must use the same key; otherwise, the VPN tunnel cannot be established.
Key Management / IKE	
IKE Life Duration	Length to time or amount of transfer before the Security Association is renegotiated.
Authentication method	Authentication mode used for keying the IPSec connection. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established.
IKE Hash	Checks that the data has not changed in transmission. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. Choices are: <ul style="list-style-type: none"> • MD5 = faster than SHA, but less secure. (<i>default</i>) • SHA = a one-way hashing algorithm that produces a 160-bit digest. SHA is more secure than MD5.
IKE Encryption	Encryption algorithm used during the Authentication phase. Choices are <ul style="list-style-type: none"> • BLOWFISH = a symmetric encryption algorithm that uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher that divides a message into fixed length blocks during encryption and decryption. Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits, and uses 16 rounds of main algorithm. (<i>default</i>) • 3DES = triple DES is a symmetric strong encryption algorithm that is compliant with the OpenPGP standard. It is the application of DES standard, where three keys are used in succession to provide additional security. • AES = Advanced Encryption Standard offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192, and 256 bits. The higher the bit rate, the stronger the encryption but the trade-off is lower throughput. More secure than 3DES. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established.

Option	Description
IPSec	
IPSec Operation	<p>Lets you select the IPSec operation. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. Choices are:</p> <ul style="list-style-type: none"> • ESP = Encapsulation Security Payload (ESP) protocol. ESP ensures both data authentication and confidentiality for IP data. ESP is able to guarantee both these services by creating a new IP packet within an ESP header and trailer. <i>(default)</i> • AH = Authentication Header (AH) protocol. AH ensures data integrity and replay protection for IP data. AH is able to guarantee data integrity by using a hash algorithm (such as MD5) and a secret shared key to produce a Hashed Message Authentication Code (HMAC).
ESP Transform	<p>Authentication algorithm used to encrypt packet data. Choices are</p> <ul style="list-style-type: none"> • DES = faster than 3DES, but less secure. <i>(default)</i> • 3DES = most secure method than DES, but with lower throughput. • BLOWFISH = a block cipher with 8-byte blocks and 128-bit keys that provides strong encryption and is faster than DES. • NONE = no authentication used. • AES = more secure than either DES or 3DES. The higher the bit rate, the stronger the encryption but the trade-off is lower throughput. • TWOFISH = a block cipher with 16-byte blocks and 256-bit keys that is stronger and faster than Blowfish encryption. <p>Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. This field is gray and unavailable if AH is selected for IPSec operation.</p>
ESP AUTH	<p>Authentication method used when ESP is selected for IPSec Operation. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. Choices are:</p> <ul style="list-style-type: none"> • MD5 = a one-way hashing algorithm that produces a 128-bit digest. <i>(default)</i> • SHA = a one-way hashing algorithm that produces a 160-bit digest. SHA is more secure than MD5. • SHA2_256 = a two-way hashing algorithm that produces a 256-bit digest. SHA2_256 is more secure than SHA. <p>This field is gray and unavailable if AH is selected for IPSec operation.</p>
AH	<p>Authentication method used when AH is selected for IPSec Operation. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. Choices are:</p> <ul style="list-style-type: none"> • MD5 = a one-way hashing algorithm that produces a 128-bit digest. <i>(default)</i> • SHA = a one-way hashing algorithm that produces a 160-bit digest. SHA is more secure than MD5. • SHA2_256 = a two-way hashing algorithm that produces a 256-bit digest. SHA2_256 is more secure than SHA. <p>This field is gray and unavailable if ESP is selected for IPSec operation.</p>
Tunnel Type	<p>Type of VPN tunnel to be established. Both ends of the tunnel must use the same setting; otherwise, the VPN tunnel cannot be established. Choices are:</p> <ul style="list-style-type: none"> • Public = public tunnel. <i>(default)</i> • Private = private tunnel.
IP Sec Life Duration	<p>Number of seconds for the IPSec lifetime. The period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint.</p>
Tunnel Remote Host Configurations	

Option	Description
IP type	IP Subnet.
IP Address	IP address of the remote endpoint.
Subnet Mask	Subnet mask of the remote endpoint.

Using the VPN Log

VPN log information appears below the tunnel table on the VPN – Tunnel Configuration menu. Buttons below the log let you clear or refresh (update) the log information displayed, or send the logs to a drive location. Before you can send the logs to a drive location, enable email and syslog notification on the Email/Syslog Alert menu (see page 125).

Using the VPN – PPTP / L2TP User Configuration Menu

Using the VPN – PPTP / L2TP User Configuration menu, you can set up to 50 PPTP / L2TP user accounts and define a pre-shared phrase. To access the VPN – PPTP / L2TP User Configuration menu, click **VPN** in the menu bar and then click the **PPTP/L2TP Configuration** submenu. Figure 87 shows an example of the menu.

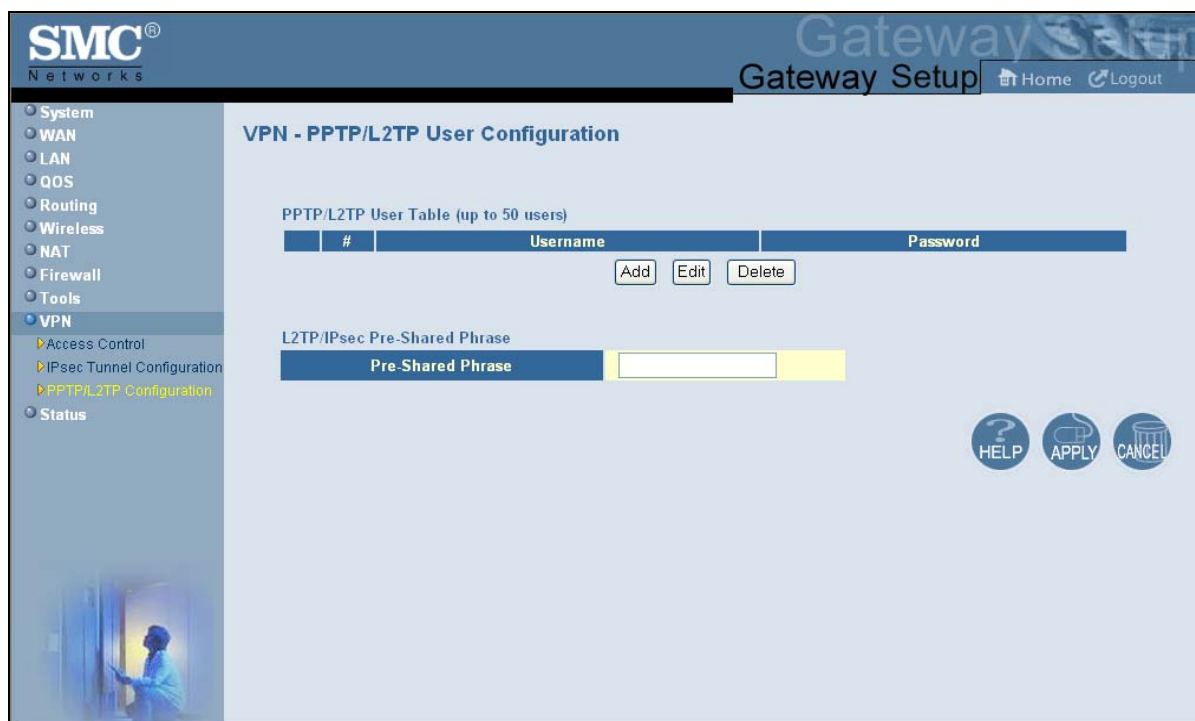


Figure 87. VPN – PPTP / L2TP User Configuration Menu

Defining PPTP / L2TP Users

Using the following procedure, you can add up to 50 PPTP / L2TP users.

1. Click **VPN** in the menu bar.
2. On the VPN menu, uncheck one of the following options and click **Apply** (see Figure 83). Otherwise, the buttons for adding, editing, and deleting the VPN – PPTP / L2TP configurations on the VPN – PPTP / L2TP User Configuration menu will be unavailable.
 - **Disable PPTP VPN Functions**
 - **Disable L2TP over IPsec VPN Functions**
3. In the menu bar, under **VPN**, click the **PPTP/L2TP Configuration** submenu.
4. In the VPN – PPTP / L2TP User Configuration menu, click the **Add** button. The Adding PPTP User menu in Figure 88 appears.



The screenshot shows the SMC Networks Gateway Setup interface. The top navigation bar includes the SMC Networks logo, the title 'Gateway Setup', and links for 'Home' and 'Logout'. A left sidebar menu lists various configuration categories: System, WAN, LAN, QOS, Routing, Wireless, NAT, Firewall, Tools, and VPN. The VPN menu is expanded, showing sub-items: Access Control, IPsec Tunnel Configuration, PPTP/L2TP Configuration, and Status. The main content area is titled 'Adding PPTP User' and contains the instruction: 'Set up the user account for PPTP/L2TP tunnel here.' Below this instruction are two input fields: 'User Name' and 'Password', both highlighted in yellow. At the bottom of the form are three buttons: 'Back', 'Apply', and 'Cancel'. A circular 'HELP' button is located in the bottom right corner of the main content area.

Figure 88. Adding PPTP User Menu

5. Complete the fields in the Adding PPTP User menu (see Table 35).
6. Click **Apply** to add the PPTP user. (Or click **Back** to return to the previous menu or **Cancel** to cancel the operation.) If you clicked **Apply**, the PPTP user is added to the **PPTP/L2TP User Table**.
7. To add more PPTP users (up to 50), repeat steps 4 through 6.

8. To change the settings for a PPTP user, click the radio button to the left of the PPTP user you want to change and click the **Edit** button. When the Adding PPTP User menu appears, edit the settings (see Table 35) and click **Apply**. Click **Apply** in the VPN – PPTP / L2TP User Configuration menu to save your settings.
9. To delete a PPTP user, click the radio button to the left of the PPTP user you want to delete and click the **Delete** button. No precautionary message appears before you delete a PPTP user. Click **Apply** in the VPN – PPTP / L2TP User Configuration menu to save your settings.

Table 35. Adding PPTP User Menu Options

Option	Description
User Name	Username used to authenticate the PPTP/L2TP user.
Password	Password used to authenticate the PPTP/L2TP user.

Defining L2TP / IPsec pre-shared Phrase

The configuration of L2TP with IPsec requires that all VPN clients and gateways use the same pre-shared key (or “phrase”). If the pre-shared phrase is changed because it has been compromised, you must manually change the phrase on each device that uses a pre-shared phrase to connect to the VPN gateway. A pre-shared phrase can be up to 256 characters. The longer and more complex the phrase, the harder it is to guess.

Using the VPN – PPTP / L2TP User Configuration menu, you can define the pre-shared phrase that the Gateway uses.

1. Click **VPN** in the menu bar.
2. On the VPN menu, uncheck one of the following options and click **Apply** (see Figure 83). Otherwise, the buttons for adding, editing, and deleting the VPN – PPTP / L2TP configurations on the VPN – PPTP / L2TP User Configuration menu will be unavailable.
 - **Disable PPTP VPN Functions**
 - **Disable L2TP over IPsec VPN Functions**
3. In the menu bar, under **VPN**, click the **PPTP/L2TP Configuration** submenu.
4. In the VPN – PPTP/L2TP User Configuration menu, under **L2TP/IPsec Pre-Shared Phrase**, enter the pre-shared phrase in the **Pre-Shared Phrase** field (see Figure 89).
5. Click the **Apply** button.

Figure 89. Pre-Shared Phrase Field

Viewing Status Information

The Status page is a read-only screen that shows the:

- Connection status for the Gateway's WAN and LAN interfaces
- Firmware and hardware versions
- Any illegal attempts to access your network
- Information about all DHCP clients currently connected to the Gateway
- Network and cable modem system event logs, with buttons for clearing, refreshing, or sending the logs to a drive location (before you can send the logs to a drive location, enable email and syslog notification on the Email/Syslog Alert menu - see page 125)
- LAN client log, with buttons for refreshing and releasing IP addresses

The Status menu appears when you first log in to the Web management interface. You can also display it by clicking Status in the menu bar.

SMC NETWORKS Gateway Setup Home Logout

Status

You can use the Status screen to see the connection status for the SMCD3GN2 WIRELESS interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your SMCD3GN2.

RG Functions: Enabled
 NAT: Enabled
 DHCP Server: Enabled
 Firewall: Enabled

Current Time: Thu Aug 11 16:37:14 2011 System Up Time: 807 days 03h:58m:46s

INTERNET	GATEWAY	INFORMATION
WAN IP: 10.30.20.229	DHCP Gateway IP Address: 192.168.2.1	Model Name: SMCD3GN2-0200
WAN Subnet Mask: 255.255.255.0	Subnet Mask: 255.255.255.0	Software Version: 3.1.2.1
WAN Gateway IP: 10.30.20.1		Hardware Version: 1A
Primary DNS: 192.168.2.111	DNS Proxy IP Address: 192.168.2.1	RF Cable MAC Address: 90.26.F3.02.FF.D0
Secondary DNS: 172.16.2.250		Wireless MAC Address: 90.26.F3.02.FF.D8
		RG WAN MAC Address: 90.26.F3.02.FF.D0
		Serial Num: 1215216AM1
		Operating Mode:

WIRELESS

SSID: 809F00
 Encryption Type: WPA
 Encryption Length: 64 Bits
 WPA Mode: Auto (WPA-PSK or WPA2-PSK)
 Cipher Type: TKIP and AES
 SSID MAC: 90.26.F3.02.FF.D8
 Channel Being Used: 11

Interfaces Uptime and Traffic Count

LAN Uptime: 17h 58m:46s Receiving 489796 bytes
 Sending 457383 bytes
 WAN Uptime: 03h 57m:00s Receiving 473314 bytes
 Sending 30952 bytes

Network Log

View network activity and security logs

```

(08/04/11 12:40:05) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/04/11 12:40:23) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/04/11 12:41:18) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/04/11 12:41:40) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/04/11 12:33:41) 10.229.1.11 rootadmin Login Failed(0000)
(08/04/11 12:39:58) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/04/11 14:01:38) 10.229.1.11 rootadmin Login Failed(Incorrect usernam
(08/08/11 07:12:51) 172.16.2.170 [Admin]:rootadmin Login Success
(08/08/11 12:44:33) 172.16.2.184 rootadmin Login Failed(Incorrect usernam
    
```

Clear Refresh Send the Logs

Cable Modem System Event Log

View Cable Modem operation (start up, get time etc)

```

Time:08/04/11 12:39:30, Level:warning, Content:R2ND Event R2ND: Stused R2
Time:08/04/11 12:39:30, Level:error, Content:Dnsproper Configuration File
    
```

Clear Refresh Send the Logs

HELP

Figure 90 shows an example of the status information shown.

SMC NETWORKS Gateway Setup Home Logout

Status

You can use the Status screen to see the connection status for the (SMCD3GN2) WIRELESS interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your (SMCD3GN2).

RG Functions: Enabled
 NAT: Enabled
 DHCP Server: Enabled
 Firewall: Enabled

Current Time: Thu Aug 11 16:37:14 2011 System Up Time: 807 days 83h:58m:46s

INTERNET	GATEWAY	INFORMATION
WAN IP: 10.30.20.229	DHCP Gateway IP Address: 192.168.2.1	Multi Name: SMCD3GN2-0200
WAN Subnet Mask: 255.255.255.0	Subnet Mask: 255.255.255.0	Software Version: 3.1.2.1
WAN Gateway IP: 10.30.20.1		Hardware Version: 1A
Primary DNS: 192.168.2.111	DNS Proxy IP Address: 192.168.2.1	RF Cable MAC Address: 90.26.F3.82.FF.D0
Secondary DNS: 172.16.2.250		Wireless MAC Address: 90.26.F3.82.FF.D8
		RG WAN MAC Address: 90.26.F3.82.FF.D0
		Serial Num: 12151316AM1
		Operating Mode:

WIRELESS

SSID: 82PFD0
 Encryption Type: WPA
 Encryption Length: 64 Bits
 WPA Mode: Auto (WPA-PSK or WPA2-PSK)
 Cipher Type: TKIP and AES
 SSID MAC: 90.26.F3.82.FF.D8
 Channel Being Used: 11

Interfaces Uptime and Traffic Count

LAN Uptime: 17h 58m:46s / Receiving 4889796 bytes / Sending 4077883 bytes
 WAN Uptime: 83h 57m:00s / Receiving 4733114 bytes / Sending 30952 bytes

Network Log

View network activity and security logs

```

(08/04/11 12:40:05) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/04/11 12:40:23) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/04/11 12:41:18) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/04/11 12:41:40) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/04/11 12:33:41) 10.229.1.11 root@smcd3gn2 Login Failed(Empty)
(08/04/11 12:39:58) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/04/11 14:01:38) 10.229.1.11 root@smcd3gn2 Login Failed(Incorrect usernam
(08/08/11 07:12:51) 172.16.2.170 [admin]:root@smcd3gn2 Login Success
(08/08/11 12:44:33) 172.16.2.184 root@smcd3gn2 Login Failed(Incorrect usernam
    
```

Clear Refresh Send the Logs

Refresh IP Release

Cable Modem System Event Log

View Cable Modem operation (start up, get time etc)

```

Time:08/04/11 12:39:30, Level:warning, Content:R2ND Event R2ND: Staged R2
Time:08/04/11 12:39:30, Level:error, Content:Dnsproper Configuration File
    
```

Clear Refresh Send the Logs

HELP

Figure 90. Example of Status Page

Viewing Cable Status Information

The Cable Status page is a read-only screen that shows the user's cable initialization procedures, along with the cable upstream and downstream status.

The Cable Status menu appears when you first log in to the Web management interface. You can also display it by clicking Status in the menu bar and then clicking the Cable Status submenu.

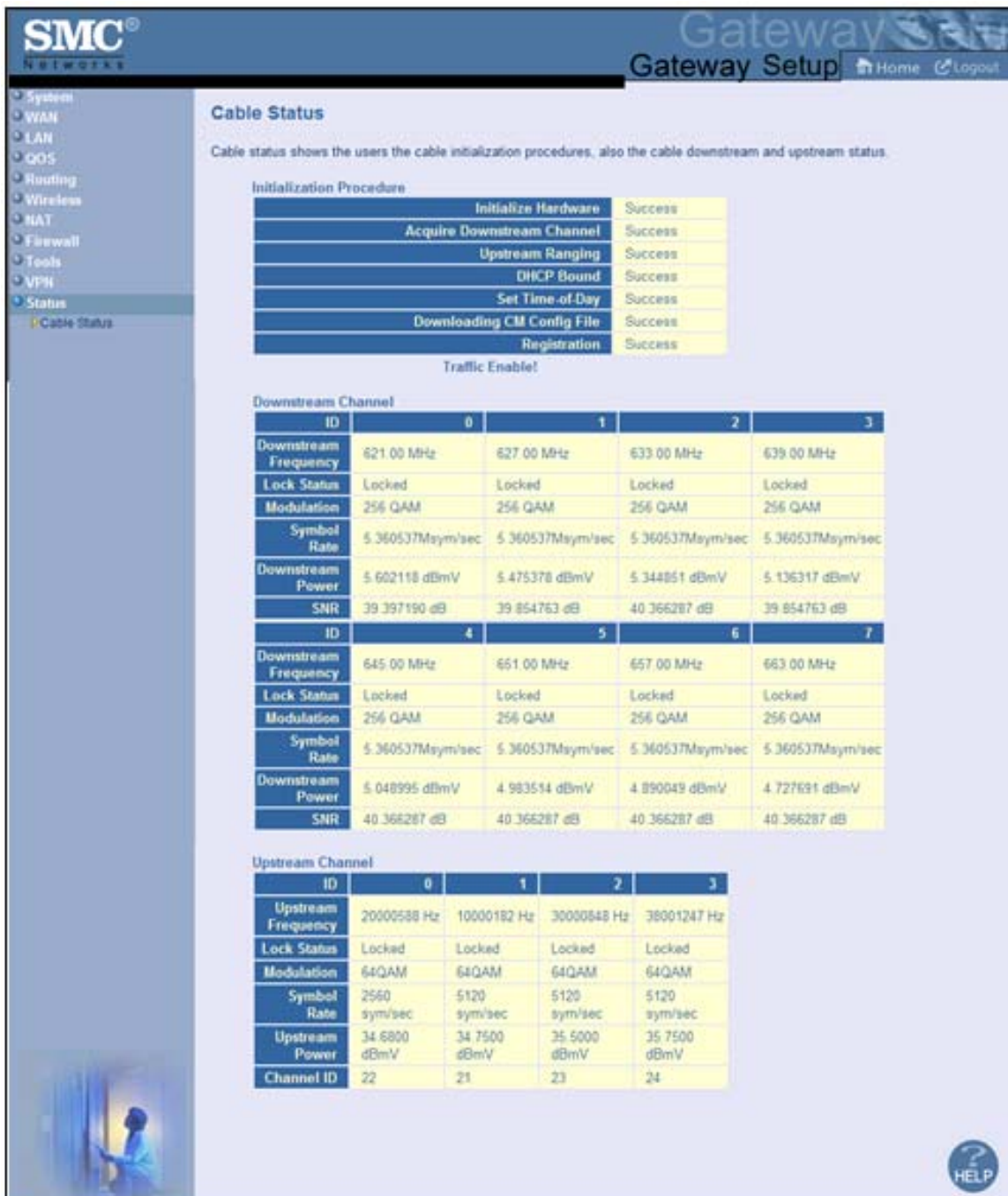


Figure 91 shows an example of the cable status information shown.

SMC Networks Gateway Setup Home Logout

- System
- WAN
- LAN
- QOS
- Routing
- Wireless
- NAT
- Firewall
- Tools
- VPN
- Status
 - Cable Status

Cable Status

Cable status shows the users the cable initialization procedures, also the cable downstream and upstream status.

Initialization Procedure

Procedure	Status
Initialize Hardware	Success
Acquire Downstream Channel	Success
Upstream Ranging	Success
DHCP Bound	Success
Set Time-of-Day	Success
Downloading CM Config File	Success
Registration	Success

Traffic Enable!

Downstream Channel

ID	0	1	2	3
Downstream Frequency	621.00 MHz	627.00 MHz	633.00 MHz	639.00 MHz
Lock Status	Locked	Locked	Locked	Locked
Modulation	256 QAM	256 QAM	256 QAM	256 QAM
Symbol Rate	5.360537Msym/sec	5.360537Msym/sec	5.360537Msym/sec	5.360537Msym/sec
Downstream Power	5.602118 dBmV	5.475378 dBmV	5.344851 dBmV	5.136317 dBmV
SNR	39.397190 dB	39.854763 dB	40.366287 dB	39.854763 dB

ID	4	5	6	7
Downstream Frequency	645.00 MHz	651.00 MHz	657.00 MHz	663.00 MHz
Lock Status	Locked	Locked	Locked	Locked
Modulation	256 QAM	256 QAM	256 QAM	256 QAM
Symbol Rate	5.360537Msym/sec	5.360537Msym/sec	5.360537Msym/sec	5.360537Msym/sec
Downstream Power	5.048995 dBmV	4.983514 dBmV	4.890049 dBmV	4.727691 dBmV
SNR	40.366287 dB	40.366287 dB	40.366287 dB	40.366287 dB

Upstream Channel

ID	0	1	2	3
Upstream Frequency	20000588 Hz	10000182 Hz	30000848 Hz	38001247 Hz
Lock Status	Locked	Locked	Locked	Locked
Modulation	64QAM	64QAM	64QAM	64QAM
Symbol Rate	2560 sym/sec	5120 sym/sec	5120 sym/sec	5120 sym/sec
Upstream Power	34.6800 dBmV	34.7500 dBmV	35.5000 dBmV	35.7500 dBmV
Channel ID	22	21	23	24

HELP

Figure 91. Example of Cable Status Page

Appendix A - Compliances

FCC 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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference. 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.

The 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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A is firmware-limited to channels 1 through 11.

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 & your body.

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - The cable distribution system should be grounded (earthed) in accordance with ANSI/NFPA 70, the National Electrical Code (NEC), in particular Section 820.93, Grounding of Outer Conductive Shield of a Coaxial Cable.

- 1
- 1-to-1 Mapping menu, 98
- A**
- Access control, 103
 - adding customer-defined access rule, 107
 - adding customer-defined filter, 112
 - adding predefined access rule, 104
 - adding predefined filter, 110
- Access Control (VPN) menu, 143
- Access Control menu, 103
- Adding
 - customer-defined access rule for access control, 107
 - customer-defined filter for access control, 112
 - customer-defined service for port forwarding, 95
 - predefined access rule for access control, 104
 - predefined filter for access control, 110
 - predefined service for port forwarding, 93
- Additional Public Lan menu, 55
- Advanced Wireless Settings menu, 89
- Alert options, 124
- Alerts, 121
- Apple Macintosh TCP/IP configuration, 26
- Auto-negotiation, 50
- B**
- Blocking
 - domain, 120
 - keyword, 119
- C**
- Cable Status menu, 154
- Changing login password, 38
- Cipher type, 81
- Computer exempted from URL blocking, 119
- Configuration, 28
- Configuring
 - access control, 103
 - alert options, 124
 - auto-negotiation, 50
 - DHCP, 48
 - duplex mode, 50
 - email alerts, 123
 - firewall, 101
 - idle timeout, 38
 - login password, 38
 - port forwarding, 92
 - private LAN IP address, 48
 - special applications, 115
 - syslog entries, 124
 - TCP/IP, 19
 - wireless security, 14
- Connecting
 - LAN, 17
 - WAN, 18
- Conventions in this document, viii
- CoS Settings menu, 62
- Customer UI Setup menu, 43
- Customer-defined
 - service for port forwarding, 95
 - service table, 92
- Customer-defined access rule, 107
- Customer-defined filter, 112
- D**
- DHCP setting, 48
- Diagnostics menu, 134
- Disabling
 - firewall, 30

- LAN ports, 50
- security software, 30
- VPN, 141
- Disabling proxy settings
 - Firefox, 29
 - Internet Explorer, 29
 - Safari, 30
- DMZ (Demilitarized Zone) menu, 125
- Document
 - conventions, viii
 - organization, viii
- Domain blocking, 120
- DSCP Based QoS menu, 64
- DSCP Remarking menu, 68
- Duplex mode, 50

E

- Email alerts, 121, 123
- Email/Syslog Alert menu, 121
- Enabling
 - VPN, 141
- Enabling LAN ports, 50
- Ether Switch Port Control menu, 50
- Exempted computers, 119

F

- Factory defaults
 - restoring, 15
- Firefox, disabling proxy settings, 29
- Firewall
 - configuring, 101
 - disabling, 30
- Front panel, 12
 - LEDs, 13

G

- Gateway
 - configuring, 28
 - connecting to the LAN, 17
 - connecting to the WAN, 18
 - front panel, 12

- installing, 16
- key features, vii
- LEDs, 13
- locating, 17
- package contents, 11
- powering on, 18
- preconfiguring, 29
- rear panel, 14
- rebooting and losing custom settings, 15, 132
- system requirements, 11
- Web management, 31

I

- Idle timeout, 38
- Ignoring pings, 114
- Installation, 16
- Internet Explorer, disabling proxy settings, 29

K

- Key features, vii
- Keyword blocking, 119

L

- LAN Access Control menu, 51
- LAN connection, 17
- LAN ports, enabling or disabling, 50
- LAN Settings menu, 48
- Lease time, 48
- LEDs, 13
- Locating the Gateway, 17
- Logging in to Web management, 31
- Login password, 38

M

- MAC Spoofing menu, 47
- Menus
 - 1-to-1 Mapping, 98
 - Access Control, 103
 - Access Control (VPNs), 143
 - Additional Public Lan, 55
 - Advanced Wireless Settings, 89

- Cable Status, 154
 - CoS Settings, 62
 - Customer UI Setup, 43
 - Diagnostics, 134
 - DMZ (Demilitarized Zone), 125
 - DSCP Based QoS, 64
 - DSCP Remarking, 68
 - Email/Syslog Alerts, 121
 - Ether Switch Port Control, 50
 - LAN Access Control, 51
 - LAN Settings, 48
 - MAC Spoofing, 47
 - NAT Settings, 91
 - OSPF Control, 75
 - Password Settings, 38
 - Port Based QoS, 61
 - Port Forwarding, 92
 - Public IP Access Control, 57
 - QoS Settings, 59
 - Queue Settings, 66
 - Reboot, 132
 - Remote Management, 42
 - RIP Control, 72
 - Routing, 70
 - Schedule Rules, 120
 - Security Settings (Firewall), 101
 - SNTP Settings, 140
 - Special Application, 115
 - Static Routes, 70
 - Status, 152
 - System Settings, 36
 - Trigger, 116
 - URL Blocking, 118
 - VPN, 141
 - VPN – PPTP / L2TP User Configuration, 149
 - VPN – Tunnel Configuration, 144
 - WAN Settings, 45
 - Wireless Basic Settings, 79
 - Wireless Encryption Settings, 81
 - WPS Setup, 84
 - Microsoft
 - TCP/IP configuration for Windows 2000, 20
 - TCP/IP configuration for Windows 7, 24
 - TCP/IP configuration for Windows Vista, 22
 - TCP/IP configuration for Windows XP, 21
- N
- NAT Settings menu, 91
- O
- OSPF, 75
- P
- Package contents, 11
 - Password Settings menu, 38
 - Password, changing, 38
 - Ping, 134
 - Pings, responding to or ignoring, 114
 - Port Based QoS menu, 61
 - Port forwarding
 - adding customer-defined service, 95
 - adding predefined service, 93
 - Port Forwarding menu, 92
 - Port triggering, 116
 - Powering-on the Gateway, 18
 - Preconfiguration guidelines, 29
 - Predefined
 - service for adding port forwarding, 93
 - service table, 92
 - Predefined access rule, 104
 - Predefined filter, 110
 - Private LAN IP settings
 - DHCP, 48
 - domain name, 48
 - IP address, 48
 - IP subnet mask, 48
 - lease time, 48
 - Proxy settings, 29
 - Public IP Access Control Lan menu, 57
- Q
- QoS Settings menu, 59
 - Queue Settings menu, 66

R

RADIUS configuration, 38
 Rear panel, 14
 Reboot menu, 132
 Rebooting
 losing custom settings, 15, 132
 Remote Management menu, 42
 Requirements, 11
 Responding to pings, 114
 Restoring factory defaults, 15
 RIP, 72
 Routing menu, 70

S

Safari, disabling proxy settings, 30
 Schedule Rules menu, 120
 Screens in Web management, 32
 Security mode, 81
 Security Settings (Firewall) menu, 101
 Security software, 30
 Security, configuring wireless, 14
 Service table
 customer-defined, 92
 predefined, 92
 SNMP Settings menu, 140
 Special Application menu, 115
 Spoofing MAC addresses, 47
 SSID setting, 81
 SSIDs, 79
 Static Routes menu, 70
 Status menu, 152
 Syslog
 alerts, 121
 entries, 124
 System requirements, 11
 System Settings menu, 36

T

TACACS configuration, 38
 TACACS+ configuration, 38
 TCP/IP configuration, 19

Apple Macintosh, 26
 Microsoft Windows 2000, 20
 Microsoft Windows 7, 24
 Microsoft Windows Vista, 22
 Microsoft Windows XP, 21
 Timeout for Web management session, 38
 Trace route, 134
 Trigger menu, 116
 Triggering ports, 116

U

URL Blocking menu, 118

V

VPN – PPTP / L2TP User Configuration menu, 149
 VPN – Tunnel Configuration menu, 144
 VPN menu, 141

W

WAN connection, 18
 WAN ping, 134
 WAN Settings menu, 45
 WAN trace route, 134
 Web management
 1-to-1 Mapping menu, 98
 Access Control menu, 103
 Access Control menu (VPNs), 143
 Additional Public Lan menu, 55
 Advanced Wireless Settings menu, 89
 Cable Status menu, 154
 CoS Settings, 62
 Customer UI Setup menu, 43
 Diagnostics menu, 134
 DMZ (Demilitarized Zone) menu, 125
 DSCP Based QoS, 64
 DSCP Remarking, 68
 Ether Switch Port Control menu, 50
 LAN Access Control menu, 51
 LAN Settings menu, 48
 logging in, 31
 MAC Spoofing menu, 47

- NAT Settings menu, 91
- OSPF Control menu, 75
- Password Settings menu, 38
- Port Based QoS, 61
- Port Forwarding menu, 92
- Public IP Access Control menu, 57
- QoS Settings menu, 59
- Queue Settings, 66
- Reboot menu, 132
- Remote Management menu, 42
- RIP Control menu, 72
- Routing menu, 70
- Schedule Rules menu, 120
- screens, 32
- Security Settings (Firewall) menu, 101
- SNTP Settings menu, 140
- Special Application menu, 115
- Static Routes menu, 70
- Status menu, 152
- System Settings menu, 36
- Trigger menu, 116
- URL Blocking menu, 118
- URL Email/Syslog Alert menu, 121
- VPN – PPTP / L2TP User Configuration menu, 149
- VPN – Tunnel Configuration menu (VPNs), 144
- VPN menu, 141
- WAN Settings menu, 45
- Wireless Basic Settings menu, 79
- Wireless Encryption Settings menu, 81
- WPS Setup menu, 84
- Wireless
 - mode, 79
 - operation, 79
 - security, 14
- Wireless Basic Settings menu, 79
- Wireless Encryption Settings menu, 81
- WPA mode, 81
- WPS Setup menu, 84



20 Mason
Irvine, CA. 92618
U.S.A.
<http://www.smc.com>

Document number: 3121RRR081111