SMC®
Networks

User Manual

SMCD3GN

DOCSIS 3.0 Wireless Cable Modem Gateway

FASTFIND LINKS

Getting to Know Your Gateway

Installing Your Gateway

Configuring Your Computer for TCP/IP

Configuring Your Gateway

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

SMCD3GN Wireless Cable Modem Gateway User Manual

Contents

SMCD3GN Wireless Cable Modem Gateway User Manual

Preface

Congratulations on your purchase of the SMCD3GN Wireless Cable Modem Gateway. The SMCD3GN 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 you need to install and configure your new SMCD3GN Wireless Cable Modem Gateway.

SMCD3GN Wireless Cable Modem Gateway User Manual

Key Features

The following list summarizes the Gateway's key features.

- Integrated, CableLabs-compliant DOCSIS 1.1/ 2.0 /3.0 cable modem.

- Integrated cable modem port for Internet connection to cable modem service.

- Four 10/100/1000 Mbps Auto-Sensing LAN ports with Auto-MDI/MDIX.

- High-speed 300 Mbps IEEE 802.11n Wireless Access Point.

- Internet connection to cable modem service via an integrated cable modem port.

- 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 any UPnP device seamlessly.

- 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 your Gateway package, system requirements, and an overview of the Gateway's front and rear panels.

- **Chapter 2** - describes how to install your Gateway.

- **Chapter 3 -** describes how to configure TCP/IP settings on the computer you will use to configure your Gateway.

- **Chapter 4** - describes how to configure your Gateway.

- **Appendix A -** lists the Gateway's specifications.

- **Appendix B -** 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.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
screen/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 Your Gateway

Before you install your SMCD3GN 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

Unpack the items in your SMCD3GN Wireless Cable Modem Gateway contents and confirm that no items are missing or damaged. Your package should include:

- One SMCD3GN Wireless Cable Modem Gateway

- One Power adapter (12V/2A)

- One Category 5E Ethernet cable

- One CD that contains this User Manual

If any items are missing or damaged, please contact your place of purchase. Keep the carton, including the original packing material, in case you need to store the product or return it.

System Requirements

To complete your 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 your SMCD3GN Wireless Cable Modem Gateway contains a set of light-emitting diode (LED) indicators. These LEDs show the status of your Gateway and simplify troubleshooting.

Figure 1 shows the front panel of the SMCD3GN Wireless Cable Modem Gateway. Table 1 describes the front panel LEDs.

Figure 1. Front Panel of the SMCD3GN 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.
LINK	Green	Blinking = data is transmitting. ON = Gateway is operational. OFF = no Ethernet link detected.
DIAG	Amber	ON = system failure. OFF = normal operation.
LAN 1 – LAN 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 GMbps. 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 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 goes 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 your SMCD3GN 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.
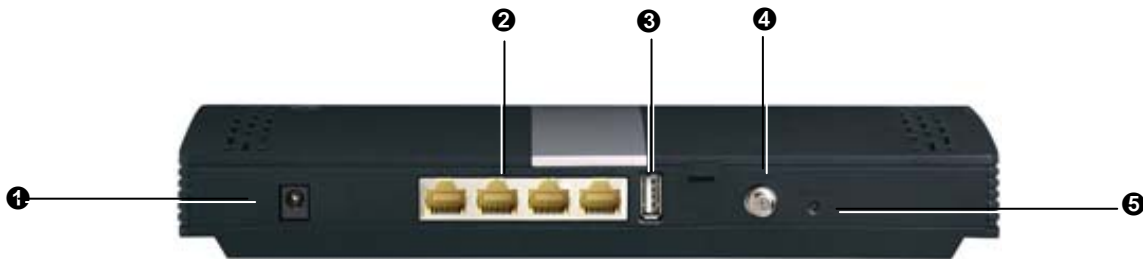
Figure 2. Rear View of the SMCD3GN Wireless Cable Modem Gateway

Table 2. SMCD3GN Wireless Cable Modem Gateway Rear Panel Components

	Item	Description
❶	Power (12VDC)	Connect the supplied power adapter to this port.
❷	LAN 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.
❸	USB	USB 2.0 high-speed port for storing configurations externally.
❹	Cable	Connect your coaxial cable line to this port.
❺	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 your Gateway.

Restoring Factory Defaults

Using the Reset button on the back panel, you can power cycle the Gateway and return it to its original factory default settings. As a result, any changes you made to the Gateway's default settings will be removed. To reset the Gateway and keep any overrides you made to the factory default settings, use the software reset method described under "Using the Reboot Menu to Reboot the Gateway" on page 59.

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.

This chapter describes how to install your SMCD3GN Wireless Cable Modem Gateway. The topics covered in this chapter are:

- Finding a Suitable Location (page 16)

- Connecting to the LAN (page 16)

- Connecting the WAN (page 17)

- Powering on the Gateway (page 17)

Finding a Suitable Location

Your SMCD3GN 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 you 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. Your Gateway 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 **LAN** ports on the rear panel of the Gateway (see Figure 3).
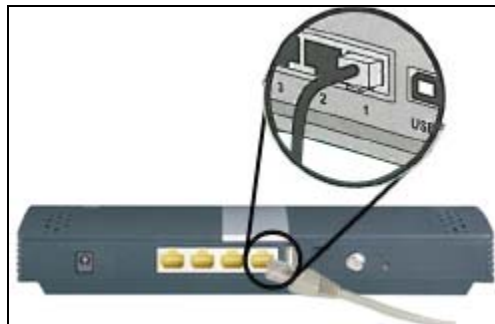

Figure 3. Connecting to a LAN Port on the Gateway Rear Panel

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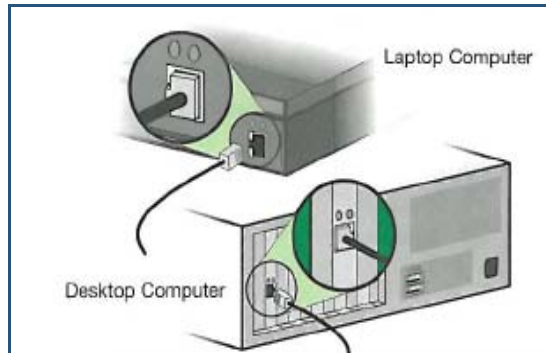

Figure 4. Connecting the Gateway to the a Laptop or Desktop Computer

Connecting the WAN

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

1. 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 13). Use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.

2. Hand-tighten the connectors to secure the connection.

3. If the modem was not installed by your cable provider (ISP) or is replacing another cable modem, contact your cable operator to register the SMCD3GN. If the modem is not registered with your cable operator, it will be unable to connect to the cable network system.

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 adapter to the port labeled **12VDC** on the rear panel of the Gateway (see Figure 2 on page 13).

2. Connect the other end of the power adapter 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 12).

⚠ **WARNING:** Only use the power adapter supplied with the Gateway. Using a different power adapter can damage your Gateway and void the warranty.

3 Configuring Your Computer for TCP/IP

After you install your SMCD3GN Wireless Cable Modem Gateway, configure the TCP/IP settings on a computer that will be used to configure your 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 19)

- Configuring Microsoft Windows XP (page 20)

- Configuring Microsoft Windows Vista (page 21)

- Configuring an Apple® Macintosh® Computer (page 23)

SMCD3GN Wireless Cable Modem Gateway User Manual

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).
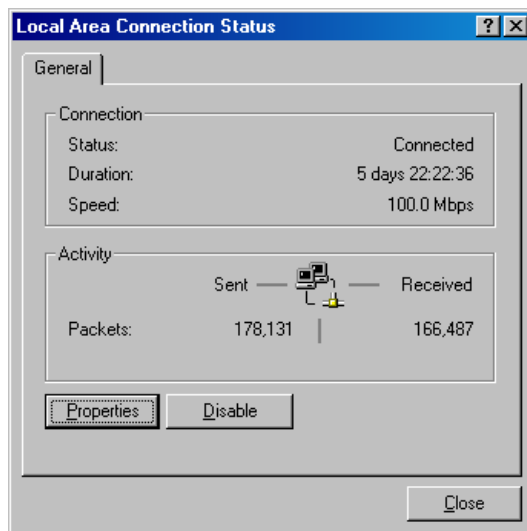

Figure 5. Local Area Connection Status Window

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.

SMCD3GN Wireless Cable Modem Gateway User Manual

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 19.

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.
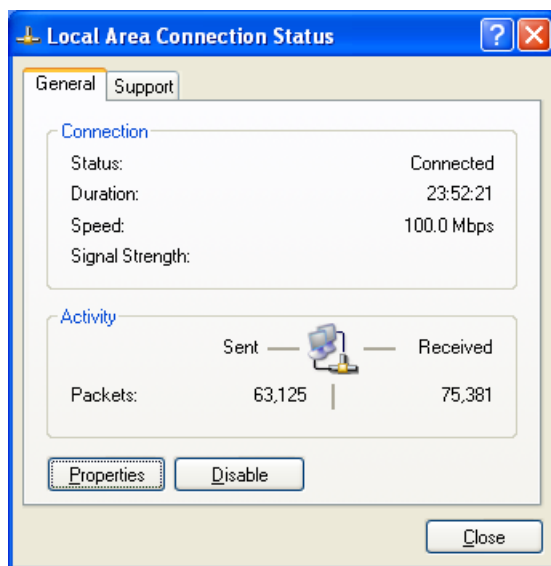
Figure 6. Local Area Connection Status Window

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 19.

1. On the Windows taskbar, click Start, click Control Panel, and then select 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.
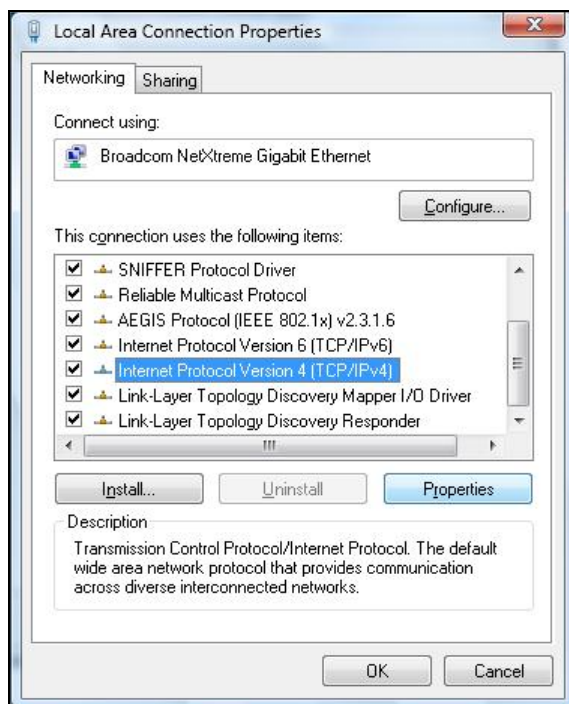

Figure 7. Local Area Connection Properties Window

21

SMCD3GN Wireless Cable Modem Gateway User Manual

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).
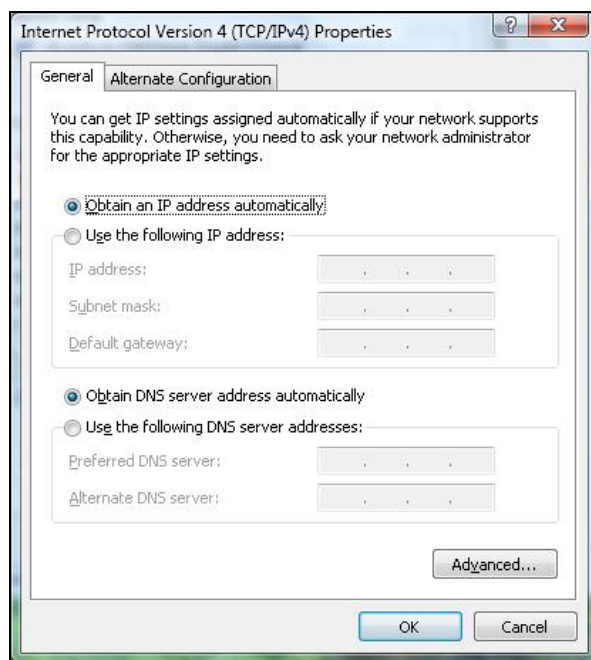

Figure 8. Internet Protocol Properties Window

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

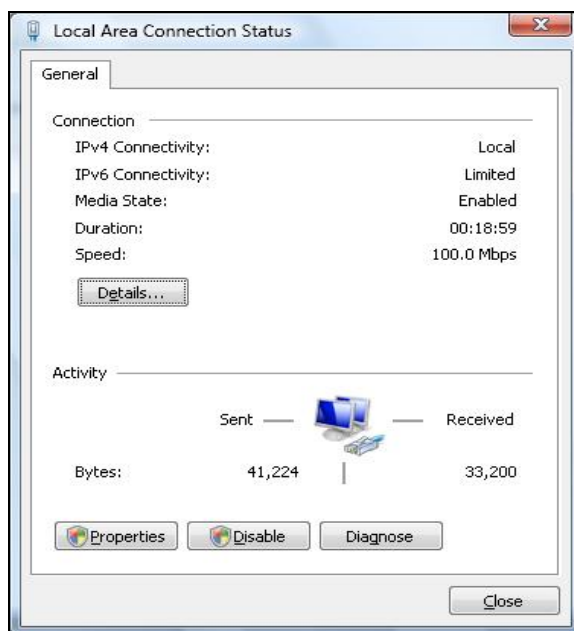8. Click the **OK** button again to save your changes.

Figure 9. Local Area Connection Status Window

22
SMCD3GN Wireless Cable Modem Gateway User Manual

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.

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

2. Verify that NIC connected to the SMCD3GN is selected in the **Show** field.

3. In the **Configure** field on the **TCP/IP** tab, select **Using DHCP** (see Figure 10).

4. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.

Figure 10. Selecting Using DHCP in the Configure Field

4 Configuring Your Gateway

After configuring your computer for TCP/IP using the procedure appropriate for your operating system, use that computer's Web browser to configure your SMCD3GN Gateway. This chapter describes how to use your Web browser to configure your Gateway.

The topics covered in this chapter are:

- Pre-configuration Guidelines (page 25)

- Accessing the Gateway's Web Management (page 27)

- Understanding the Web Management Interface Screens (page 28)

- Web Management Interface Menus (page 29)

Pre-configuration Guidelines

Before you configure your 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.

Confirming Your Gateway's Link Status

Confirm that the **LINK** LED on the Gateway front panel is ON (see Figure 1 on page 11). If the LED is OFF, replace the Ethernet cable connecting your computer and Gateway.

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 your Gateway from the convenient Web-based management interface. From your Web browser (Microsoft Internet Explorer or Netscape Navigator, versions 5.0 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 SMCD3GN Wireless Cable Modem Gateway's web-based management screens, use the following procedure.

1. Launch a Web browser.

Note: Your computer does not have to be online to configure your Gateway.

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

Address http://192.168.0.1/

The Login User Password screen appears (see Figure 11)

LOGIN USER PASSWORD

Login Screen

Username: [   ]

Password: [   ]

[LOGIN] [CANCEL]

Figure 11. Login User Password Screen

3. In the Login User Password screen, enter the default username **cusadmin** and the default password **password**. Both the username and password are case sensitive. After you log in to the Web management interface, we recommend you change the default password on the Password Settings menu (see page 31).

Note: Your cable modem operator may customize the login password, so please check with your operator for the correct password to use.

4. Click the **Login** button to access the Gateway. The Status page appears, showing connection status information about your 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 12). If the displayed information exceeds that 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.
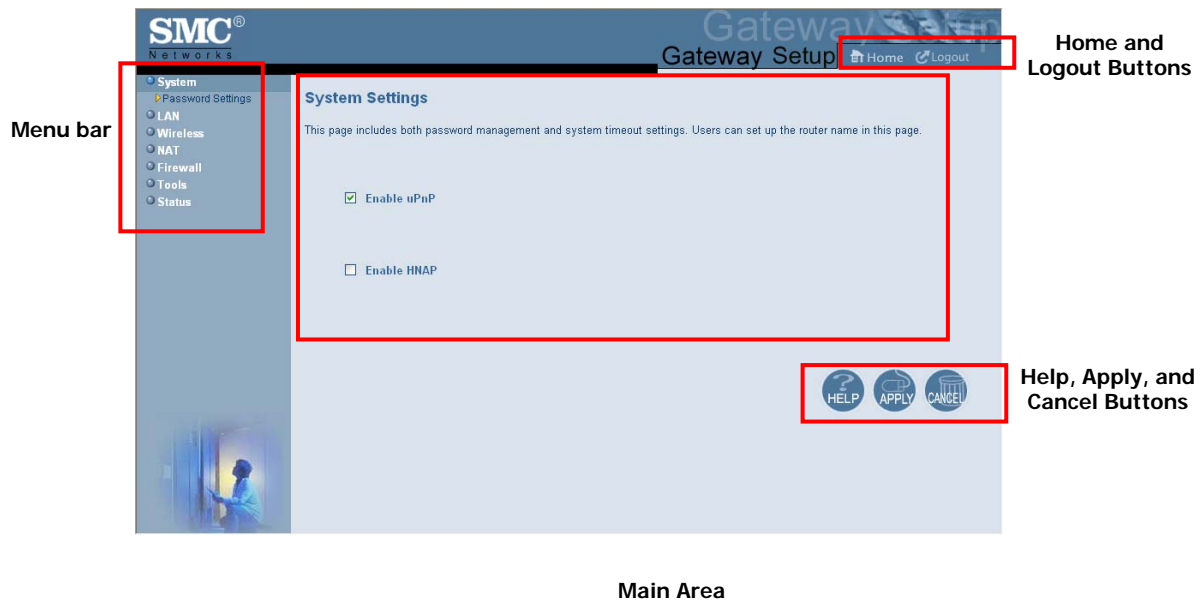
Main Area

Figure 12. 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 submenu **Password Settings** appears below the **System** menu (see Figure 13).
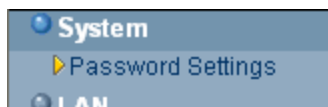

Figure 13. Example of System Submenu

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

Table 3 describes the menus in the Web management interface.

Table 3. Web Management Interface Menus

Menu	Description	See Page
System Settings	Lets you enable or disable UPnP.	30
Password Settings	Lets you configure and manage password settings and set the system timeout.	31
Wireless	Lets you configure the wireless, encryption, MAC filtering, and advanced wireless settings.	35
NAT	Lets you configure predefined and custom port forwarding settings to allow Internet users to access local services such as the Web Server or FTP server at your local site.	43
Firewall	Lets you configure firewall settings to limit the risk of hacker attack. Submenus let you configure a specific client/server as a demilitarized zone (DMZ) that is exempt from the firewall limitations and protection.	48
Tools	Lets you reboot the Gateway.	59
Status	Shows the connection status of your Gateway. This is the same screen that appears when you log in to the Gateway.	60

System Settings Menu

The System Settings menu lets you:

- Enable or disable UPnP and HNAP

- Configure and manage your password

- Set the system timeout settings

To access the System Settings menu, click **System** in the menu bar. Figure 14 shows an example of the menu and Table 4 describes the setting you can select.
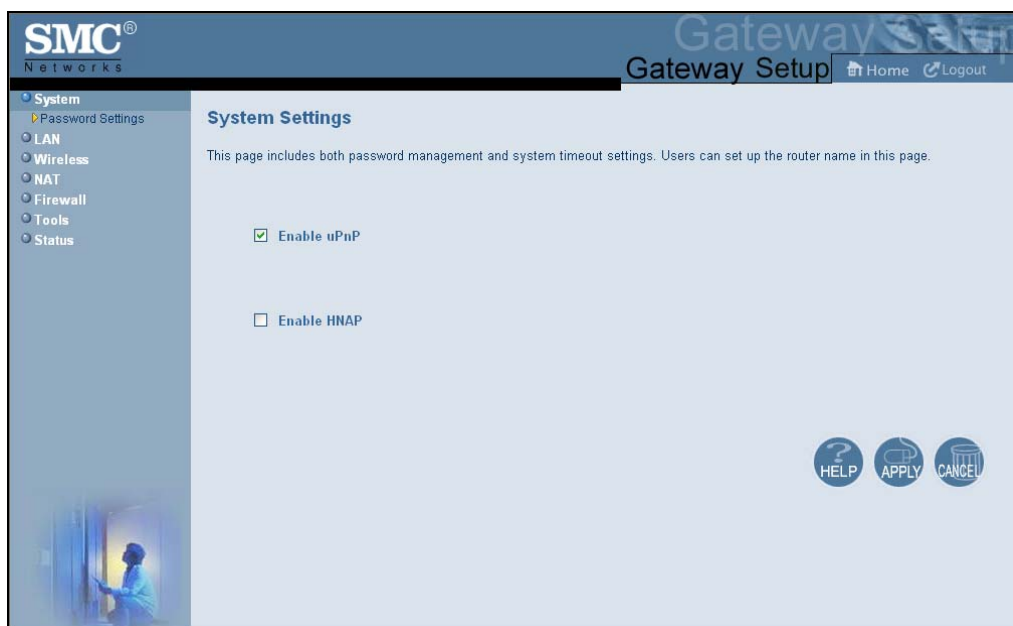

Figure 14. System Settings Menu

Table 4. System Settings Menu Option

Option	Description
Enable UPnP	Configures your 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 your 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. Check = uPnP is enabled on the Gateway. (*default*) Uncheck = uPnP is disabled on the Gateway.
Enable HNAP	Configures your Gateway as a Home Network Administration Protocol (HNAP) device. HNAP allows your Gateway to be configured and managed by remote entities, such as Network Magic or any software application that discovers and manages network devices. Check = HNAP is enabled on the Gateway. Uncheck = HNAP is disabled on the Gateway. (*default*)

Password Settings Menu

The Password Settings menu lets you change the Gateway's default password. The first time you log in to the Web management interface, we recommend you change the Gateway's default password to protect it from being tampered with.

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.

To access the Password Settings menu, click **System** in the menu bar and then click the **Password Settings** submenu. Figure 15 shows an example of the menu and Table 5 describes the settings you can select.

Figure 15. Password Settings Menu

Table 5. Password Settings Menu Options

Option	Description
Current Password	Enter the current case-sensitive password. For security purposes, every typed character appears as a dot (•). The default password is **password**.
New Password	Enter the new case-sensitive 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 password you typed in the **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.

LAN Settings Menu

The LAN Settings menu lets you configure the LAN IP settings for the Gateway. The private LAN IP is also the IP of the DHCP server that dynamically allocates IP addresses for client computers located behind the Gateway.

To access the LAN Settings menu, click **LAN** in the menu bar. Figure 16 shows an example of the menu and Table 6 describes the settings you can select.
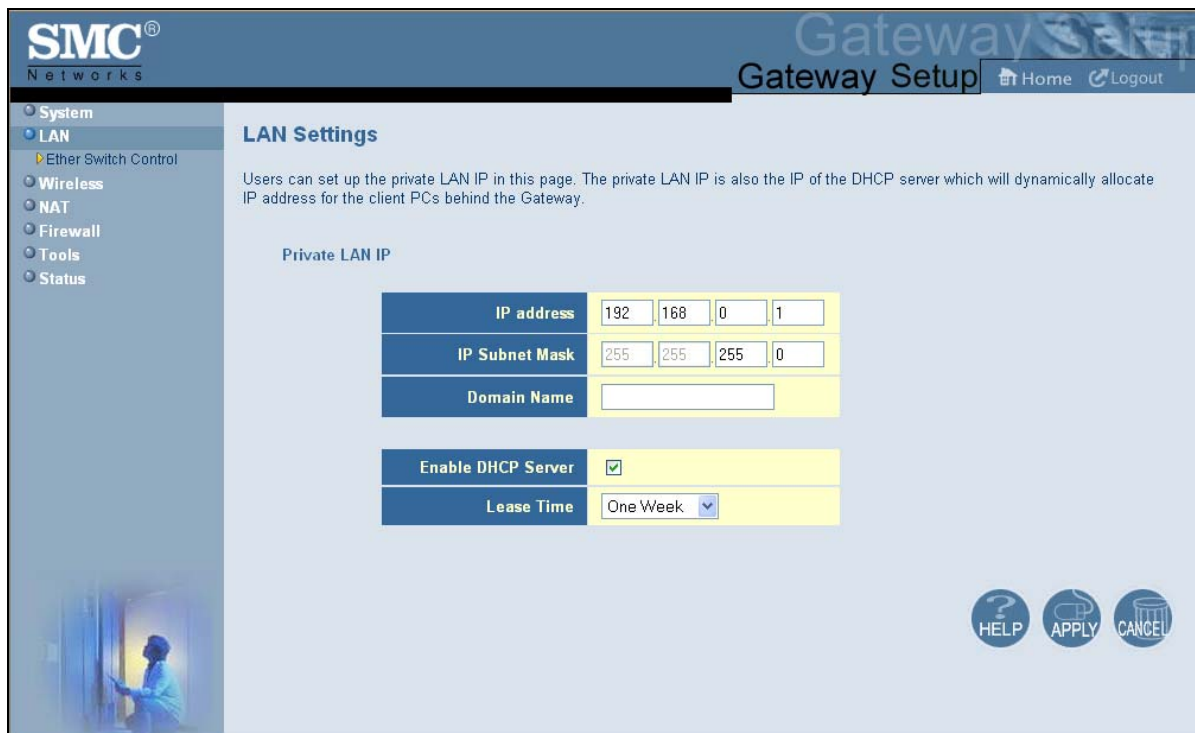
Figure 16. LAN Settings Menu

SMCD3GN Wireless Cable Modem Gateway User Manual

Table 6. LAN Settings Menu Options

Option	Description
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 for dynamic client address allocation. • Checked = DHCP server is enabled. (default) • 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.

Ether Switch Port Control Menu

By default, your Gateway are enabled and configured to auto-negotiate speed and duplex on its four LAN ports. 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 specific 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 17 shows an example of the menu.
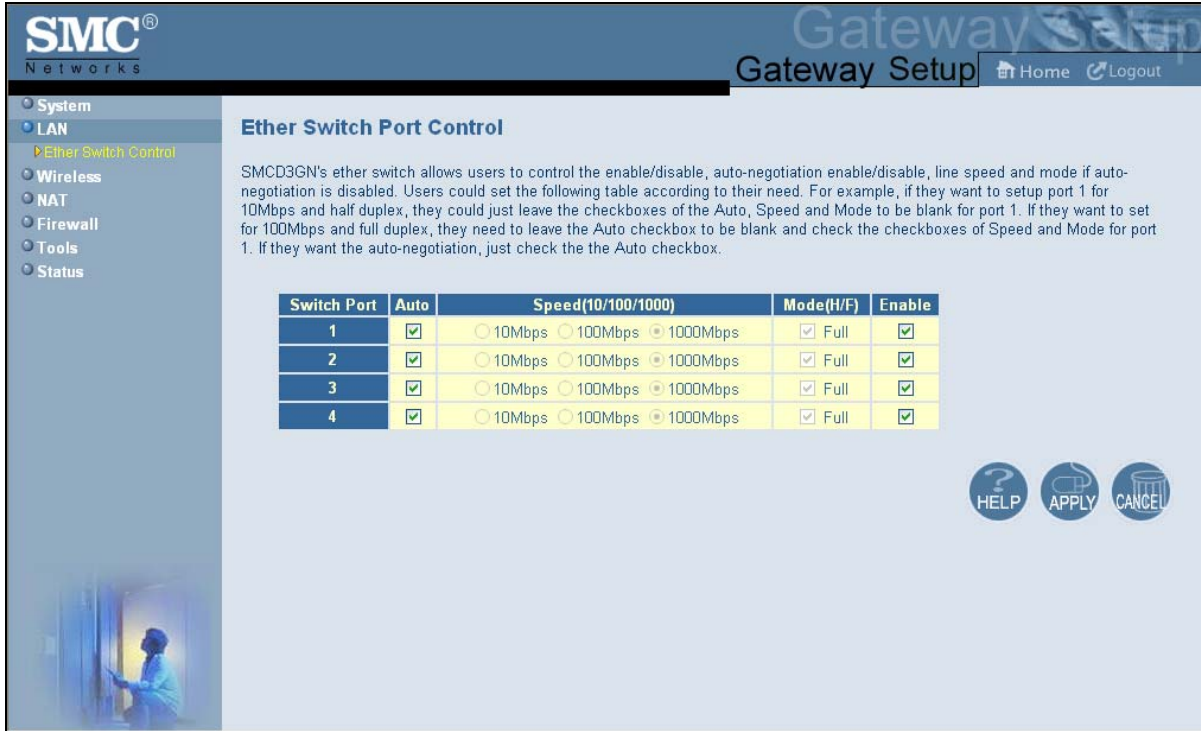
Figure 17. Ether Switch Port Control Menu

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. 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**.

Wireless Basic Settings Menu

The Wireless Basic Settings menu lets you enable or disable the Gateway's wireless setting. To access the Wireless Basic Settings click **Wireless** in the menu bar. Figure 18 shows an example of the menu.

By default, the setting is enabled. When wireless operation is enabled, you can use the submenus below the **Wireless** menu to configure the Gateway's encryption, MAC filtering, and advanced wireless settings.

To disable it, select **DISABLE** from the **Wireless ON/OFF** drop-down list. When wireless operation is disabled, the wireless submenus are not displayed in the menu bar.

Figure 18. Wireless Basic Settings Menu

Wireless Encryption Settings Menu

Using the Wireless Encryption Settings menu, you can protect the data transmitted across your wireless network.

To access the Wireless Encryption Settings menu, click **Wireless** in the menu bar and then click the **Encryption** submenu. Figure 19 shows an example of the menu and Table 7 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 35).

Figure 19. Wireless Encryption Settings Menu

Table 7. Wireless Encryption Settings Menu Options

Option	Description
SSID	Network name of the of the primary wireless carrier. This field usually is predefined and cannot be changed by users.
Security Mode	Selects the security mode used to protect transmissions across the wireless network. • 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 20 and Table 8. • 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 Figure 21 and Table 9. (default)

Figure 20. WEP Options

Table 8. 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 3	Fields for entering up to three WEP keys manually. Alternatively, you can have the Generate Keys button to generate these keys automatically.
Default WEP Key	Specifies which of the three WEP keys the Gateway is to use.
Authentication	Authentication used. Choices are: • Open System = clients can only associate to the wireless access point using Open Option. • 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.

Figure 21. WPA-Personal Options

Table 9. WPA-Personal Options

Option	Description
WPA Mode	Lets clients use WPA-PSK, WPA2-PSK, or both WPA modes. Default is Auto.
Cipher type	Algorithm encryption to be used. Choices are: • TKIP • AES • TKIP and AES (*default*)
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	The shared secret between your Gateway and access points and wireless clients. Please check with your cable operator to see whether your operator uses a default pre-shared key.
Pre-Authentication	Enables secure fast roaming, without noticeable signal latency. By default, this option is disabled.

MAC Filtering

Using the MAC Filtering menu, you can allow 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. Figure 22 shows an example of the menu and Table 10 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 35).
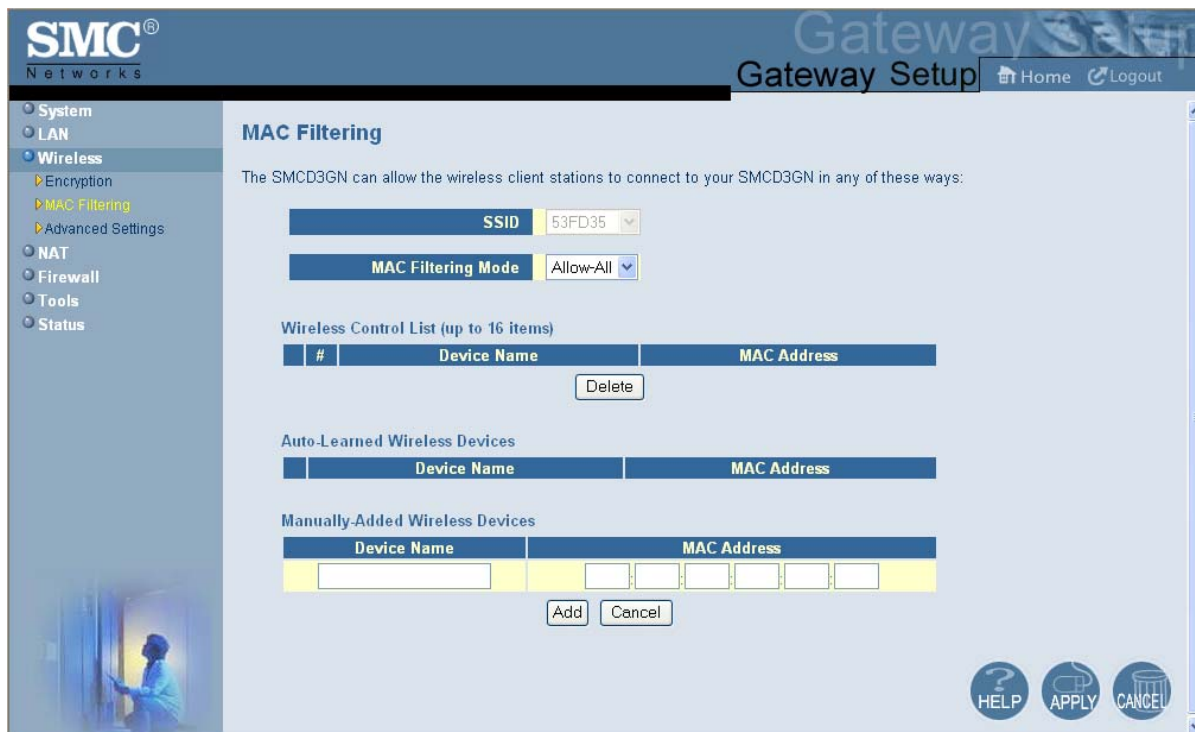
Figure 22. MAC Filtering Menu

Table 10. MAC Filtering Options

Option	Description
SSID	Network name of the of the primary wireless carrier. This field usually is predefined and cannot be changed by users.
MAC Filtering Mode	Determines which wireless client stations can connect to your Gateway. Te choices are: • Allow- All = all wireless client stations can connect to the Gateway. • 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 add 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 the name and Media Access Channel (MAC) address of the device of the wireless devices to be used in your MAC filter table. Click **Add** to add the device to the Wireless Control List.

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 23 shows an example of the menu and Table 11 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 35).
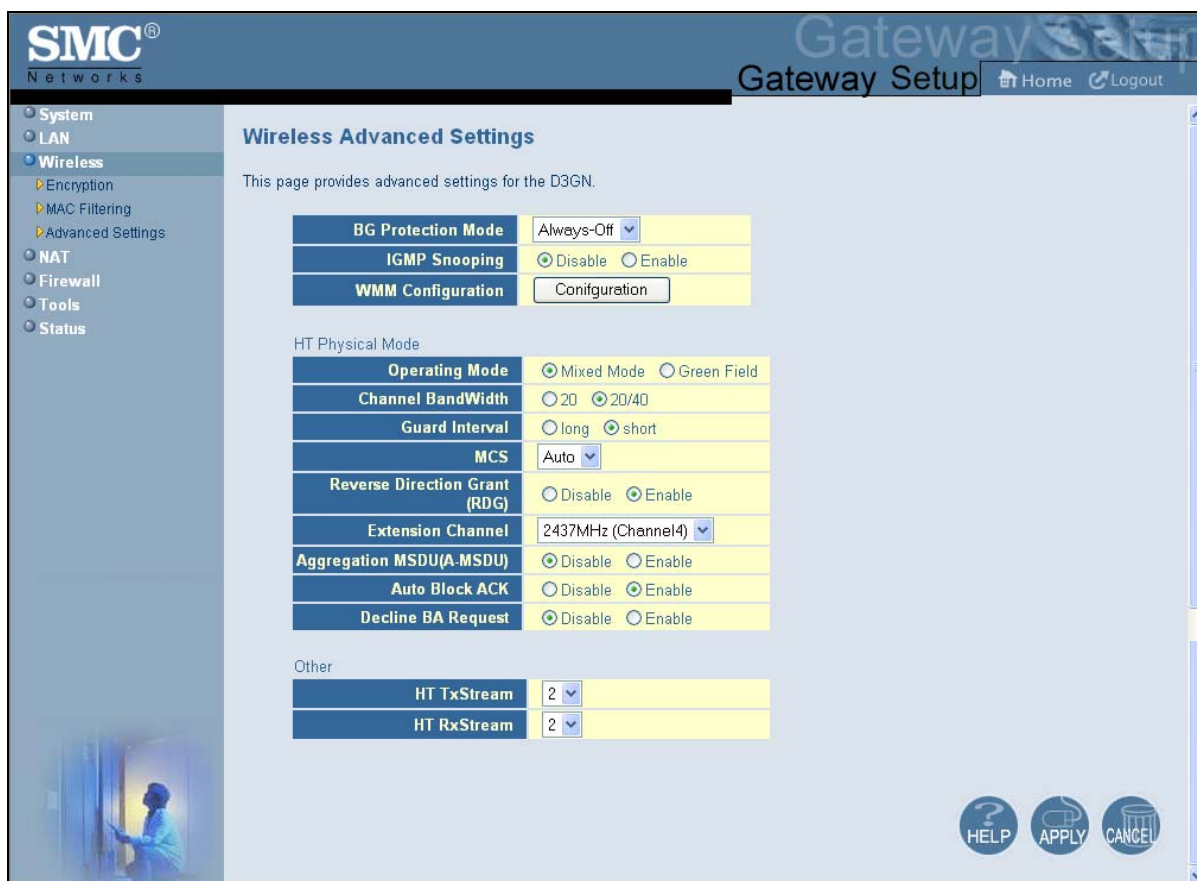
Figure 23. Wireless Advanced Settings Menu

Table 11. 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: 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. (*default*)
IGMP Snooping	Enables or disables the Gateway from forwarding multicast traffic intelligently. • 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. (*default*)
WMM Configuration	Displays a screen for selecting Wi-Fi Multimedia (WMM) settings for your wireless access point(s).
HT Physical Mode	
Operating Mode	Lets you select between Mixed Mode and Green Field. Mixed Mode = provides backward compatibility with IEEE 802.11n/a/g/b devices. (*default*) 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. • 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. (*default*)
Guard Interval	The guard interval is the period in nanoseconds that the Gateway listens between packets. Choices are: • Long = 800 ns guard interval. • Short = 400 ns guard interval (*default*)
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 your 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.
Reverse Direction Grant (RDG)	Speeds up data transmission between the Gateway and 802.11n access points and clients by allowing wireless workstations to send/receive data simultaneously, without contending for shared medium. Default is enable.
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.
Auto Block ACK	Enables or disables Auto Block ACL function. Default is disable.
Decline BA Request	Enables or disables the BA request function. Default is disable.
Other	
HT TxStream	Select 1 or 2 from the pull-down menu. Default is 2.
HT RxStream	Select 1 or 2 from the pull-down menu. Default is 2.

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 18 shows an example of the menu.
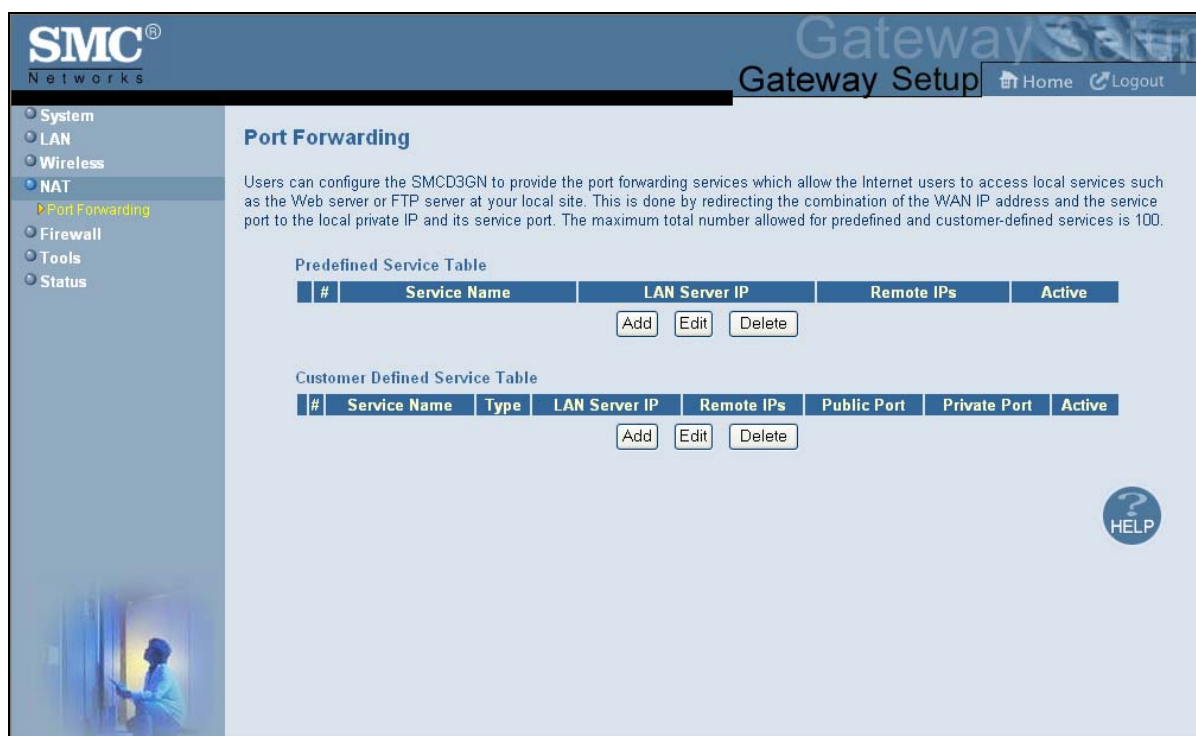
Figure 24. Port Forwarding Settings Menu

Adding a Port Forwarding Entry for a Predefined Service

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, click the **Add** button below the **Predefined Service Table**. The Predefined Service menu appears (see Figure 19).

2. Complete the fields in the Predefined Service menu (see Table 7). (Or click **Back** to return to the Port Forwarding Settings menu or **Cancel** to cancel any selections you made.)

3. Click **Apply**. The Port Forwarding menu reappears, with the predefined service you configured shown in the **Predefined Service Table**.

4. To configure additional services (up to 100, including customer-defined services), repeat steps 1 through 3. When you finish, click **Apply** in the LAN Settings menu to save your settings.

5. 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 7) and click **Apply**. Click **Apply** in the LAN Settings menu to save your settings.

6. 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. Click **Apply** in the LAN Settings menu to save your settings.
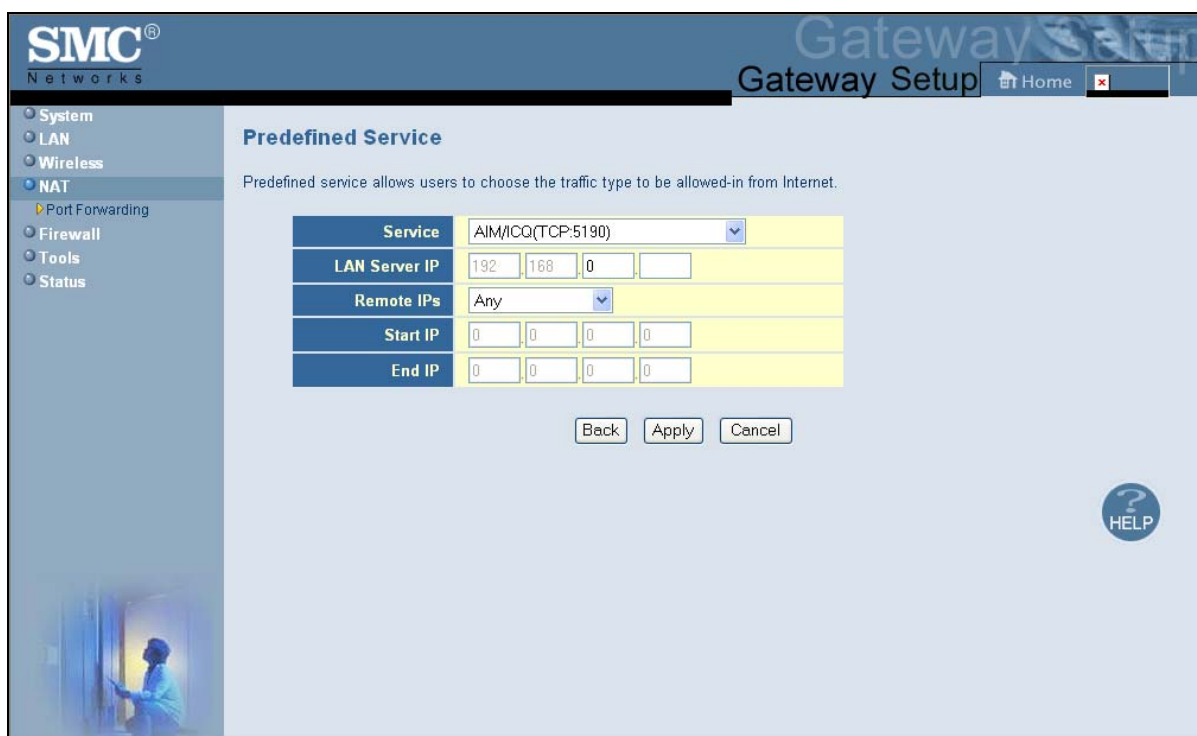
Figure 25. Predefined Service Menu

Table 12. 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.
Start IP	To forward to: • 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 a Port Forwarding Entry for a Customer-Defined Service

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 port-forwarding rules:

1. In the Port Forwarding menu, click the **Add** button below the **Customer Defined Service Table**. The Customer Defined Service menu appears (see Figure 26).

2. Complete the fields in the Customer Defined Service menu (see Table 10). (Or click **Back** to return to the Port Forwarding Settings menu or **Cancel** to cancel any selections you made.)

3. Click **Apply**. The Port Forwarding menu reappears, with the predefined service you configured shown in the **Customer Defined Service Table**.

4. To configure additional services (up to 100, including predefined services), repeat steps 1 through 3. When you finish, click **Apply** in the LAN Settings menu to save your settings.

5. 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 10) and click **Apply**. Click **Apply** in the LAN Settings menu to save your settings.

6. 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 customer-defined service, so be sure you no longer need the service before you delete it. Click **Apply** in the LAN Settings menu to save your settings.

Figure 26. Customer Defined Service Menu

Table 13. 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.
Start IP	To specify: • 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.
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).

Security Settings (Firewall) Menu

The Security Settings (Firewall) menu lets you enable or disable the Gateway's firewall. In addition, the submenus associated with this menu let you:

- Configure access control settings — see page 49

- Configure your Gateway for special applications — see page 49

- Set up URL blocking — see page 52

- Schedule routes — see page 54

- Receive email or syslog alert notifications — see page 55

- Configure a local client computer as a local DMZ for unrestricted two-way Internet access — see page 58

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 27 shows an example of the menu.

By default, your Gateway's firewall settings are enabled. To disable the firewall, uncheck **Enable Firewall Mode**.

Figure 27. Firewall Settings (Security) Menu

48
SMCD3GN Wireless Cable Modem Gateway User Manual

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.

By default, your Gateway does not block attempts to access the LAN from the Internet. To enable access control, check **Enable Access Control.**
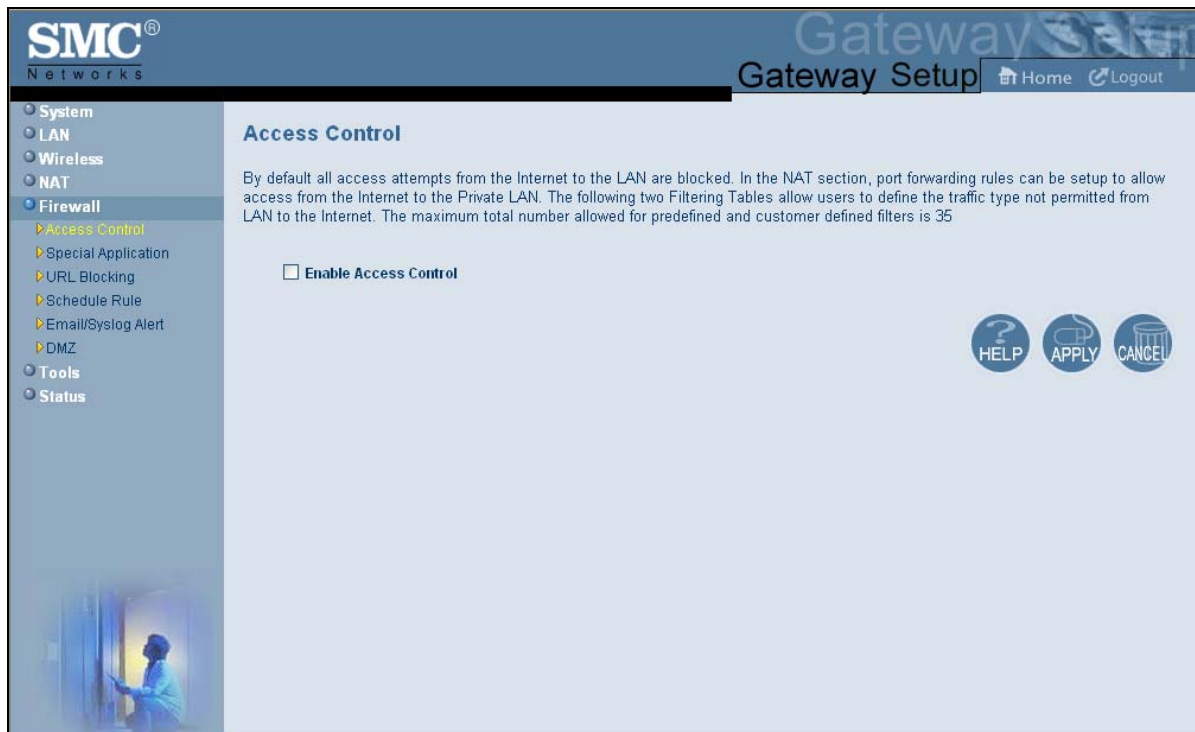
Figure 28. Access Control Menu

Configuring Special Applications

Using the Special Application menu, you can configure your 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, your 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.

The maximum allowed triggers is 50. To enable/disable the special application function, users can check/uncheck the Enable Triggering checkbox and press the APPLY icon to make it effective without reboot.

To display the Special Applications menu, click **Firewall** in the menu bar and then click the **Special Application** submenu. Figure 29 shows an example of the menu.
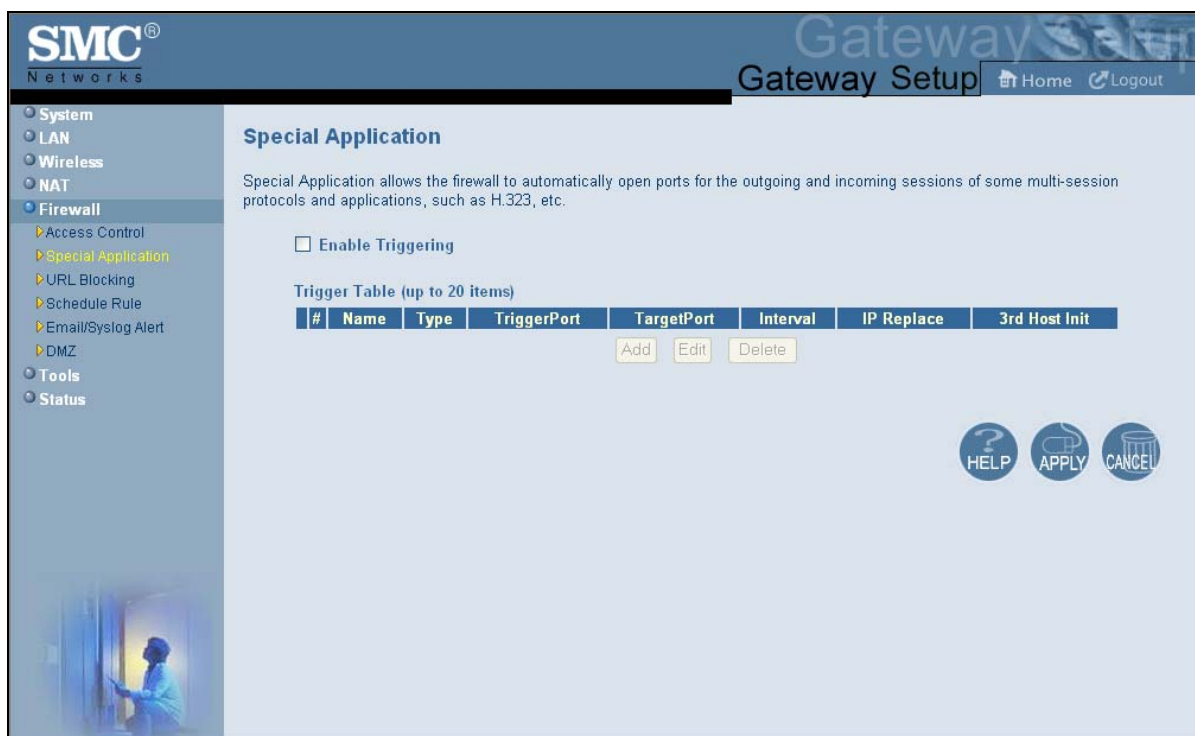
Figure 29. Special Applications Menu

To enable port triggering:

1. In the Special Application menu, check **Enable Triggering** and click the **Apply** button. The Trigger Table becomes available.

2. Click the **Add** button below the table. The Trigger menu appears (see Figure 30).

3. Complete the fields in fields Trigger menu (see Table 14). (Or click **Back** to return to the Trigger menu or **Cancel** to cancel any selections you made.)

4. Click **Apply**. The Special Application menu reappears, with the trigger you configured shown in 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 14) and click **Apply**. Click **Apply** in the Trigger 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 Trigger menu to save your settings.

Figure 30. Trigger Menu

Table 14. 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 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 3rd host	Decide whether the sessions can start from/to a third host. To prevent hacker attacks from a 3rd 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 the 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 3rd-host-initiated session is not allowed in this example, the whole communication fails.

Configuring URL Blocking

Using the URL Blocking menu, you can configure your Gateway to block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. Your 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 31 shows an example of the menu.

Note: 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 54.
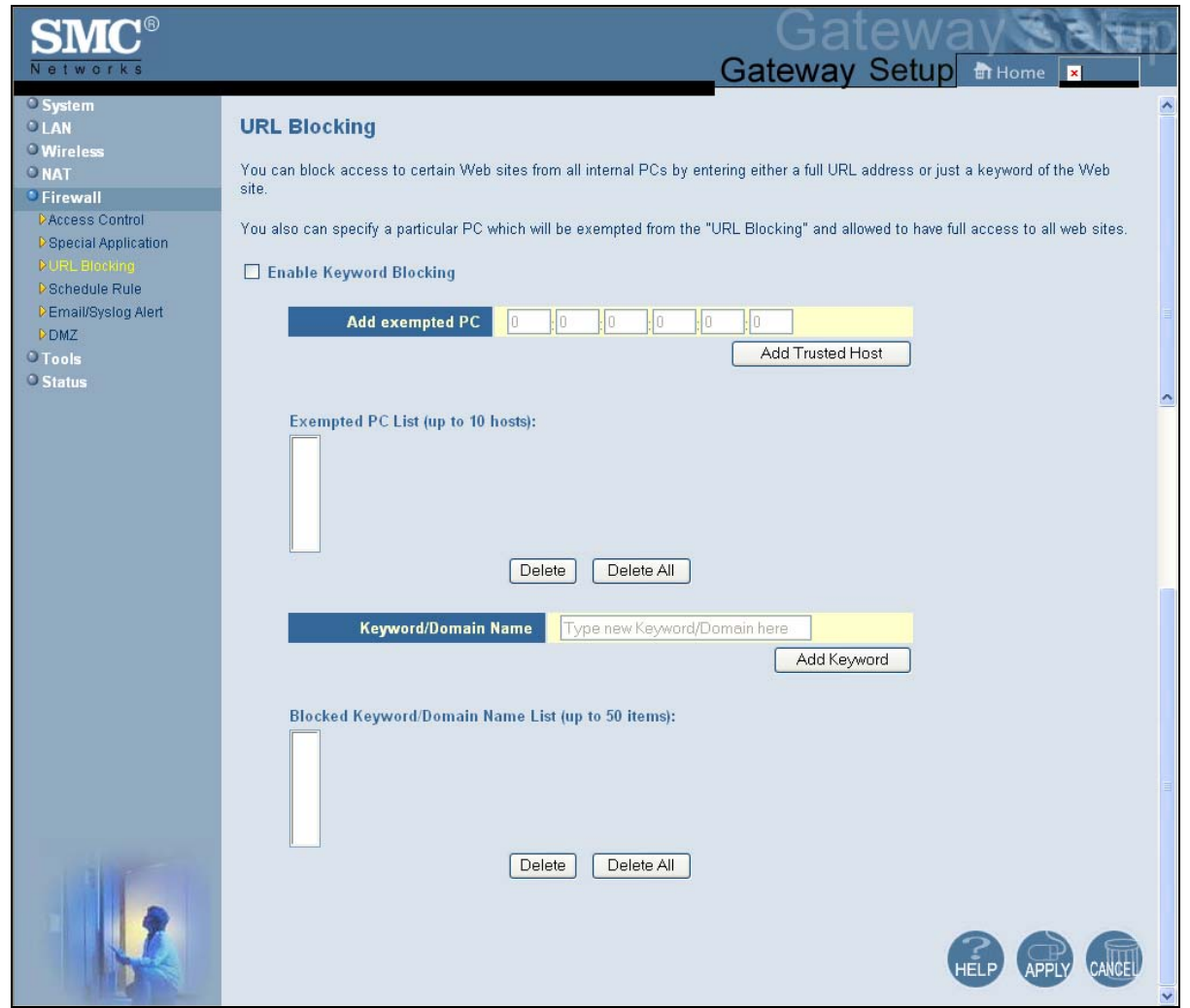
Figure 31. URL Blocking Menu

To enable URL blocking:

1. In the URL Blocking menu, check **Enable Keyword Blocking**.

2. To exempt a computer from URL blocking, enter the computer's Media Access Channel (MAC) address in the **Add exempted PC** field and click the **Add Trusted Host** button. The **Exempted PC List** shows the MAC address you entered. 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 in the field.

3. To block a site, enter in the **Type new Keyword/Domain here** field a keyword or domain name of the site you want to block and click **Add Keyword**. The **Blocked Keyword/Domain List** shows the keyword or domain you entered. Repeat this step for each additional keyword or domain (up to 50) 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 in the field.

4. Click **Apply**.

Configuring Schedule Rules

Schedule rules work with the Gateway's URL blocking feature (described on page 52) 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 32 shows an example of the menu.


Figure 32. Schedule Rule Menu

To configure a schedule rule:

1. In the Schedule Rule menu, check the days when you want to use URL blocking.

2. Specify the time when URL blocking is to start in the **Start Time** fields and the time when it is to end in the **End Time** field. Or to enable URL blocking all day, check **All Day**.

3. Click **Apply**.

Configuring Email and Syslog Alerts

Your 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. Figure 33 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 configure the to add syslog entries.

- The bottom area lets you define the alerting schedule.
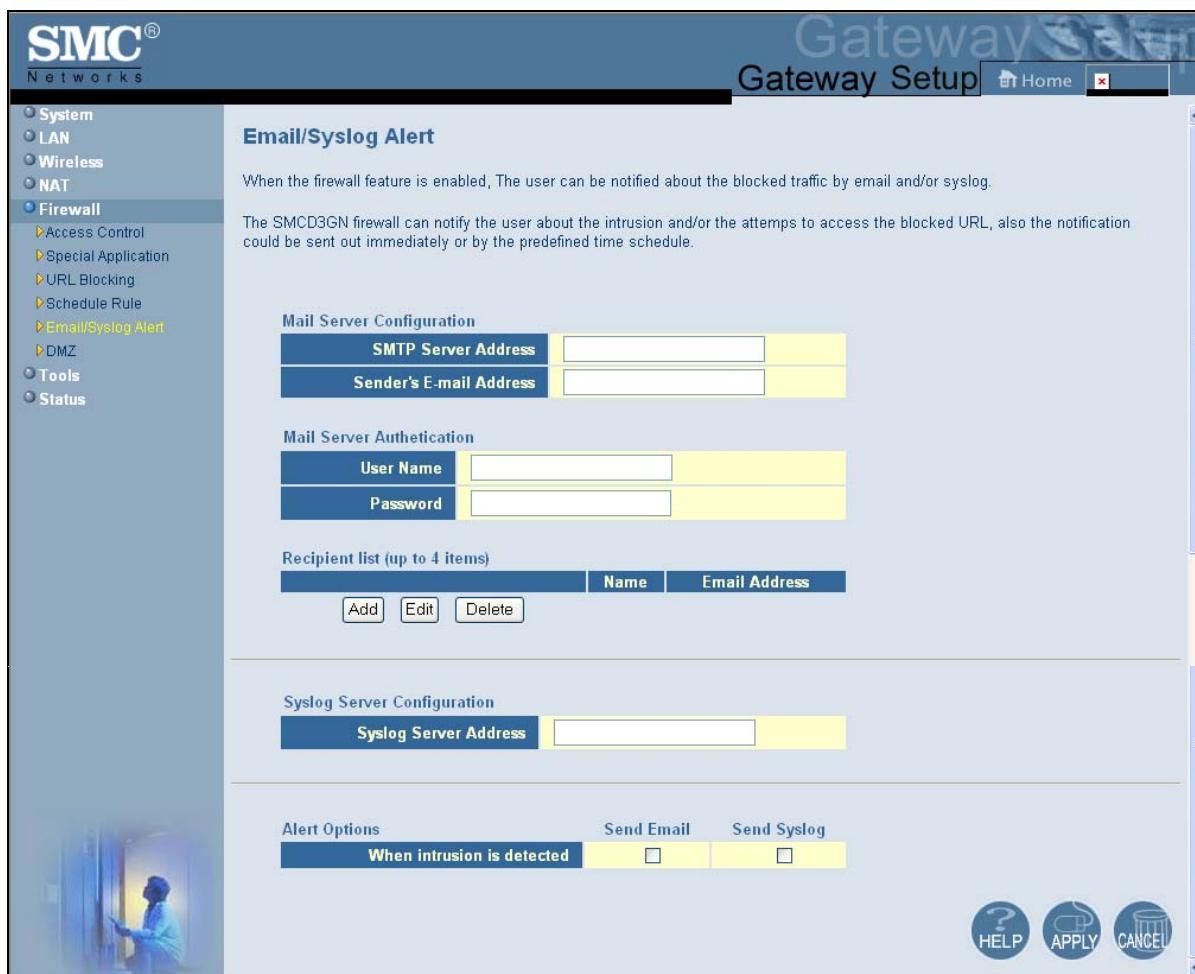
Figure 33. Email/Syslog Alert Menu

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 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 34), 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.) The email account you defined appears below this field. To send email to additional email accounts (up to 4), repeat this step.

4. To change information about an email recipient, click the radio button to the left of the recipient and click **Edit**. Then edit the person's name or email address 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 contact.

6. To generate an immediate email alert, check **Send Email** in the alert option **When intrusion is detected**.

7. Click **Apply**.

Figure 34. 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 menu, under **Syslog Server Configuration**, enter the syslog server address.

2. To generate an immediate syslog alert, check **Send Syslog** in the alert option **When intrusion is detected**.

3. Click the **Apply** button.

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 DMZ host. Adding a client to the Demilitarized Zone (DMZ) may expose your local network to various security risks because the client is not protected, so use this option as a last resort.

To access the DMZ (Demilitarized Zone) menu, click **Firewall** in the menu bar and then click the **DMZ** submenu in the menu bar. Figure 35 shows an example of the menu.
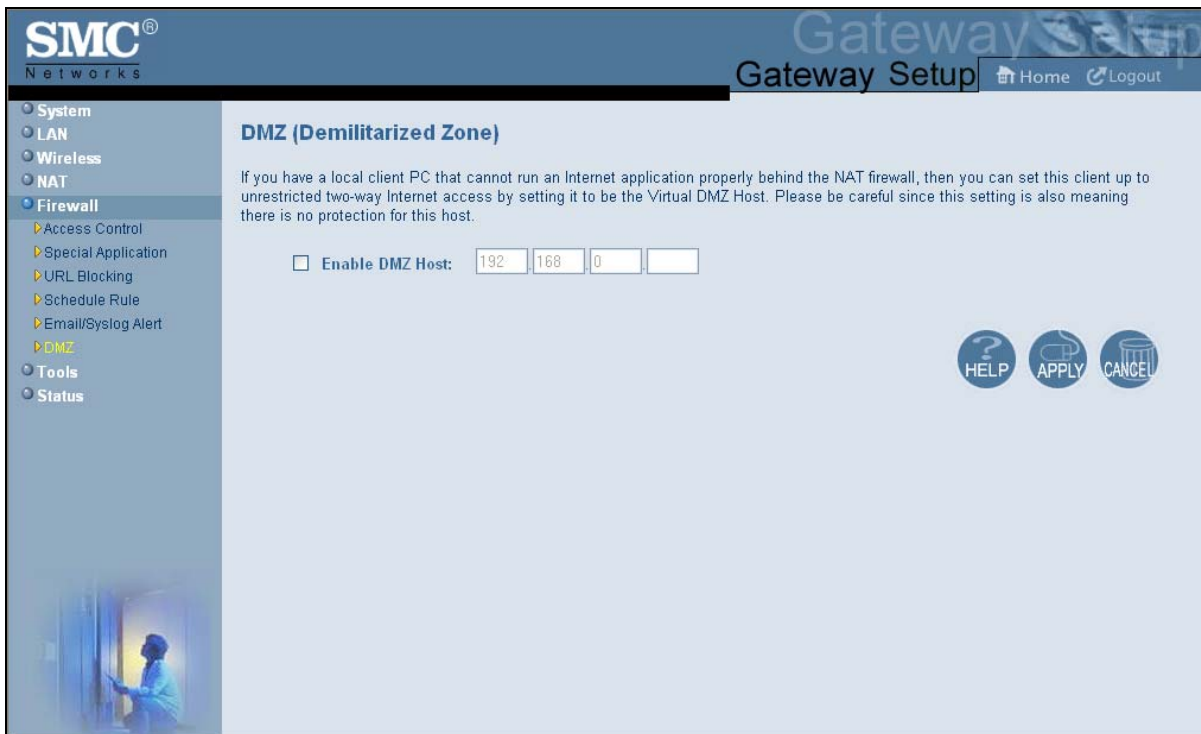
Figure 35. DMZ (Demilitarized Zone) Menu

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 public IP that is used as the DMZ host's public address.

3. Click **Apply**.

Using the Reboot Menu to Reboot the Gateway

One way to reboot the Gateway to the factory default settings is by using the Reset switch on the Gateway's rear panel. Another way is to use the Reboot menu.

Note: Rebooting the Gateway keeps any customized overrides you made to the default settings. To reboot the Gateway and return to the factory-default settings, use the Reset switch on the rear panel of the Gateway (see page 14).

To access the Reboot menu, click **Tools** in the menu bar and then click the **Reboot** submenu in the menu bar. Figure 36 shows an example of the menu.
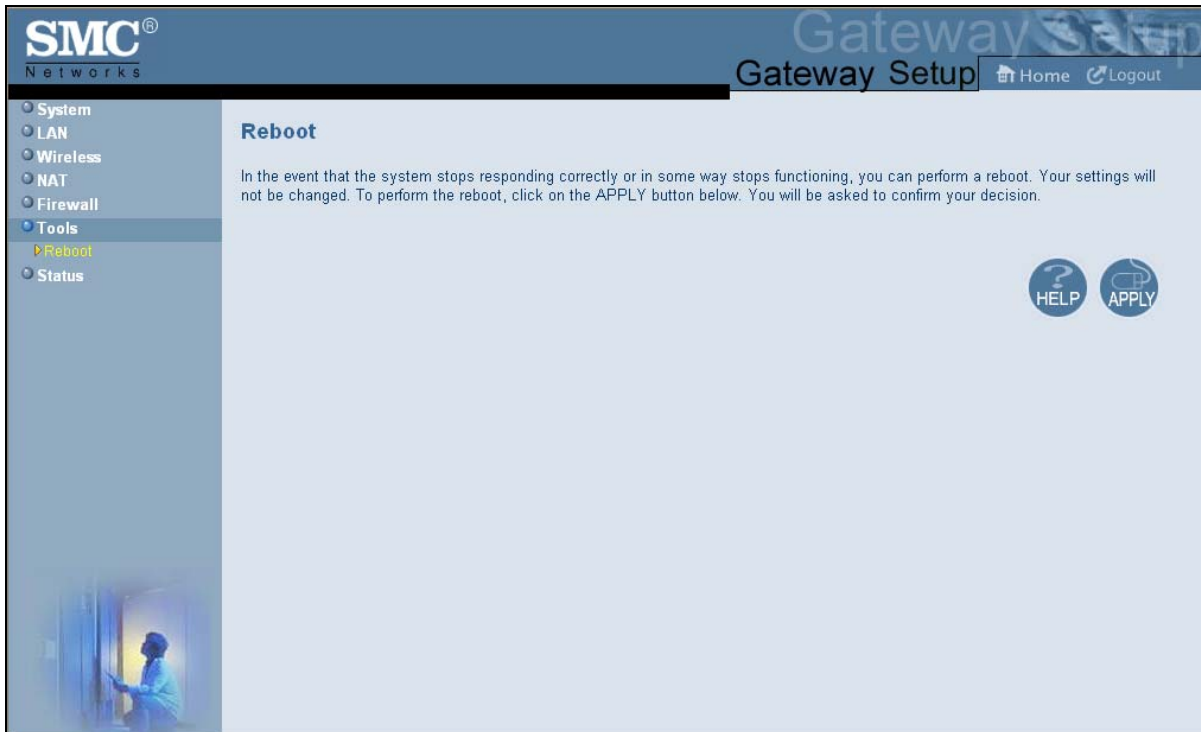
Figure 36. Reboot Menu

To reboot the Gateway:

1. In the Reboot menu, click **Apply**. The precautionary message in Figure 37 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.
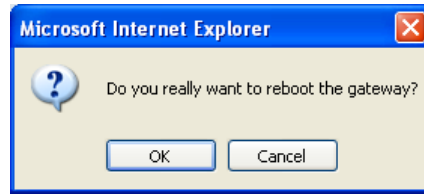
Figure 37. Precautionary Message

Viewing Status Information

The Status page is a read-only screen that shows the Gateway's wired and wireless status. The Status page also provides network, client, and cable modem event log information, with buttons for clearing and refreshing the logs, and releasing IP.

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. Figure 38 shows an example of the status information shown.

Figure 38. 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 39 shows an example of the cable status information shown.

Figure 39. Example of Cable Status Page

![SMC Networks logo]

Appendix A - Specifications

Compatibility

- Platform independent – works with PC,OSX, Linux, MAC, UNIX

- DOCSIS 1.0/1.1/2.0/3.0 compliant

- IEEE 802.3, 802.3u

- SPI firewall meet ICSA guidelines

Network Interface

- 10/100/1000 Base-T-Ethernet

- USB2.0 port*

- Wireless .11N MIMO

Ports

- Four ports 10/100/1000 MDI/MDIX auto sensing switch

- TR-68 coloring for 1 USB 2.0 Connector Type B (reserved for future use)

- TR-68 coloring for 4 Ethernet port

- Cable interface F type female 75 Ohm

Channel Bonding

- Downstream: up to 4 channels

- Upstream: up to 4 channels

Software Features

- GUI displays common troubleshooting information, modem status, and feature setup

- Full-featured CLI provides enhanced troubleshooting and setup

- DHCP server

- Ipv6 support coexist Ipv4

- Downloadable configuration files allow for easy setup and installation.

- Universal Plug and Play (UPnP) enabling any UPnP devices seamlessly

- Quality of Services (QoS) ensures high quality performance

SMCD3GN Wireless Cable Modem Gateway User Manual

- SAMBA for USB port connection of USB hard drives*

- GUI/SNMP/CLI addition to present PHY usage (multiple channels parameters)

- Port forwarding

- 64/256QAM auto detection

- Independent resets for downstream and upstream blocks

- Fragmentation and concatenation enabling Quality of Server (QoS) features

- Supports 64/128/256 bit RC4 authentication and encryption

Network Protocols

- IEEE 802.1d-compliant bridging
- DHCP Client/Server
- UDP
- DNS Relay
- ToD Client

- ARP
- ICMP
- FTP/TFTP
- Telnet

Security

- Password protected configuration access with multiple levels

- Stateful Packet Inspection (SPI) Firewall

- Network Address Translation (NAT)

- Application Level Gateways (ALG)

- Intrusion Detection

- Denial of Service (DoS) prevention

- Trojan Horse Prevention

- Smart Tracking

- VPN Passthrough (IPSec, PPTP, L2TP)

- Multiple User Profiles

- Dynamic Address-User Mapping

- Web-based authentication

- Comprehensive Logging

- Domain Validation

- Content and Filtering Features

- DMZ

Receiver

- Demodulation: 64/256QAM

- Input Frequency Range: 88MHz- 1002MHz

- Max speed: 38Mbps (64QAM) / 43Mbps (256QAM) per channel

    – DOCSIS 5120kbps/10Mbps (QPSK/16QAM)

    – DOCSIS 41.4 Mbps (64QAM)/55.2Mbps (256QAM)

    – Bounding (DOCSIS) per channel

- +222.48(+200) Mbps with 4 DS channel bounding (EuroDOCSIS)

Signal Level

- -15dBmV to +15dBmV(Automatic gain controlled by CM)

- 17 dBmV

Transmitter

- Modulation:

    – TDMA: QPSK, 8QAM, 16QAM, 32QAM, 64QAM, 128QAM

    – S-CDMA QPSK, 8QAM, 16QAM, 32QAM, 64QAM,128QAM

- Max Speed 320, 640, 1280, 2560, 5120 kbps

- (QPSK),640, 1280, 2560, 5120, 10240kbps (160QAM)

- +122.88(+108) Mbps with 4 US channel bounding (DOCSIS/EuroDOCSIS)

- Frequency Range: 5 to 42MHz (edge to edge) DOCSIS

LEDs

- Power

- DS (Downstream)

- US (Upstream)

- Online

- Link

- Diag

- WPS

- LAN (1-4)

- WiFi

- USB

Dimensions

- L x W x H: 26.8 x 15.5 x 3.5 mm (10.6 x 6.1 x 1.4 in)

- Weight: 0.50kg (1.10 lbs)

Input Power

- 12V/2A

Regulatory Certification

- FCC Part 15B Class B

- UL/cUL

Power Supply Energy Star Rating

- Level IV

SMCD3GN Wireless Cable Modem Gateway User Manual

Appendix B - 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 - This reminder is provided to call the CATV systems installer's attention to Section 820-93 of the National Electric Code which provide guideline for proper grounding and, in particular, specify that the Coaxial cable shield shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

Index

SMCD3GN Wireless Cable Modem Gateway User Manual

SMCD3GN Wireless Cable Modem Gateway User Manual

Technical Support

From USA and Canada (24 Hours a Day, 7 Days a Week)
Toll Free: 800-SMC-4YOU / 800-762-4968
Fax: 949-679-1481

Internet
Email Address: techsupport@smc.com
Driver Updates: http://www.smc.com/index.cfm?action=tech_support_drivers_downloads
www.smc.com

English: Technical Support information available at www.smc.com

English for Asia-Pacific: Technical Support information available at www.smc-asia.com

Deutsch: Technischer Support und weitere information unter www.smc.com

Espanol: En www.smc.com Ud. podra encontrar la informacion relativa a servicios de soporte technico

Francais: Informations Support Technique sur www.smc.com

Portugues: Informacoes sobre Suporte Tecnico em www.smc.com

Italiano: Le imformazioni di supporto tecnico sono disponibili su www.smc.com

Svenska: Information om Teknisk Support finns tilligangligt pa www.smc.com

Nederlands: Technische ondersteuningsinformatie beschikbaar op www.smc.com

Polski: Informacje o wsparciu technicznym sa dostepne na www.smc.com

Cestina: Technicka podpora je dostupna na www.smc.com

Magyar: Muszaki tamogat informacio elerheto -on www.smc.com

简体中文：技术支持讯息可通过www.smc-prc.com查询

繁體中文：產品技術支援與服務請上 www.smcnetworks.com.tw

ไทย: สามารถหาข้อมูลทางด้านเทคนิคได้ที่ www.smc-asia.com

한국어: 기술지원관련 정보는 www.smc-asia.com을 참고하시기 바랍니다