SMC Networks

DOCSIS 3.0 Wireless Cable Modem Gateway

SMCD3GN2 User Manual

FastFind Links

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

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

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:SMCD3GN2) 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.

SMCD3GN2 Wireless Cable Modem Gateway User Manual

May 26, 2011

Contents

Preface

Congratulations on your purchase of your SMCD3GN2 Wireless Cable Modem Gateway. Your SMCD3GN2 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 SMCD3GN2 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.
- **Appendix B -** lists the Gateway’s technical specifications.

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
ℹ	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 SMCD3GN2 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 10)
- System Requirements (page 10)
- Front Panel (page 11)
- Configuring Wireless Security (page 13)
- Rear Panel (page 13)
- Restoring Factory Defaults (page 14)

Unpacking Package Contents

Your SMCD3GN2 package should include the following items:

- One SMCD3GN2 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 your SMCD3GN2 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 your SMCD3GN2 Wireless Cable Modem Gateway. Table 1 describes the front panel LEDs.

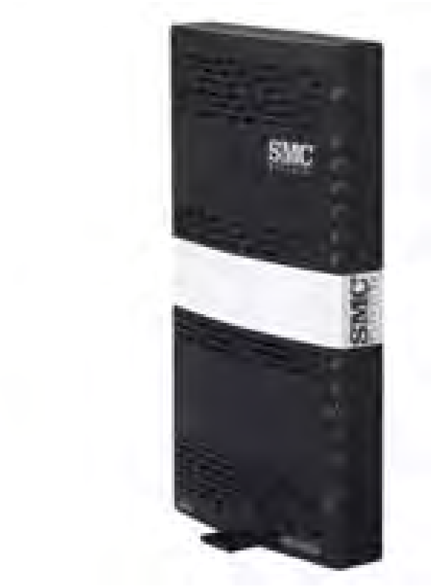


Figure 1. Front Panel of SMCD3GN2 Wireless Cable Modem Gateway

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 your SMCD3GN2 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.

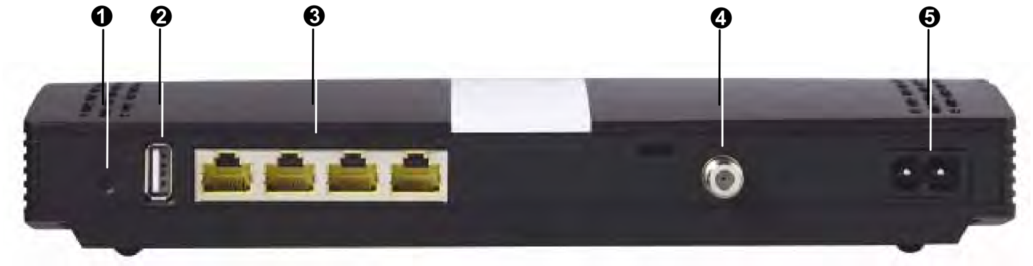


Figure 2. Rear View of your SMCD3GN2 Wireless Cable Modem Gateway

Table 2. SMCD3GN2 Wireless Cable Modem Gateway Rear Panel Components

	Item	Description
❶	Reset button	Use this button to reset the power or restore the default factory settings (see “Restoring Factory Defaults” on the next page). This button is recessed to prevent accidental resets of the Gateway.
❷	USB	USB 2.0 high-speed port for storing configurations externally.
❸	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.
❹	Cable	Connect your coaxial cable line to this port.
❺	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 99) or return the Gateway to its factory default settings (see “Using the Tools Settings Menu” on page 98).

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 Your Gateway

This chapter describes how to install your SMCD3GN2 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

The SMCD3GN2 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 SMCD3GN2 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).

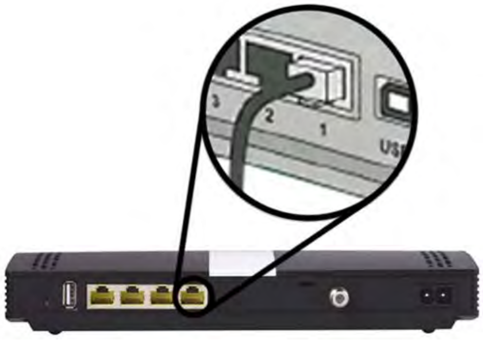


Figure 3. Connecting to an ETH Port on the Gateway Rear Panel

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

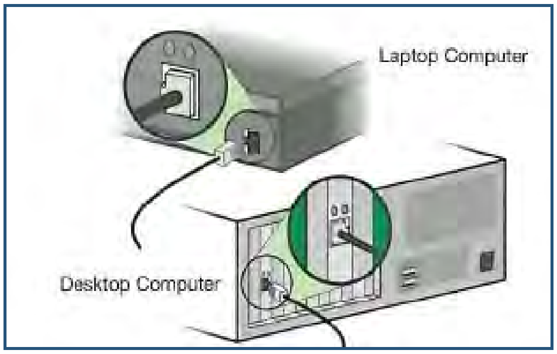


Figure 4. Connecting the Gateway to the a Laptop or Desktop Computer

Connecting the WAN

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

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.

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 13).
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 12).

⚠ **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 your SMCD3GN2 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.

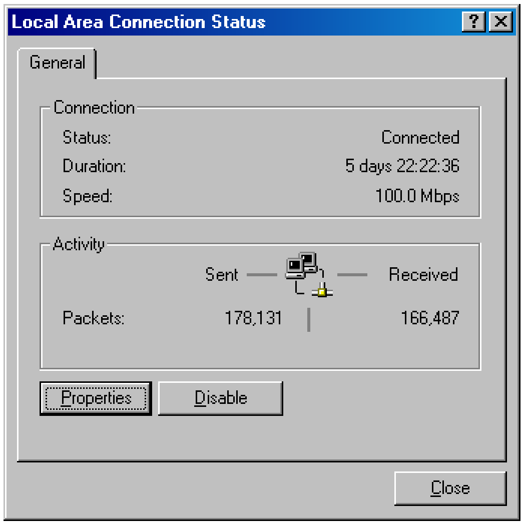
The topics covered in this chapter are:

- Configuring Microsoft Windows 2000 (page 19)
- Configuring Microsoft Windows XP (page 20)
- Configuring Microsoft Windows Vista (page 21)
- Configuring Microsoft Windows 7 (page 23)
- Configuring an Apple® Macintosh® Computer (page 25)

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).



Status: Connected
Duration: 5 days 22:22:36
Speed: 100.0 Mbps
Packets: 178,131 | 166,487

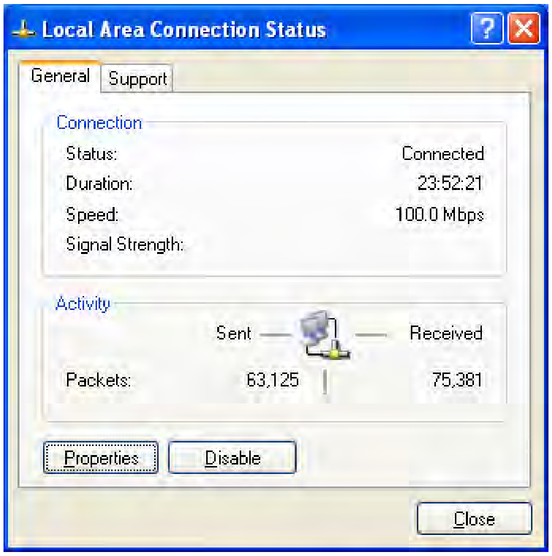
Figure 5. Local Area Connection Status Window

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 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.



Connection

Status:	Connected
Duration:	23:52:21
Speed:	100.0 Mbps
Signal Strength:	

Activity

	Sent	Received
Packets:	63,125	75,381

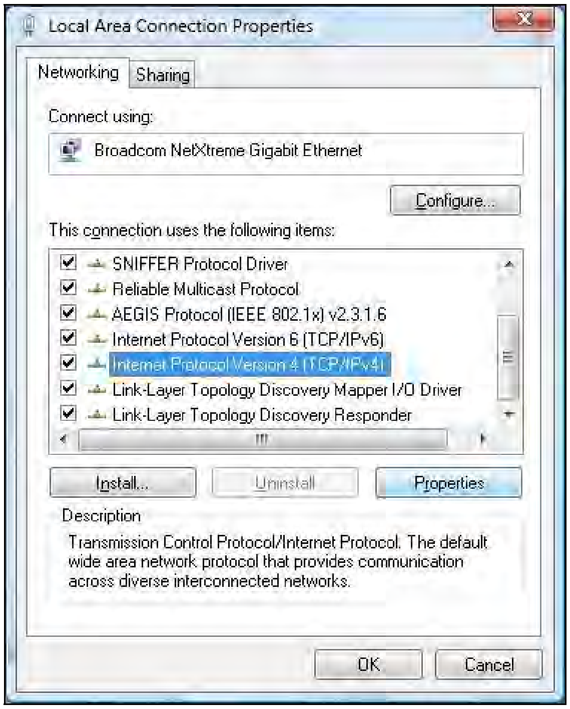
Figure 6. Local Area Connection Status Window

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 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.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

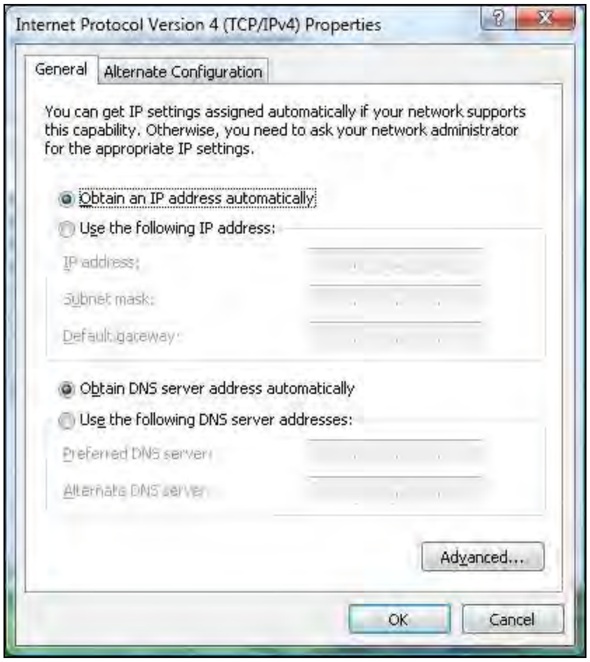
☑ SNIFFER Protocol Driver
☑ Reliable Multicast Protocol
☑ AEGIS Protocol (IEEE 802.1x) v2.3.1.6
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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).



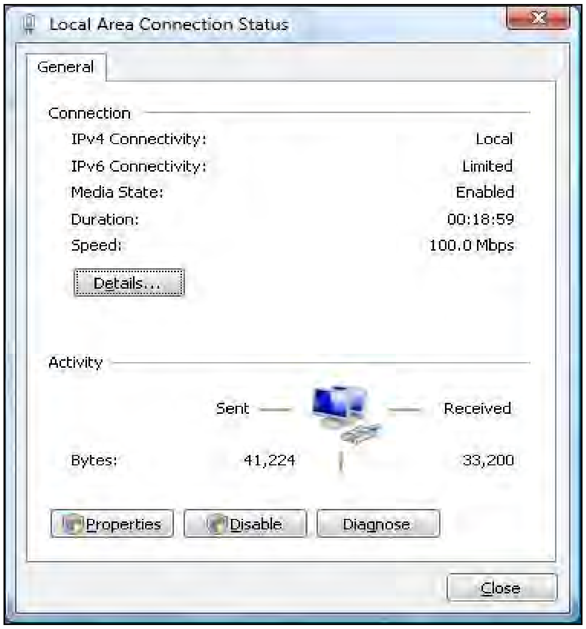
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

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.



Connection

IPv4 Connectivity:	Local
IPv6 Connectivity:	Limited
Media State:	Enabled
Duration:	00:18:59
Speed:	100.0 Mbps

Activity

	Sent	Received
Bytes:	41,224	33,200

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**

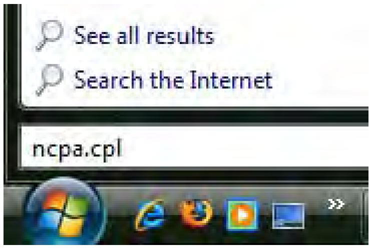


Figure 10. Typing ncpa.cpl in the Start Menu Box

The Network Connections List appears.

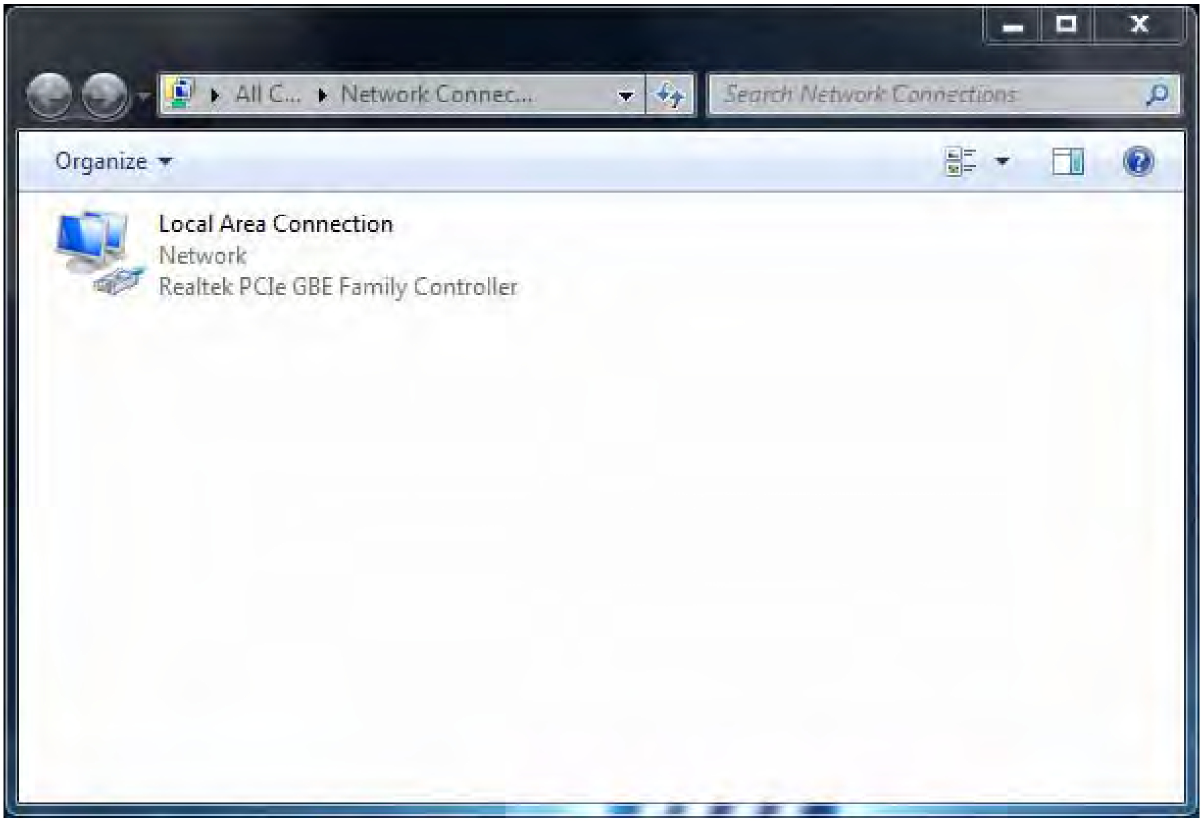
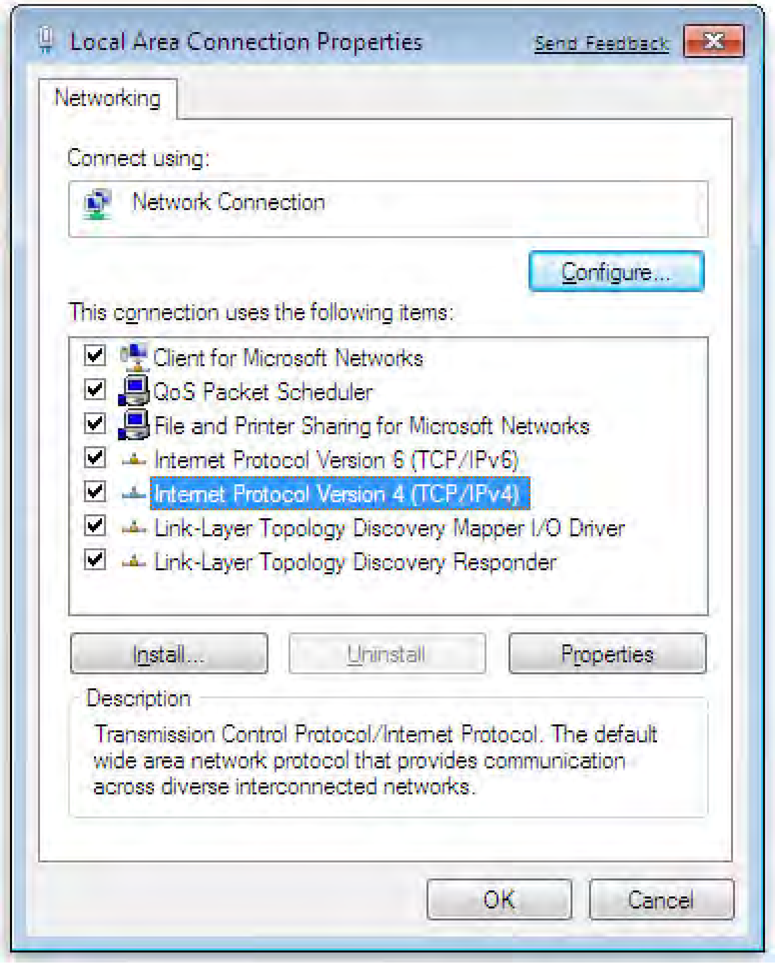


Figure 11. Example of Network Connections List

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**.



Connect using:

Network Connection

This connection uses the following items:

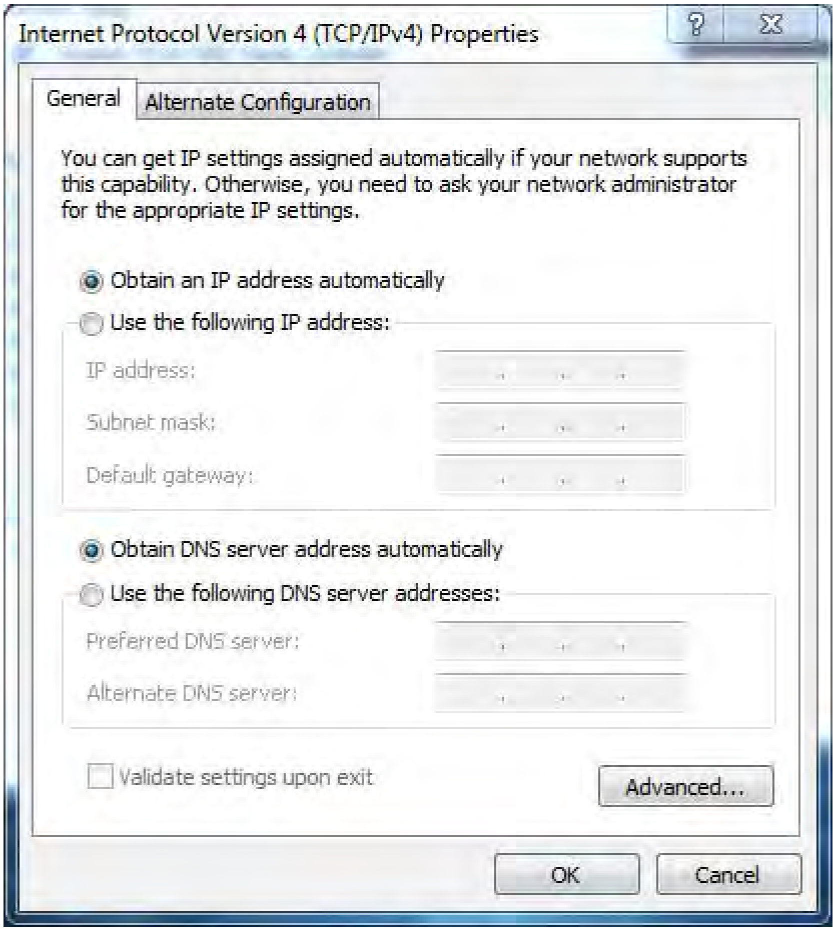
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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).



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

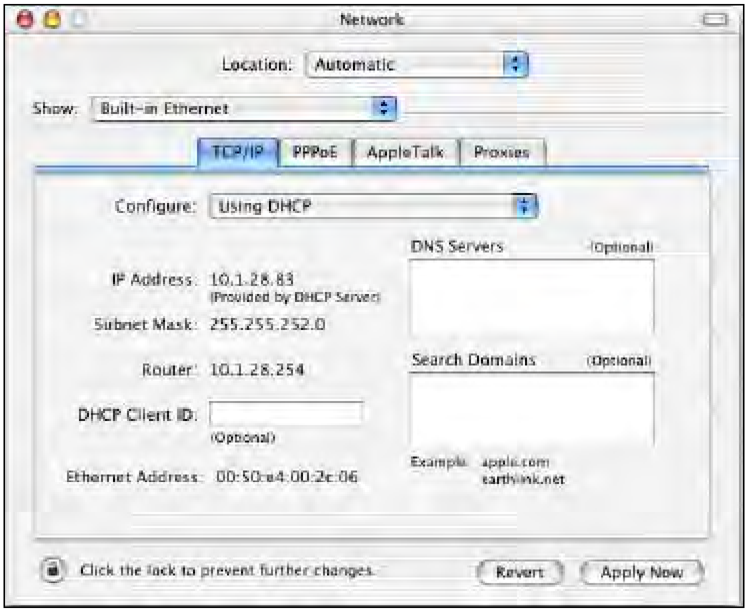
Figure 13. Properties Window

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.

1. Pull down the Apple Menu, click **System Preferences**, and select **Network**.
2. Verify that the NIC connected to your SMCD3GN2 is selected in the **Show** field.
3. In the **Configure** field on the **TCP/IP** tab, select **Using DHCP** (see Figure 14).
4. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.



Network

Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 10.1.28.83
(Provided by DHCP Server)

Subnet Mask: 255.255.252.0

Router: 10.1.28.254

DHCP Client ID:
(Optional)

Ethernet Address: 00:50:e4:00:2c:06

DNS Servers (Optional)

Search Domains (Optional)

Example: apple.com
earthlink.net

Click the lock to prevent further changes.

Figure 14. Selecting Using DHCP in the Configure Field

4 Configuring Your 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 28)
- Accessing the Gateway’s Web Management (page 30)
- Understanding the Web Management Interface Screens (page 31)
- Web Management Interface Menus (page 32)

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

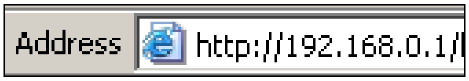
After configuring your computer for TCP/IP and performing the pre-configuration guidelines on the previous page, you can now easily configure the Gateway from the convenient Web-based management interface. From your Web browser (Microsoft Internet Explorer version 5.5 or later), you will log in to the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

To access your SMCD3GN2 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:



Address http://192.168.0.1/

The Login User Password screen appears (see Figure 15)

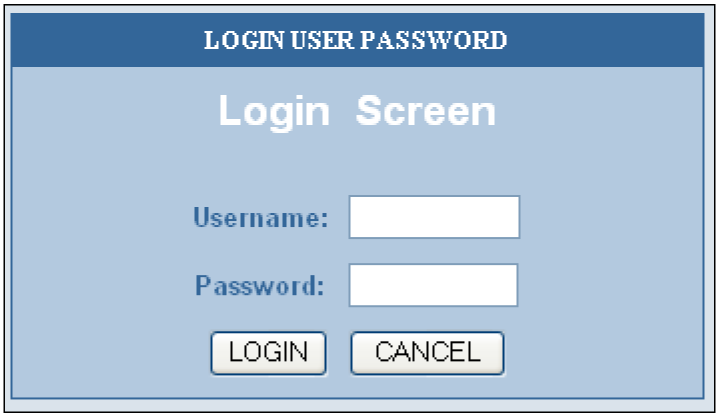


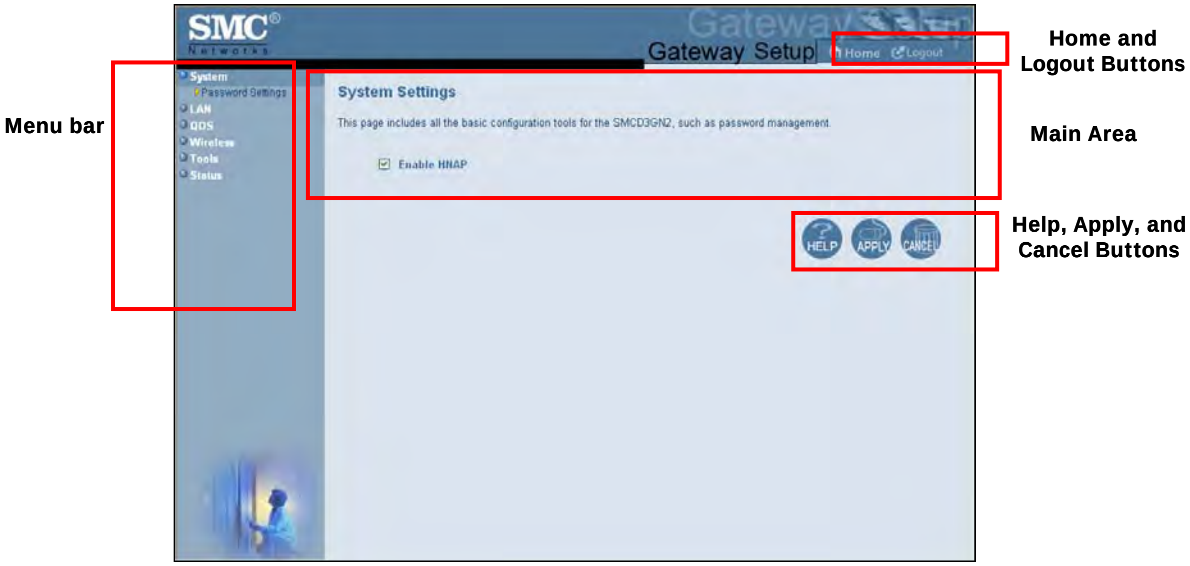
Figure 15. Login User Password Screen

3. In the Login User Password screen, type the default login username **cusdamin** and the default password **password.** Your service provider may customize the login, so please check with your services provided for correct login information. 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.



System Settings

This page includes all the basic configuration tools for the SMCD3GN2, such as password management.

☑ Enable HNAP

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 submenu **Password Settings** appears below the **System** menu (see Figure 17).

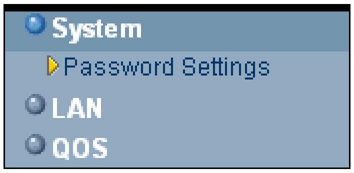


Figure 17. Example of System Submenu

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 and Submenus

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

Table 3. Web Management Interface Menus and Submenus

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

Menu and Submenus	Description	See Page
System	Lets you enable or disable uPnP and HNAP. The submenu lets you:	34
System > Password Settings	• Define the password for logging in to the Gateway's Web interface.	35
LAN	Lets you configure settings for your private LAN.	36
LAN > Ether Switch Control	• Specify fixed speed and duplex settings, and disable individual LAN ports.	39
LAN > Ether Access Control	• 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.	41
QoS	Lets you enable Quality of Service (QoS) settings. If you enable QoS, the following submenus become available for:	44
QoS > Port	• Prioritizing performance of the four Gateway LAN ports.	45
QoS > COS	• Defining four queues to which the Class of Service (CoS) is mapped.	46
QoS > DSCP	• Defining the QoS class queue to which the customized DSCP is mapped.	48
QoS > Queue	• Specifying whether QoS behavior runs with strict or weighted priority.	50
QoS > DSCP Remarking	• Defining the DSCP remarking action and mode.	52
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:	54
Wireless > Encryption	• Use encryption to protect the data transmitted across your wireless network	56
Wireless > WPS	• Enable or disable Wi-Fi Protected Setup (WPS).	60
Wireless > MAC Filtering	• Allow all wireless client stations or only trusted PCs to connect over a wireless connection.	63
Wireless > Advanced Settings	• Configure advanced wireless settings for the Gateway.	65

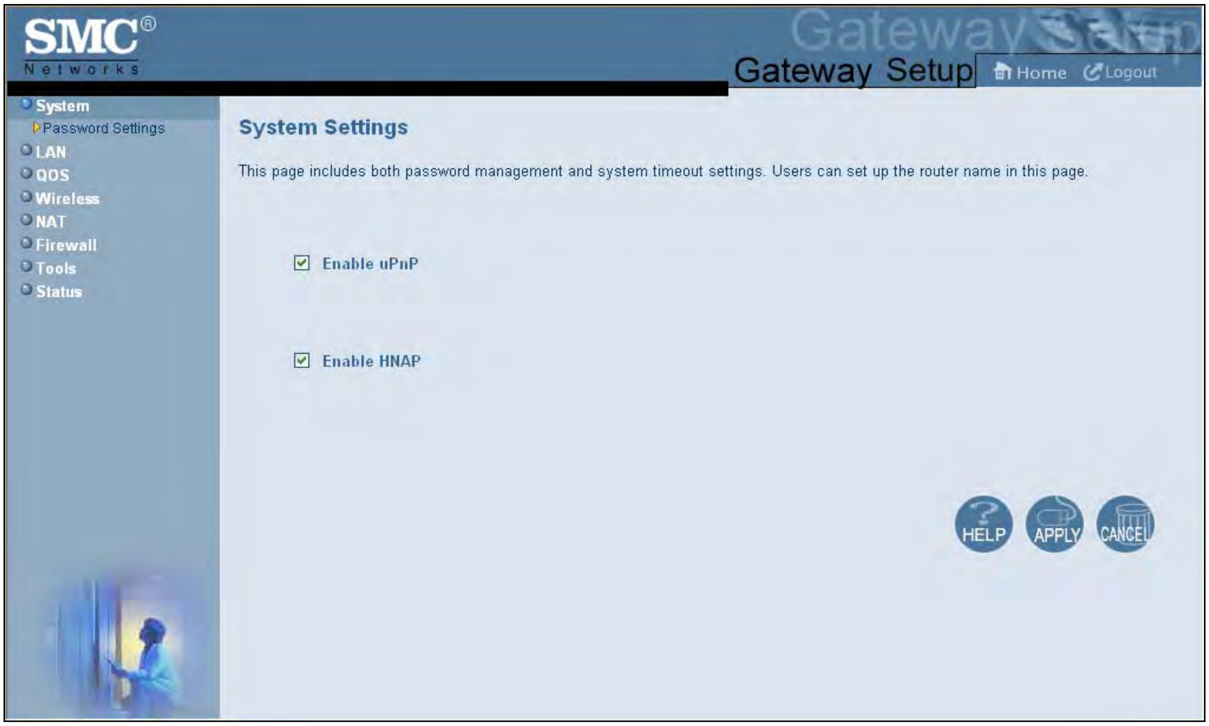
Table 3. Web Management Interface Menus and Submenus

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

Menu and Submenus	Description	See Page
NAT > Port Forwarding	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.	67
Firewall	Lets you enable or disable the Gateway's firewall. Submenus let you:	73
Firewall > Access Control	• Block traffic at the Gateway's LAN interfaces from accessing the Internet.	74
Firewall > Special Application	• Detect port triggers for detect multiple-session applications and allow them to pass the firewall.	87
Firewall > URL Blocking	• Block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site.	90
Firewall > Schedule Rule	• Define schedule rules that work with the Gateway's URL blocking feature.	92
Firewall > Email/Syslog Alert	• 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.	93
Firewall > DMZ	• Configure a local client computer for unrestricted two-way Internet access by defining it as a Virtual DMZ host.	97
Tools	Lets you reset the Gateway and return it to its factory default settings. The submenu lets you:	98
Tools > Reboot	• Reboot the Gateway while keeping all overrides you made to the device's factory default settings.	99
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:	100
Status > Cable Status	• View cable initialization procedures, and cable downstream and upstream status.	101

System Settings Menu

The System Settings menu lets you enable or disable Universal Plug and Play (uPnP) and Home Network Administration Protocol (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.



System Settings

This page includes both password management and system timeout settings. Users can set up the router name in this page.

☑ Enable uPnP

☑ Enable HNAP

Figure 18. System Settings Menu

Table 4. System Settings Menu Option

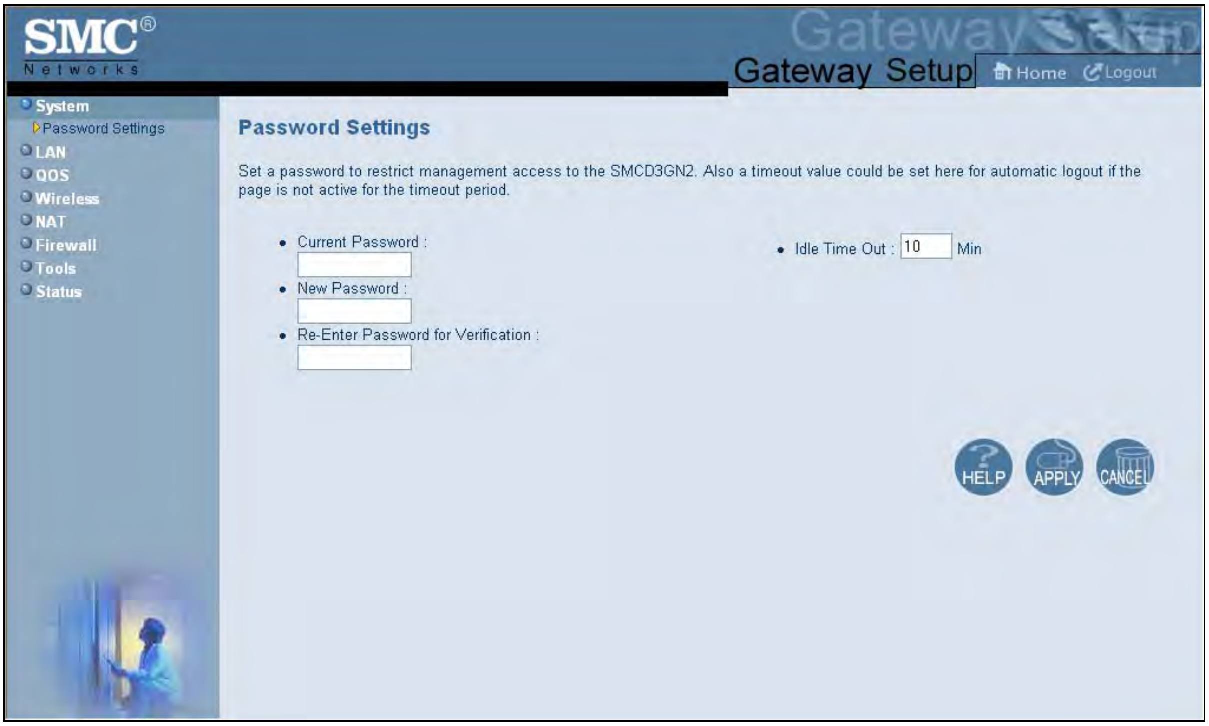
Option	Description
Enable UPnP	Configures your Gateway as a uPnP Internet gateway. UPnP allows for dynamic connectivity between devices on a network. A UPnP-enabled device like your Gateway can obtain an IP address, advertise its capabilities, learn about other connected UPnP devices and then communicate 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 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. . (*default)* • Uncheck = HNAP is disabled on the Gateway

Password Settings Menu

The Password Settings menu lets you change the default username and password used to log in to the Gateway's Web interface.

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 19 shows an example of the menu and Table 5 describes the settings you can select.



Password Settings

Set a password to restrict management access to the SMCD3GN2. Also a timeout value could be set here for automatic logout if the page is not active for the timeout period.

- Current Password :
- New Password :
- Re-Enter Password for Verification :
- Idle Time Out : 10 Min

Figure 19. Password Settings Menu

Table 5. Password Settings Menu Options

Option	Description
Current Password	Enter the current case-sensitive login password. For security purposes, every typed character appears as a dot (•). The default password is not shown for security purposes.
New Password	Enter the new case-sensitive login 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 login 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.

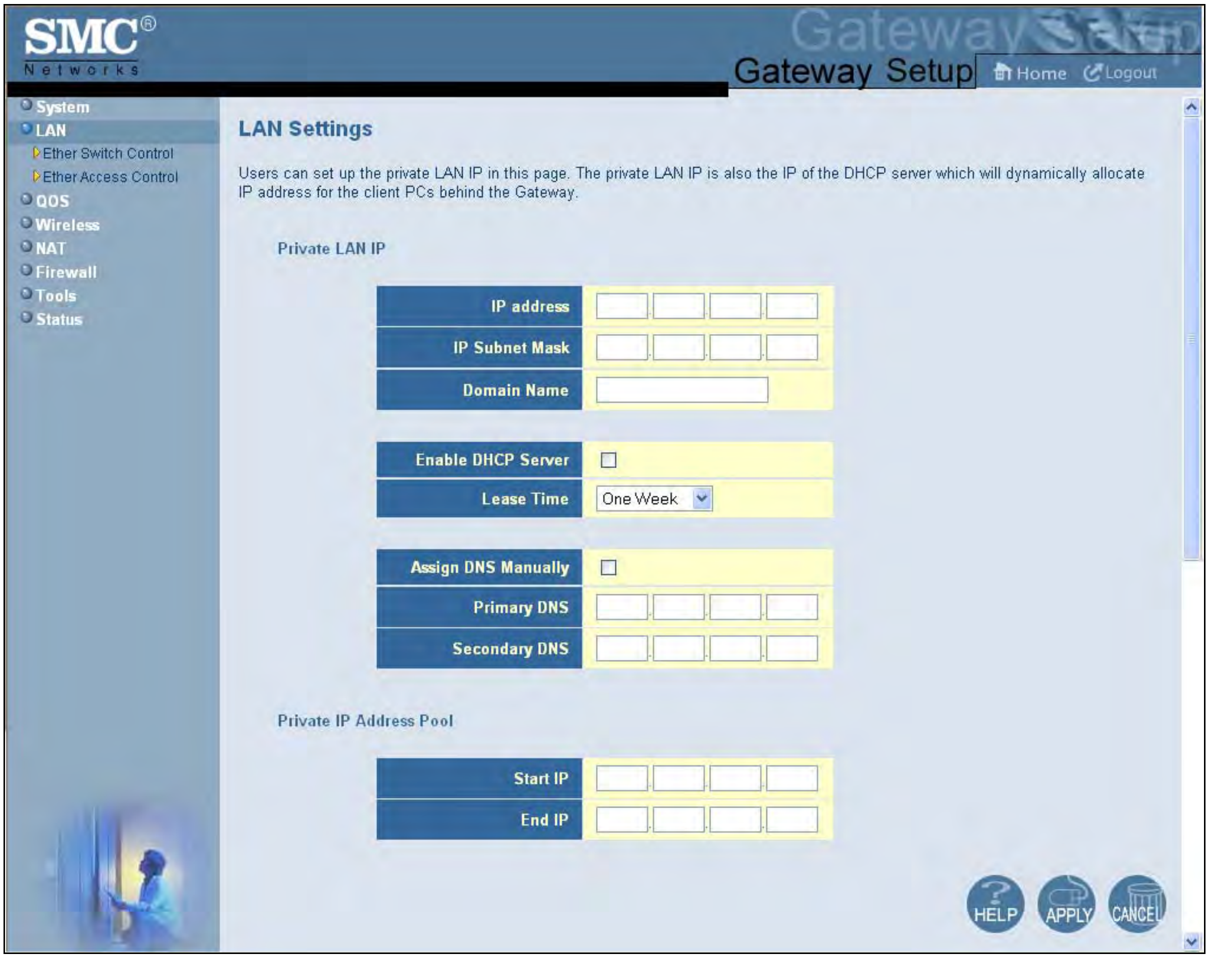
LAN Settings Menu

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

Using the LAN Settings menu, you can define private LAN IP addresses. To access the LAN Settings menu, click **LAN** in the menu bar. Figure 20 shows an example of the menu and Table 6 describes the settings you can select.



LAN Settings

Users can set up 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.

Private LAN IP

IP address	. . .
IP Subnet Mask	. . .
Domain Name	
Enable DHCP Server	□
Lease Time	One Week
Assign DNS Manually	□
Primary DNS	. . .
Secondary DNS	. . .

Private IP Address Pool

Start IP	. . .
End IP	. . .

Figure 20. LAN Settings Menu

Table 6. LAN Settings Menu Options

Option	Description
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.

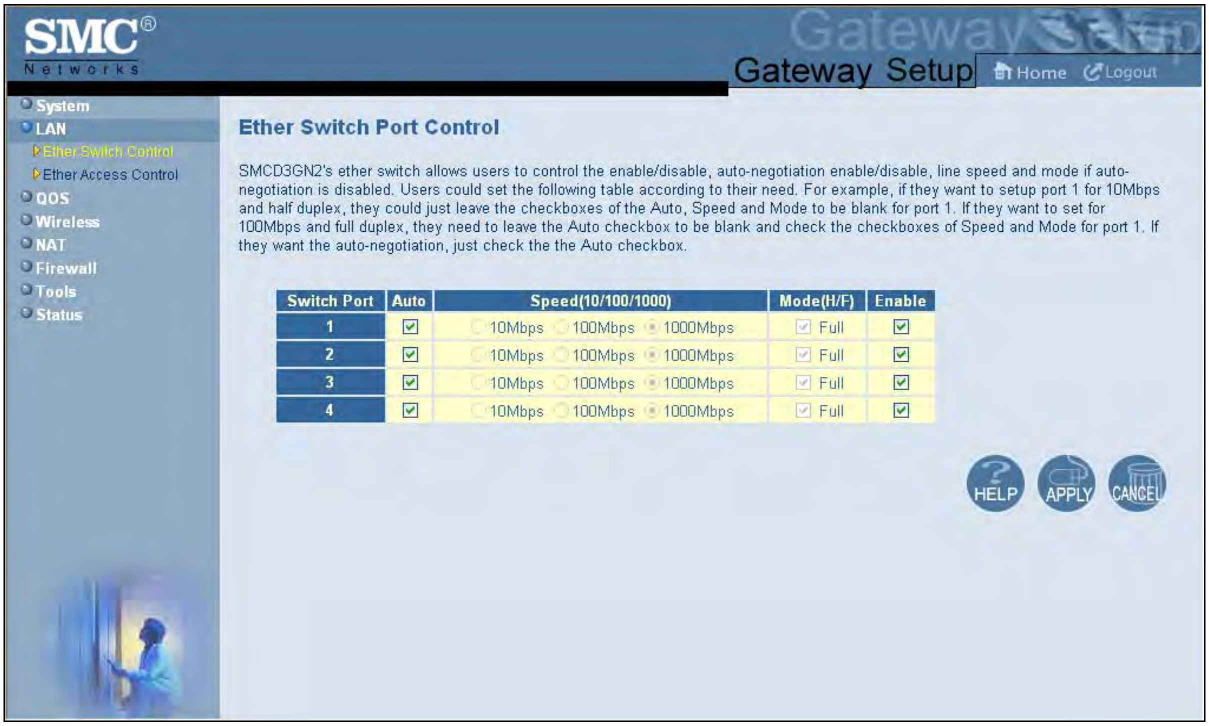
Enable DHCP Server	Enables or disables the DHCP server to allow automatic allocation of IP addresses to LAN client PCs.
	Checked = DHCP server is enabled. (default)
	Unchecked = DHCP server is disabled.

Option	Description
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. • 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. (*default*)
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.
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. • 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. 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. • 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. (*default*)
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.

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 21 shows an example of the menu.



Ether Switch Port Control

SMCD3GN2'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	☑	○ 10Mbps ○ 100Mbps ● 1000Mbps	☑ Full	☑
2	☑	○ 10Mbps ○ 100Mbps ● 1000Mbps	☑ Full	☑
3	☑	○ 10Mbps ○ 100Mbps ● 1000Mbps	☑ Full	☑
4	☑	○ 10Mbps ○ 100Mbps ● 1000Mbps	☑ Full	☑

Figure 21. Ether Switch Port Control Menu

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

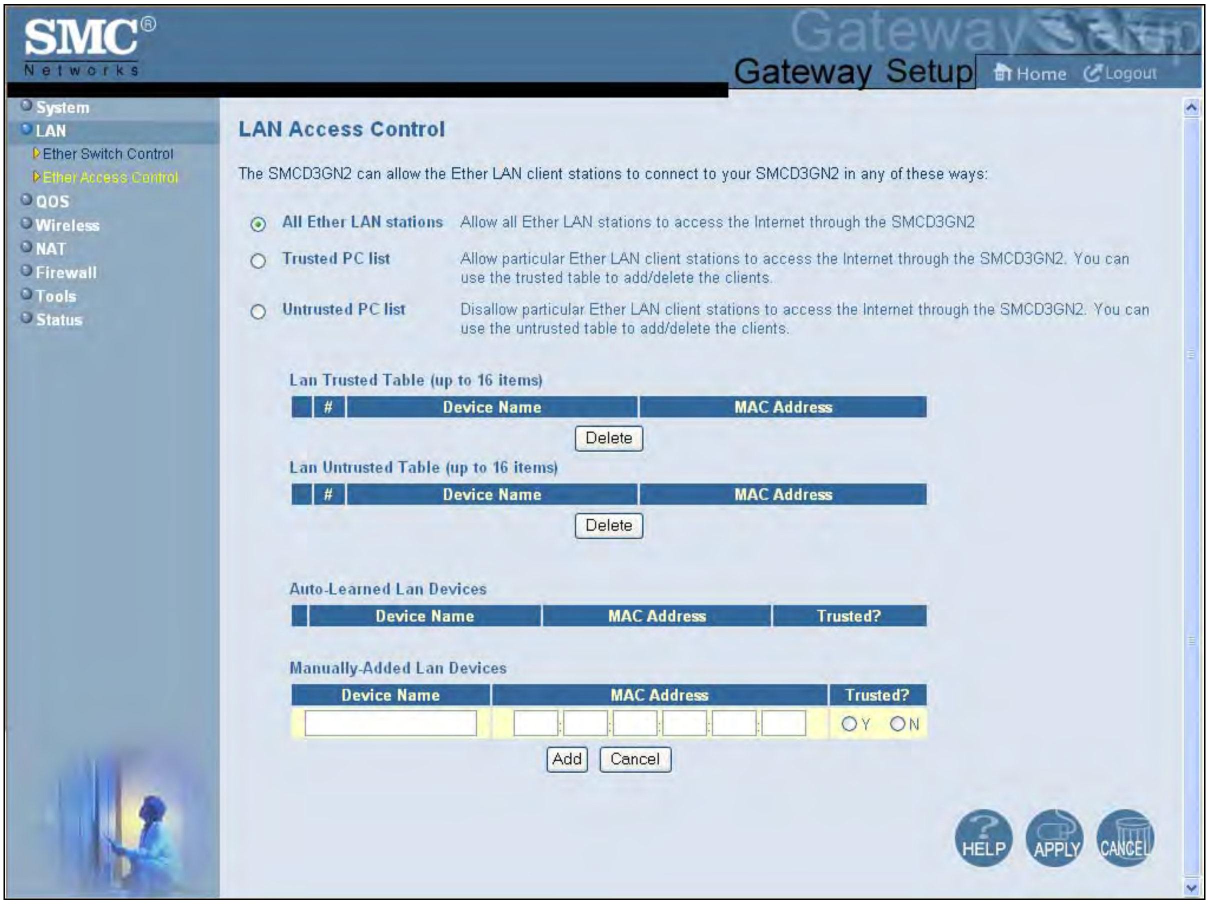
1. To change a port from auto-negotiation to a fixed speed and duplex setting:
   a. Uncheck the **Auto** check box for the port.
   b. Under **Speed (10/100/1000)**, click the radio that corresponds to the fixed speed you want to use for that port.
   c. Under the **Mode H/F** column, leave the check 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 22 shows an example of the menu.



LAN Access Control

The SMCD3GN2 can allow the Ether LAN client stations to connect to your SMCD3GN2 in any of these ways:

● All Ether LAN stations — Allow all Ether LAN stations to access the Internet through the SMCD3GN2

○ Trusted PC list — Allow particular Ether LAN client stations to access the Internet through the SMCD3GN2. 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 SMCD3GN2. You can use the untrusted table to add/delete the clients.

Lan Trusted Table (up to 16 items)

	#	Device Name	MAC Address

Delete

Lan Untrusted Table (up to 16 items)

	#	Device Name	MAC Address

Delete

Auto-Learned Lan Devices

	Device Name	MAC Address	Trusted?

Manually-Added Lan Devices

Device Name	MAC Address	Trusted?
	: : : : :	○ Y ○ N

Add Cancel

Figure 22. 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 43.

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**.

QoS Settings Menu

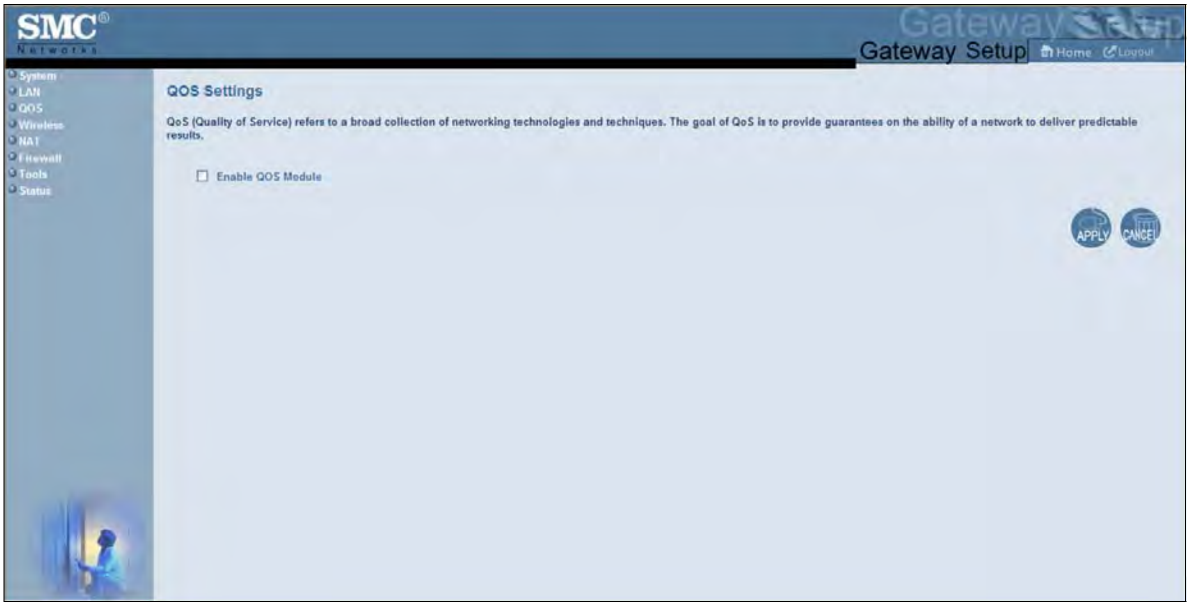
Quality of Service (QoS) refers to a collection of techniques for identifying data whose delivery across the network is time sensitive, and managing its delivery through both bandwidth allocation and prioritization schemes

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 23 shows an example of the menu.

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

When the Gateway's QoS module is enabled, 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 45.
- **COS** - lets you define four queues to which the CoS is mapped. See page 46.
- **DSCP** - lets you define the QoS class queue to which the customized DSCP is mapped. See page 48.
- **Queue** - lets you specify whether QoS behavior runs with strict or weighted priority. See page 50.
- **DSCP Remarking** - lets you define the DSCP remarking action and mode. See page 52.



QOS Settings

QoS (Quality of Service) refers to a broad collection of networking technologies and techniques. The goal of QoS is to provide guarantees on the ability of a network to deliver predictable results.

☐ Enable QOS Module

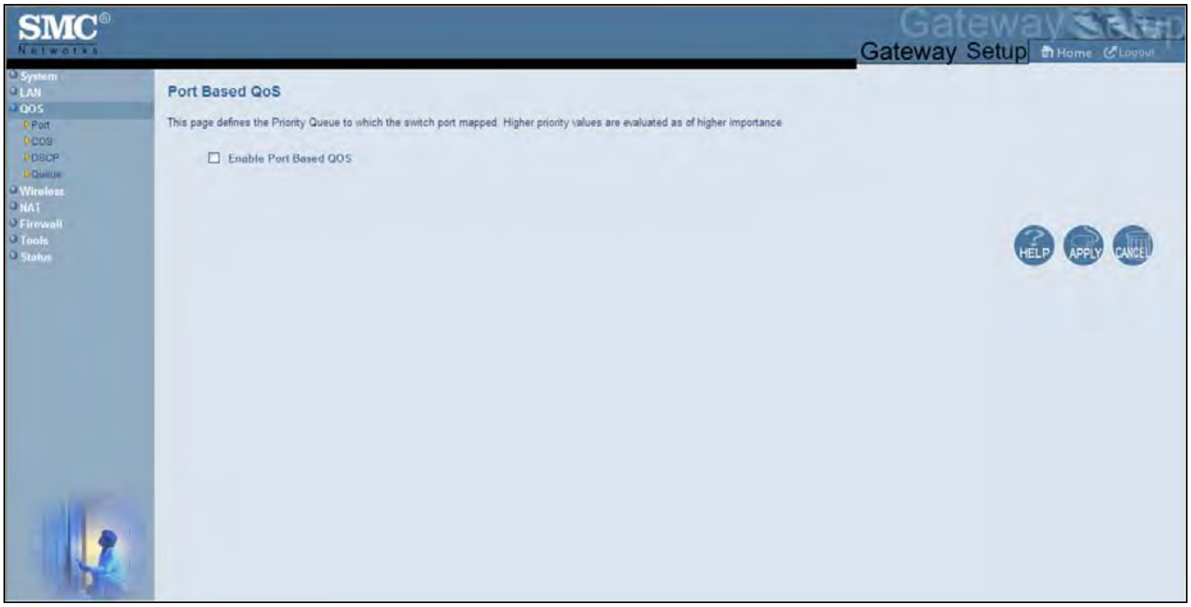
Figure 23. QoS Settings Menu

Port Based QoS Menu

The Port Based QoS menu lets you enable or disable the Gateway's port-based QoS setting. To access the Port Based QoS menu, click **QOS** in the menu bar and then click the **Port** submenu in the menu bar. Figure 24 shows an example of the menu.

- To enable the Gateway's port-based QoS setting, check **Enable Port Based QoS** and click **Apply**.
- To disable the Gateway's port-based QoS setting, uncheck **Enable Port Based QoS** and click **Apply**.

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 39).



Port Based QoS

This page defines the Priority Queue to which the switch port mapped. Higher priority values are evaluated as of higher importance

□ Enable Port Based QOS

Figure 24. Port Based QoS Menu

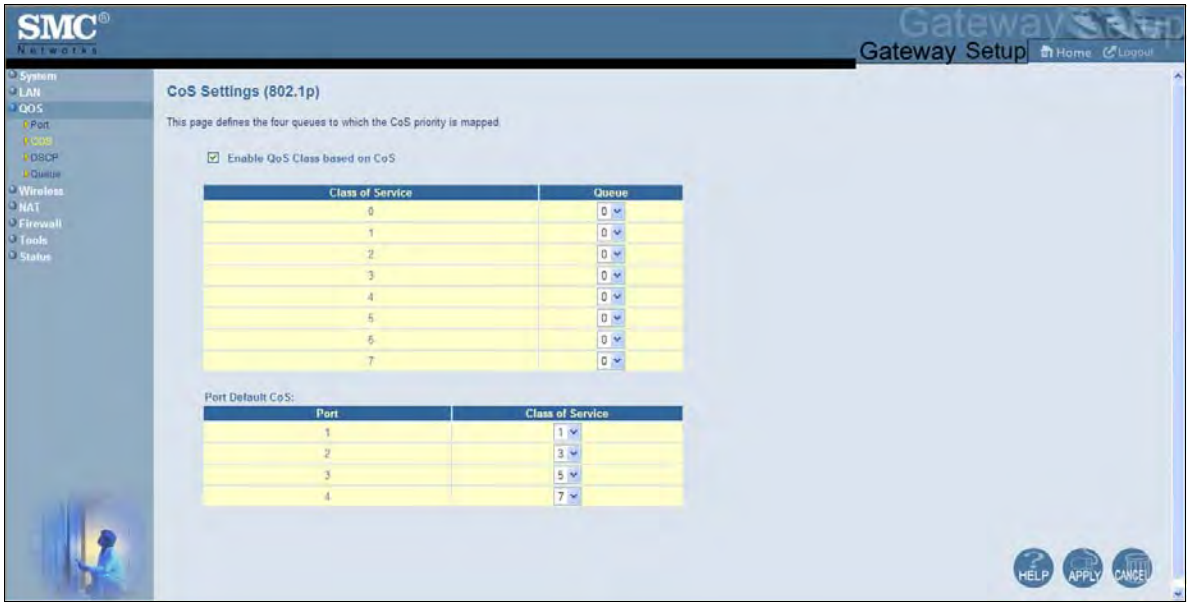
CoS Settings Menu

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 25 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 39).



CoS Settings (802.1p)

This page defines the four queues to which the CoS priority is mapped

☑ Enable QoS Class based on CoS

Class of Service	Queue
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

Port Default CoS:

Port	Class of Service
1	1
2	3
3	5
4	7

Figure 25. 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.

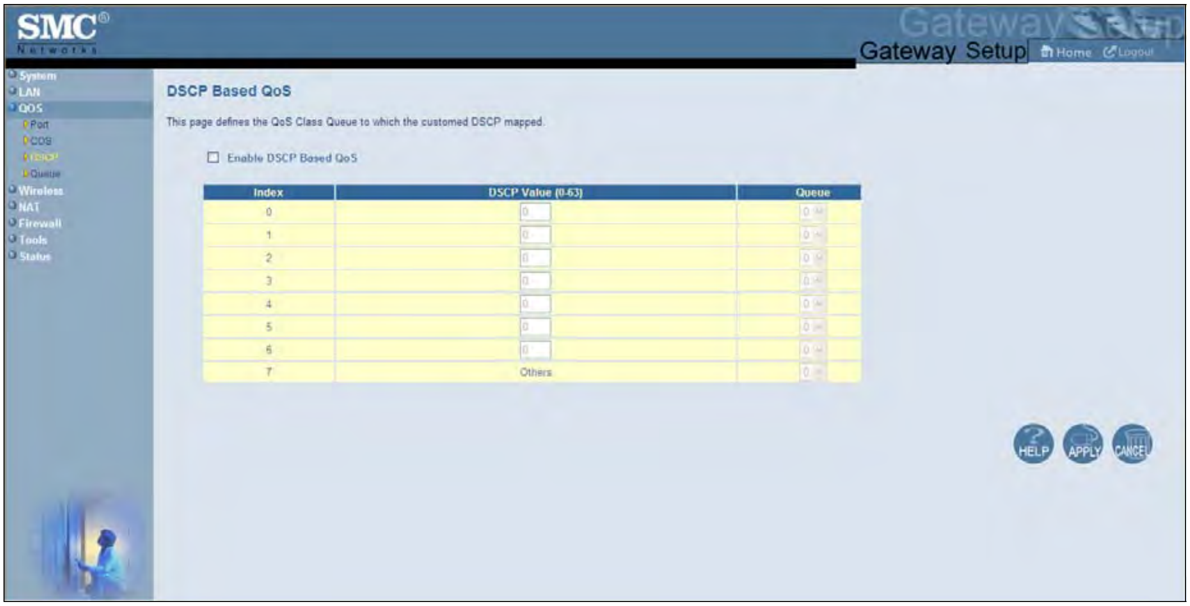
Table 7 shows the actual queuing.

Table 7. 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 26 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 39).



DSCP Based QoS

This page defines the QoS Class Queue to which the customed DSCP mapped.

□ Enable DSCP Based QoS

Index	DSCP Value (0-63)	Queue
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	Others	0

Figure 26. DSCP Based QoS Menu

To define DSCP-based QoS settings:

1. Check **Enable DHCP Based QoS**.
2. For each index, enter 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**.

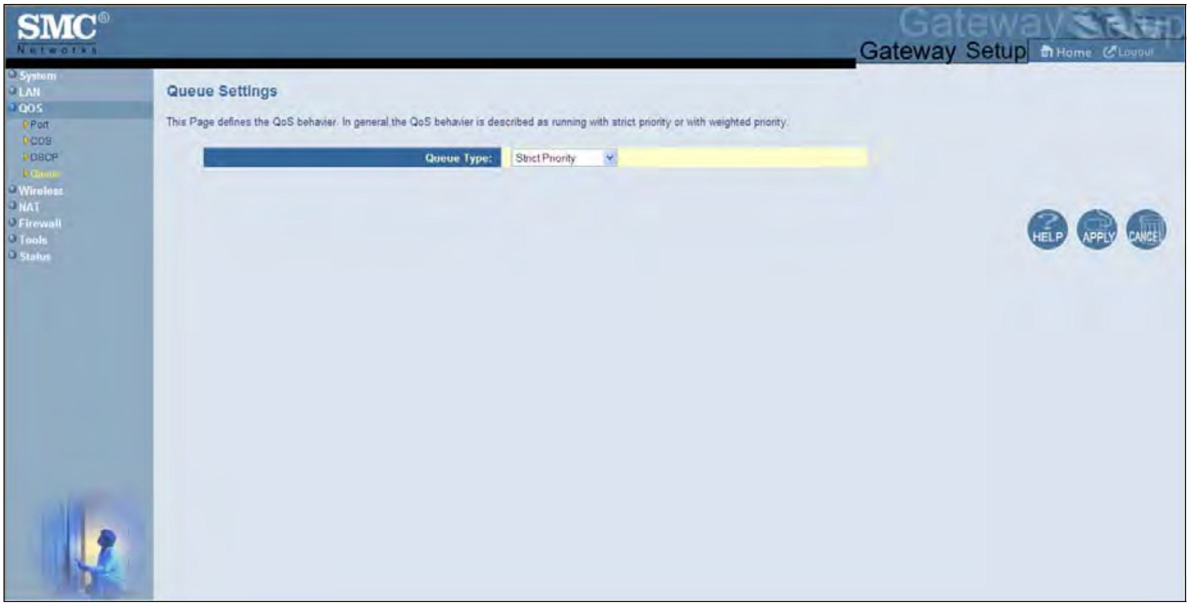
Queue Settings Menu

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 27 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 39).



Queue Settings

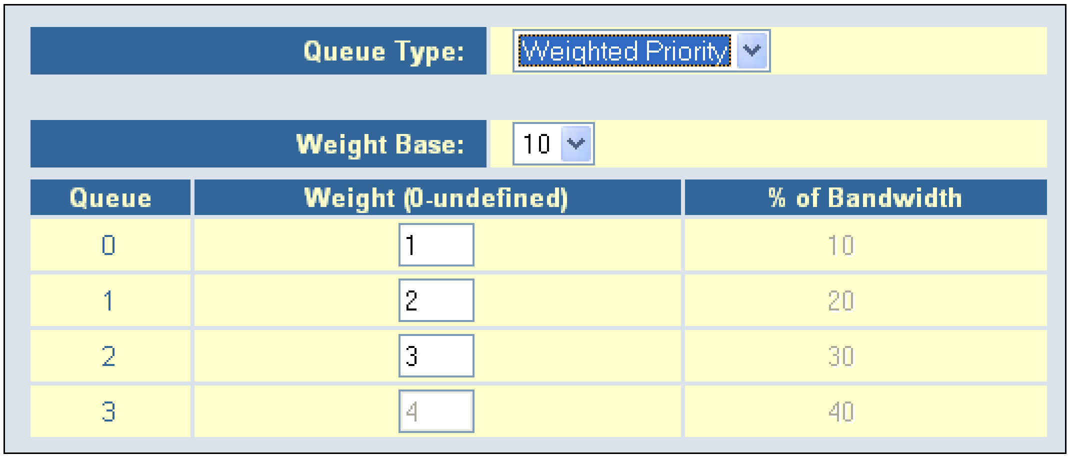
This Page defines the QoS behavier. In general,the QoS behavier is described as running with strict priority or with weighted priority.

Queue Type: Strict Priority

Figure 27. 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 28 appear.



Queue Type: Weighted Priority

Weight Base: 10

Queue	Weight (0-undefined)	% of Bandwidth
0	1	10
1	2	20
2	3	30
3	4	40

Figure 28. Weighted Priority Options

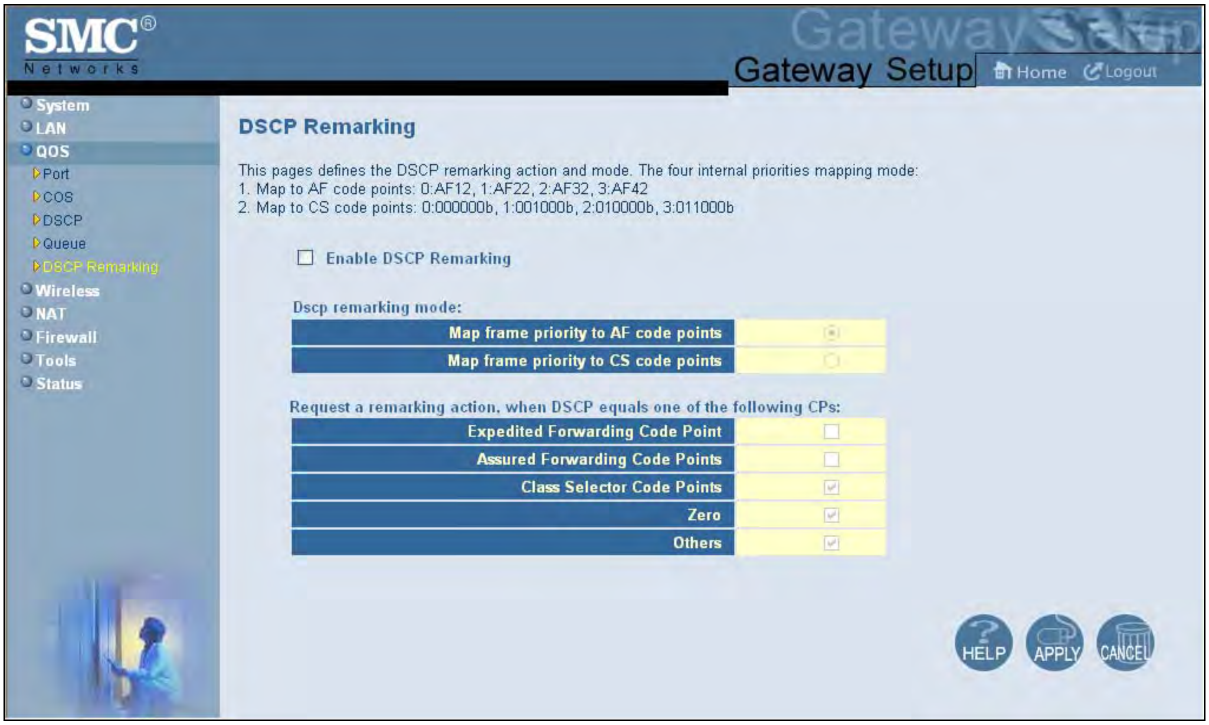
2. For **Weight Base**, select a queue weight to ensure that some sets of queues get higher thresholds than others. Queue weight directs the Gateway to set the queue thresholds proportionately. Choices are **8** or **10**. Queues with a weight of 10 are longer than those with a queue weight of 8.
3. For each Gateway queue, enter 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 29 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 39).



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	●
Map frame priority to CS code points	○

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

Expedited Forwarding Code Point	□
Assured Forwarding Code Points	□
Class Selector Code Points	☑
Zero	☑
Others	☑

Figure 29. DSCP Remarking Menu

To configure DSCP remarking settings:

1. Check **Enable DSCP Remarking**.
2. Complete the options in the menu and refer to Table 8.
3. When you finish, click **Apply**.

Table 8. DSCP Remarking Options

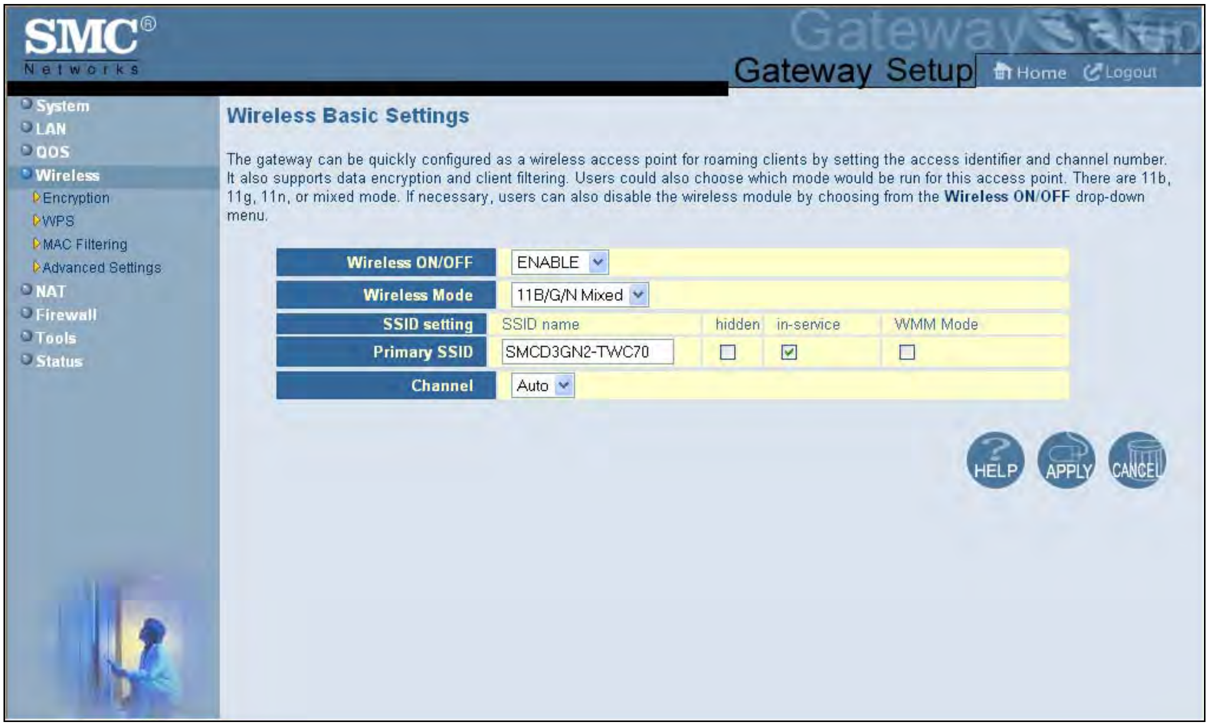
Option	Description
Dscp remarking mode	Lets you select the DSCP remarking mode that the Gateway is to use. Choices are: • Map frame priority to AF code points = select this option for Quality of Service configurations that use assured forwarding (AF) code points to mark packets. AF guarantees a certain amount of bandwidth to an AF class and allows access to extra bandwidth, if available. (*default*) • 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.

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 the primary SSID
- Configuring channel settings

To access the Wireless Basic Settings menu, click **Wireless** in the menu bar. Figure 30 shows an example of the menu and Table 9 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	ENABLE			
Wireless Mode	11B/G/N Mixed			
SSID setting	SSID name	hidden	in-service	WMM Mode
Primary SSID	SMCD3GN2-TWC70	☐	☑	☐
Channel	Auto			

Figure 30. Wireless Basic Settings Menu

Table 9. Wireless Basic Settings Menu Options

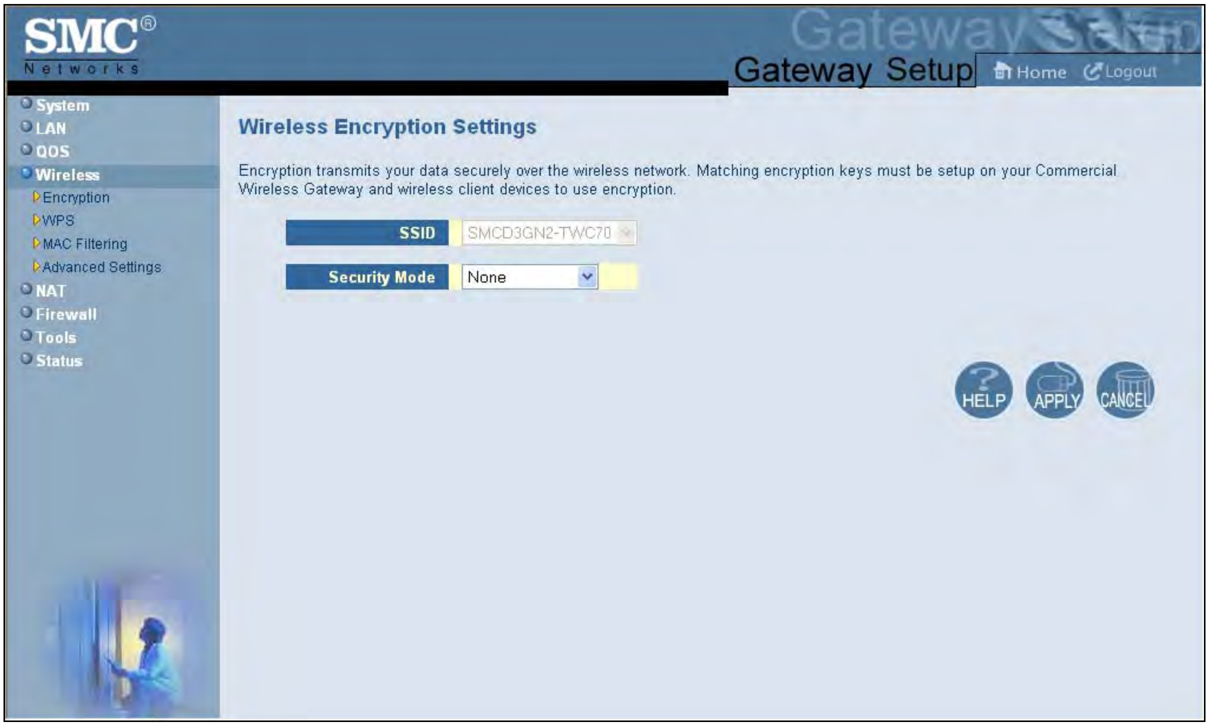
Option	Description
Wireless ON/OFF	Enables or disables the Gateway's wireless operation. • ENABLE = Gateway's wireless operation is active. Selecting this option activates the options in this menu. Clicking **Apply** displays the submenus below the Wireless menu. • DISABLE = Gateway's wireless operation is not active. Selecting this option deactivates the options in this menu. Clicking **Apply** hides the submenus below the Wireless menu. (*default*)
Wireless Mode	If wireless operation is enabled for the Gateway, this option selects the wireless mode used by the Gateway. Choices are: • 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. (*default*)
SSID setting	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 this setting is the same for all devices in your wireless network.
Primary SSID	The primary SSID can be hidden or configured for Wi-Fi Multimedia (WMM) mode. • 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	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.

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 31 shows an example of the menu and Table 10 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 54).



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.

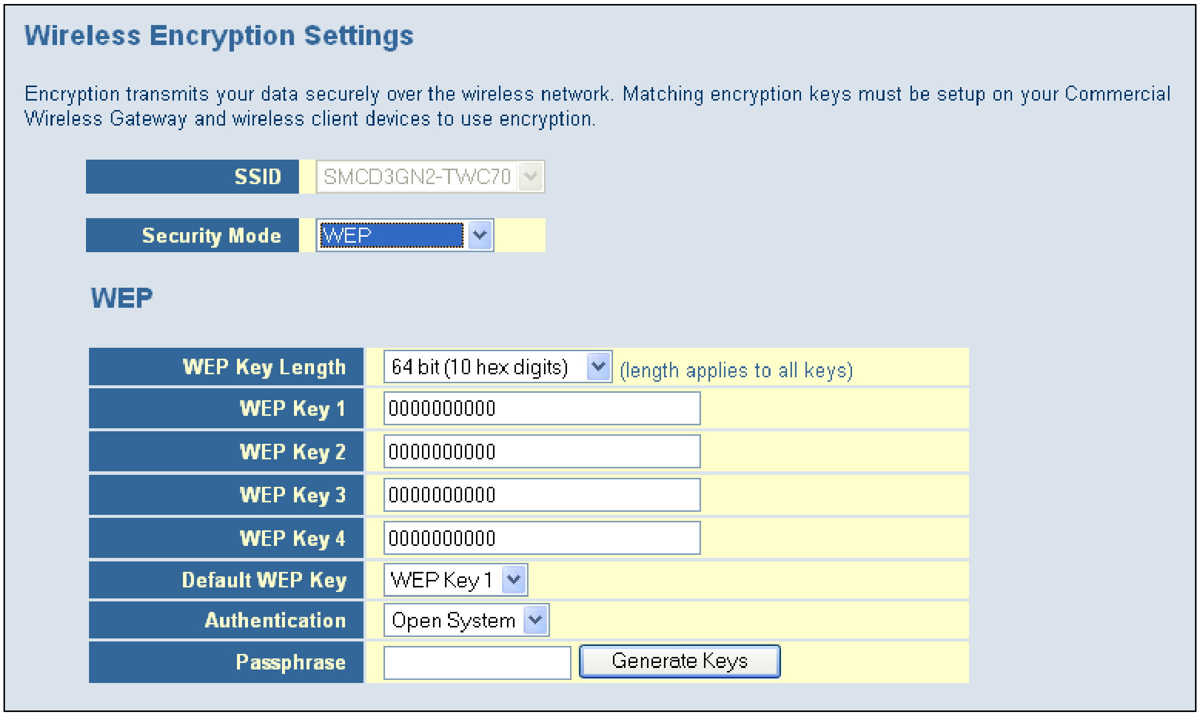
SSID: SMCD3GN2-TWC70

Security Mode: None

Figure 31. Wireless Encryption Settings Menu

Table 10. Wireless Encryption Settings Menu Options

Option	Description
SSID	Network name of the of the primary wireless carrier. This field can be changed by administrators, but not 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 32 and Table 11. • 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 33 and Table 12. (*default*)



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: SMCD3GN2-TWC70

Security Mode: WEP

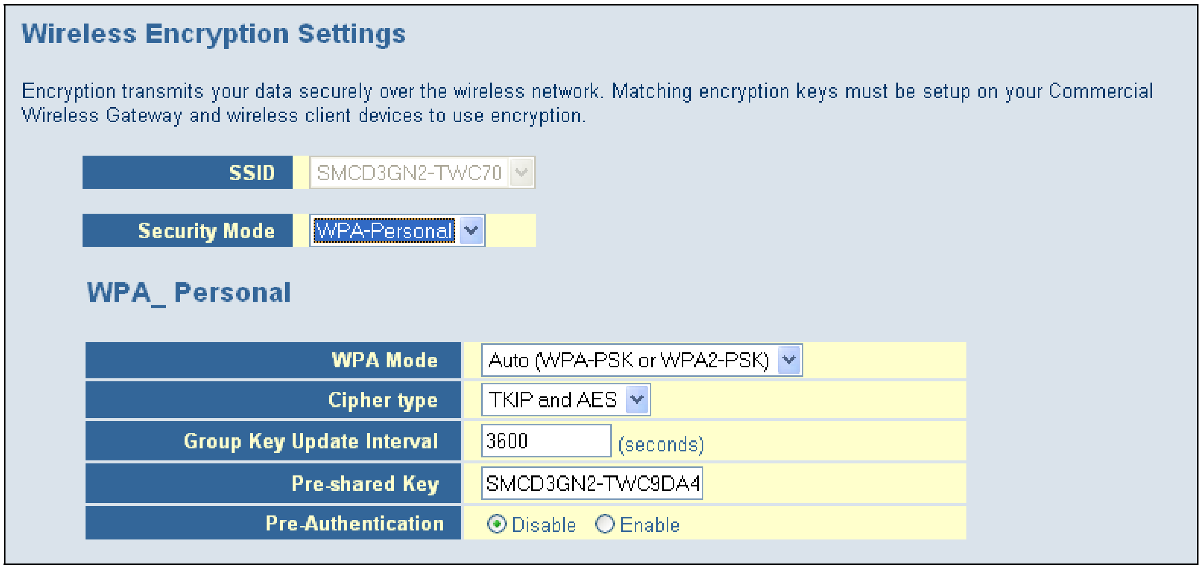
WEP

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	

Figure 32. WEP Options

Table 11. 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: • Open System = clients can only associate to the wireless access point using Open Option. (*default*) • 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 from 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: SMCD3GN2-TWC70

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: SMCD3GN2-TWC9DA4

Pre-Authentication: ● Disable ○ Enable

Figure 33. WPA_Personal Options

Table 12. WPA_Personal Options

Option	Description
WPA Mode	Lets you select the WPA mode they want to use. Choices are: • 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 WPA2-PSK) = select this setting if your access points and wireless clients support either WPA-PSK or WPA2-PSK. (*default*)
Cipher type	Algorithm encryption to be used. Choices are: • 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. (*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	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.

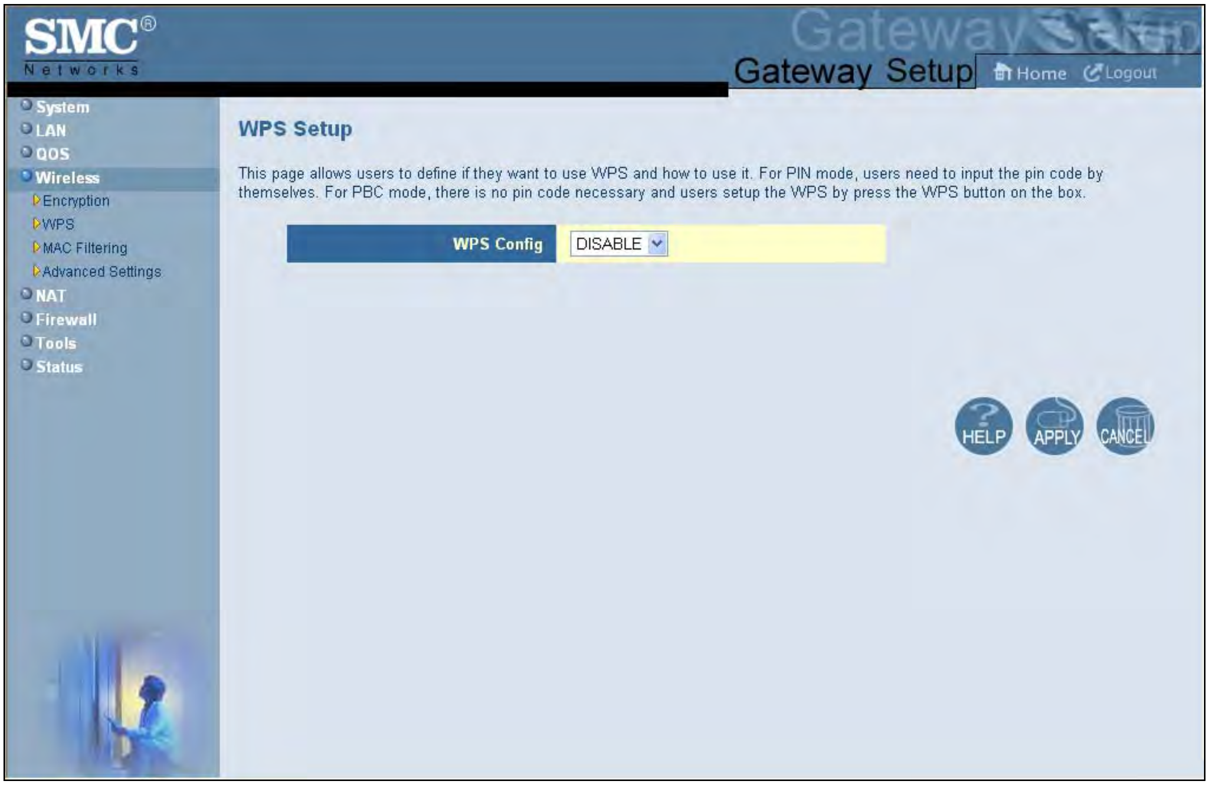
The advantages of WPS are:

- 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 34 shows an example of the menu. Using the **WPS Config** drop-down list, select the appropriate option to enable or disable WPS setup.



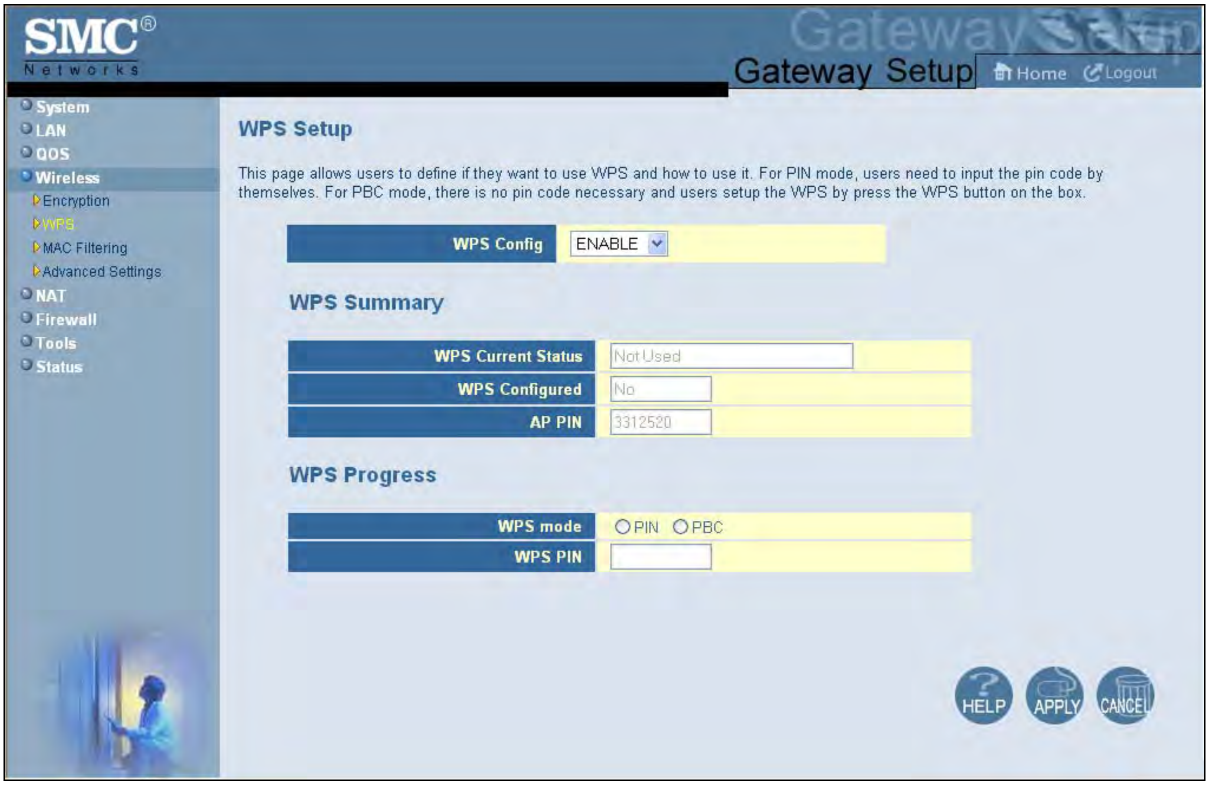
WPS Setup

This page allows users to define if they want to use WPS and how to use it. For PIN mode, users need to input the pin code by themselves. For PBC mode, there is no pin code necessary and users setup the WPS by press the WPS button on the box.

WPS Config: DISABLE

Figure 34. WPS Setup Menu

By default, WPS is disabled. If you select **ENABLE** and click **Apply**, the options in Figure 35 are displayed. Table 13 describes the options shown.



WPS Setup

This page allows users to define if they want to use WPS and how to use it. For PIN mode, users need to input the pin code by themselves. For PBC mode, there is no pin code necessary and users setup the WPS by press the WPS button on the box.

WPS Config: ENABLE

WPS Summary

WPS Current Status: Not Used

WPS Configured: No

AP PIN: 3312520

WPS Progress

WPS mode: ○ PIN ○ PBC

WPS PIN:

Figure 35. WPS Setup Menu with WPS Config Enabled

Table 13. WPS Summary and WPS Progress Options

Option	Description
WPS Config	Enables or disables the Gateway's WPS setup. • ENABLE = Gateway's WPS setup is available. (*default*) • 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. • PIN = requires you to enter a PIN in the WPS Setup menu to configure WPS. • PBC = Push Button Configuration. Lets you 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 required to enable WPS. The PIN must be 8 alpha-numeric characters long.

MAC Filtering

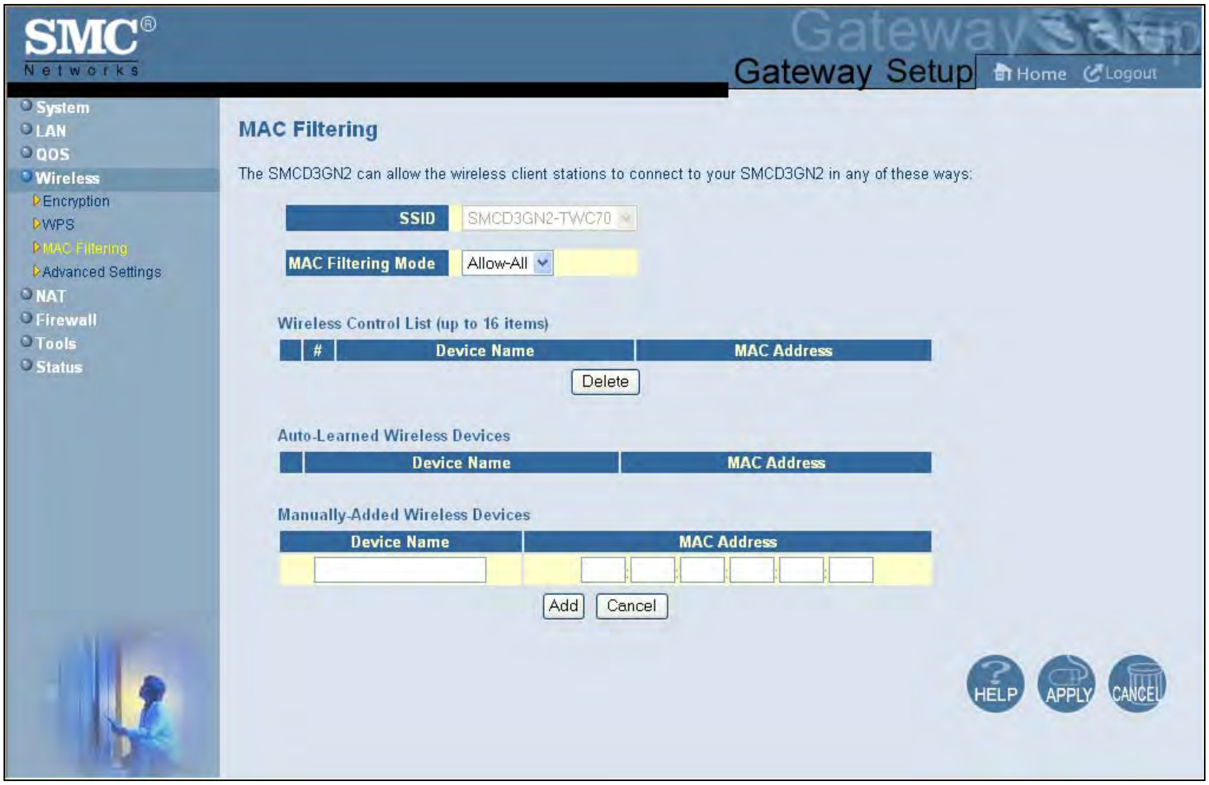
Using the MAC Filtering menu, you can define up to 16 MAC address filters to prevent PCs from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. This is useful because a specific NIC's MAC address never changes, unlike its IP address, which can be assigned by a DHCP server or hard-coded to various addresses over time.

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. Figure 36 shows an example of the menu and Table 14 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 54).



MAC Filtering

The SMCD3GN2 can allow the wireless client stations to connect to your SMCD3GN2 in any of these ways:

SSID: SMCD3GN2-TWC70

MAC Filtering Mode: Allow-All

Wireless Control List (up to 16 items)

	#	Device Name	MAC Address

Auto-Learned Wireless Devices

	Device Name	MAC Address

Manually-Added Wireless Devices

Device Name	MAC Address

Figure 36. MAC Filtering Menu

Table 14. MAC Filtering Options

Option	Description
SSID	Network name of the of the primary wireless carrier.
MAC Filtering Mode	Determines which wireless client stations can connect to the Gateway. The choices are: • Allow- All = all wireless client stations can connect to the Gateway. (*default*) • 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.

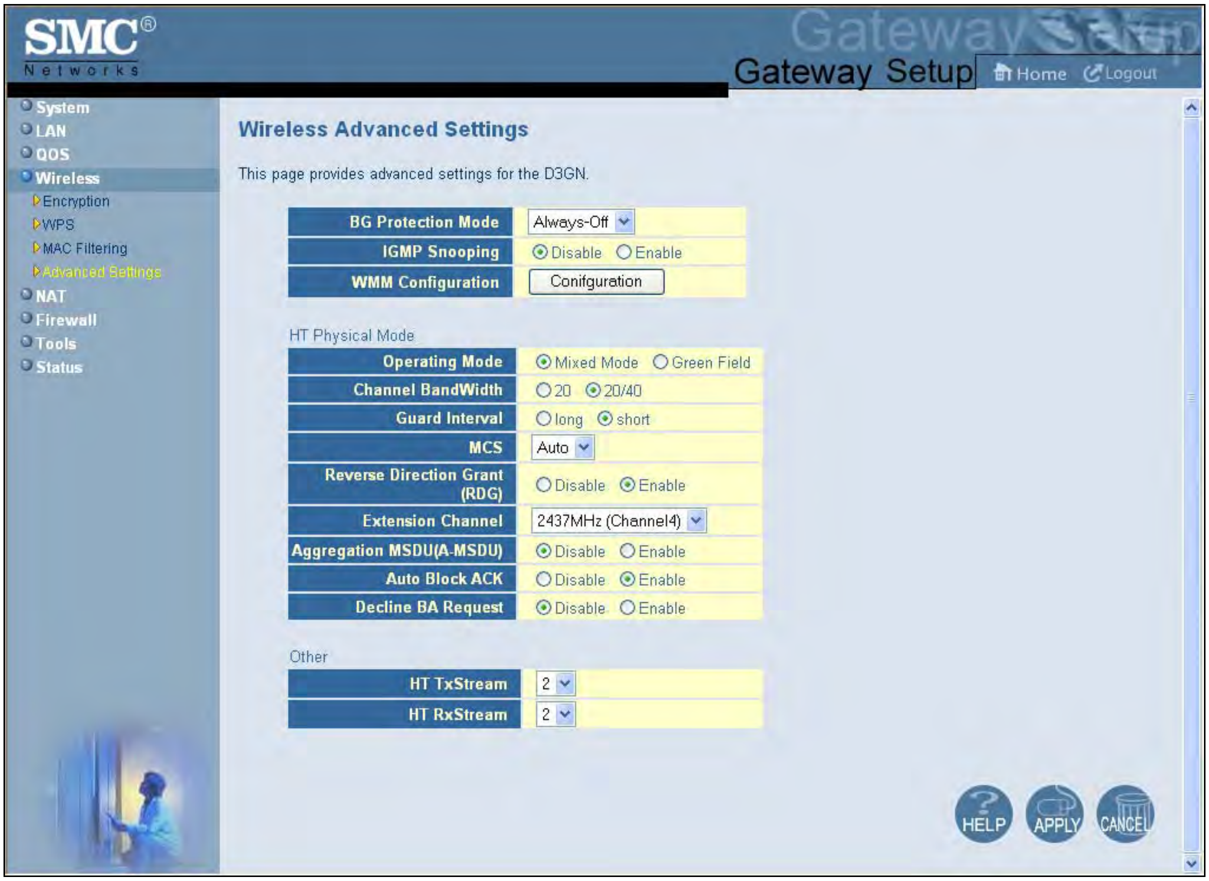
1. To add wireless client stations that the Gateway automatically learned on the network, perform the following steps under **Auto-Learned Lan Devices**:
   a. Click a wireless client station that the Gateway learned automatically.
   b. Click **Add**. The wireless client station is added to the **Wireless Control List**.
   c. To add more auto-learned wireless client stations (up to 16), repeat steps 1a and 1b.
2. To manually add wireless client stations, perform the following steps under **Manually-Added Wireless Devices**:
   a. Under **Device Name**, enter a unique name for the device (that is, a name that does not already appear in the **Wireless Control List**).
   b. Under **MAC Address**, enter the MAC address of the device.
   c. Click **Add** to add the wireless client station to the **Wireless Control List**.
   d. To manually add more wireless client stations (up to 16), repeat steps 2a through 2c.
3. 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.
4. When you finish, click **Apply**.

Advanced Wireless Settings Menu

Using the Advanced Wireless Settings 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 37 shows an example of the menu and Table 15 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 54).



Wireless Advanced Settings

This page provides advanced settings for the D3GN.

BG Protection Mode	Always-Off
IGMP Snooping	● Disable ○ Enable
WMM Configuration	Conifguration

HT Physical Mode

Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ long ● short
MCS	Auto
Reverse Direction Grant (RDG)	○ Disable ● Enable
Extension Channel	2437MHz (Channel4)
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable

Other

HT TxStream	2
HT RxStream	2

Figure 37. Wireless Advanced Settings Menu

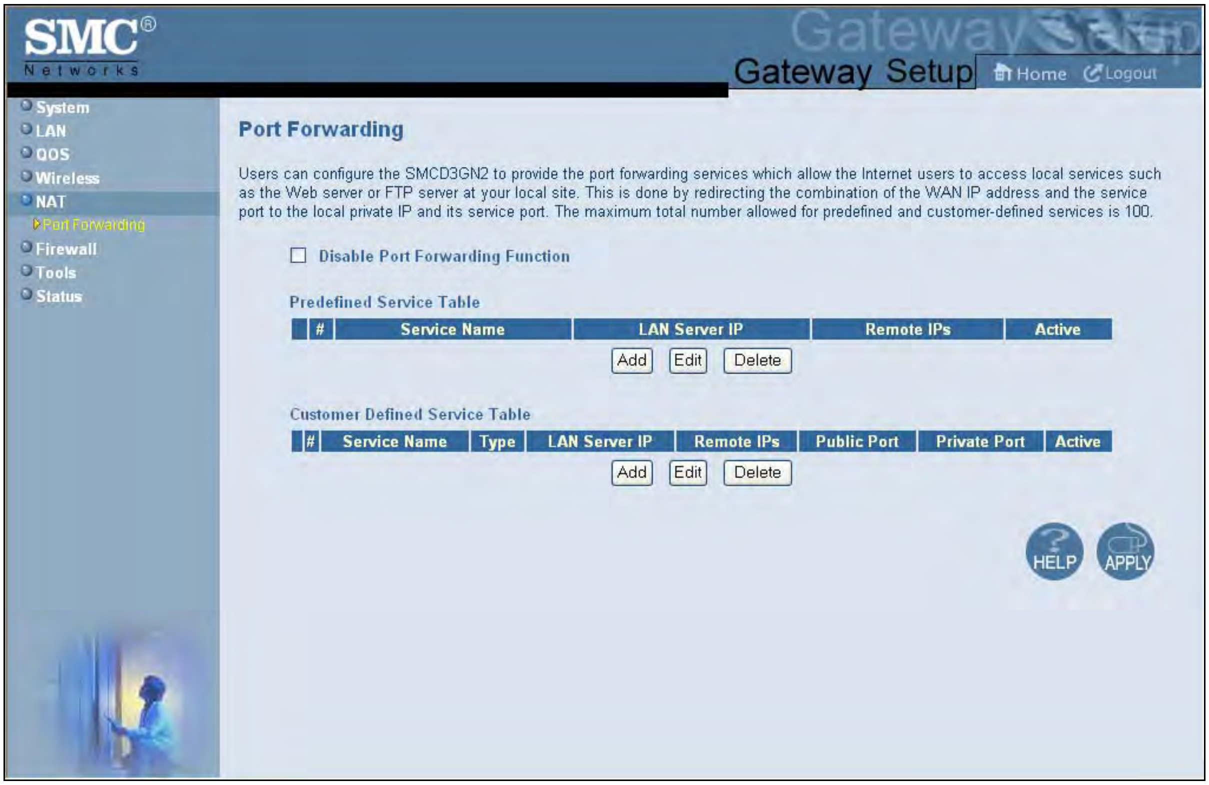
Table 15. Wireless Advanced Settings Options

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 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 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.
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 enable.
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 38 shows an example of the menu.



Port Forwarding

Users can configure the SMCD3GN2 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

Add Edit Delete

Customer Defined Service Table

	#	Service Name	Type	LAN Server IP	Remote IPs	Public Port	Private Port	Active

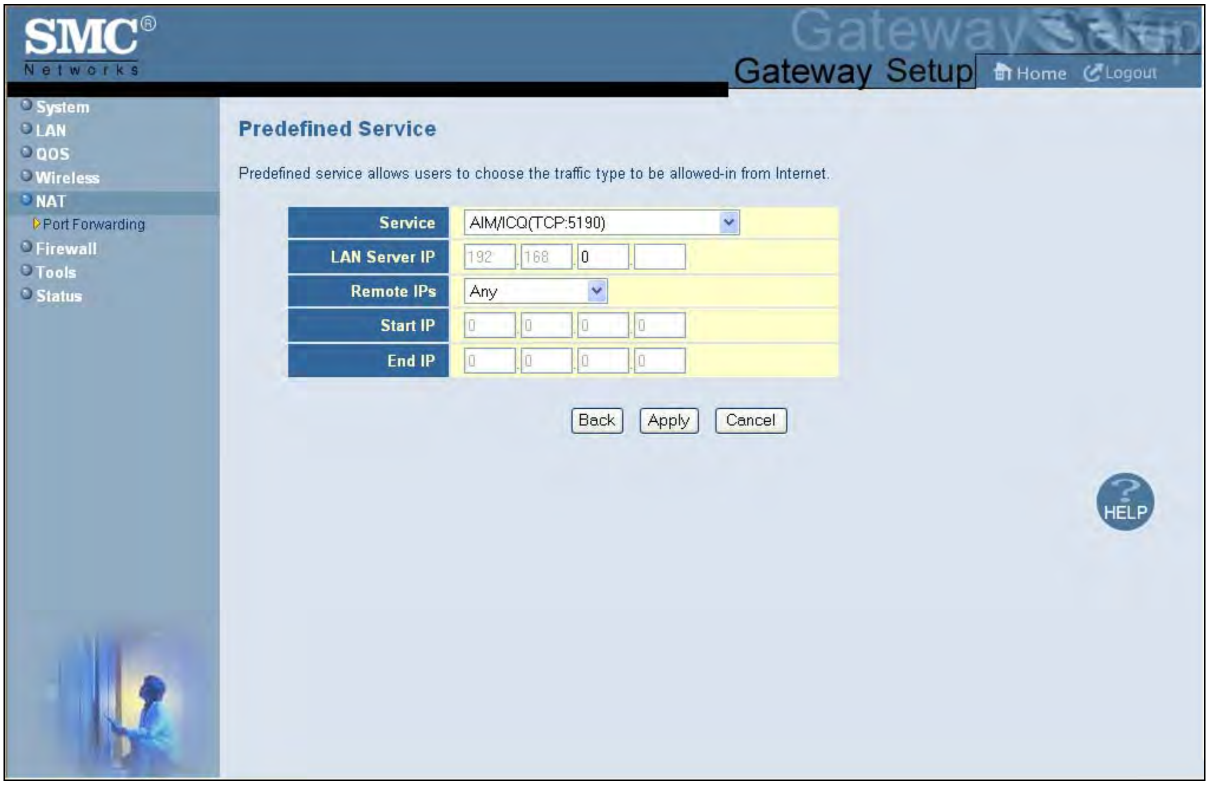
Add Edit Delete

Figure 38. 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, uncheck **Disable Port Forwarding Function** if it is checked.
2. Click the **Add** button below the **Predefined Service Table**. The Predefined Service menu appears (see Figure 39).
3. Complete the fields in the Predefined Service menu (see Table 16).
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 2 through 4.
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 16) 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.



Predefined Service

Predefined service allows users to choose the traffic type to be allowed-in from Internet.

Service	AIM/ICQ(TCP:5190)
LAN Server IP	192 . 168 . 0 .
Remote IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0

Figure 39. Predefined Service Menu

Table 16. 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. • 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: • 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

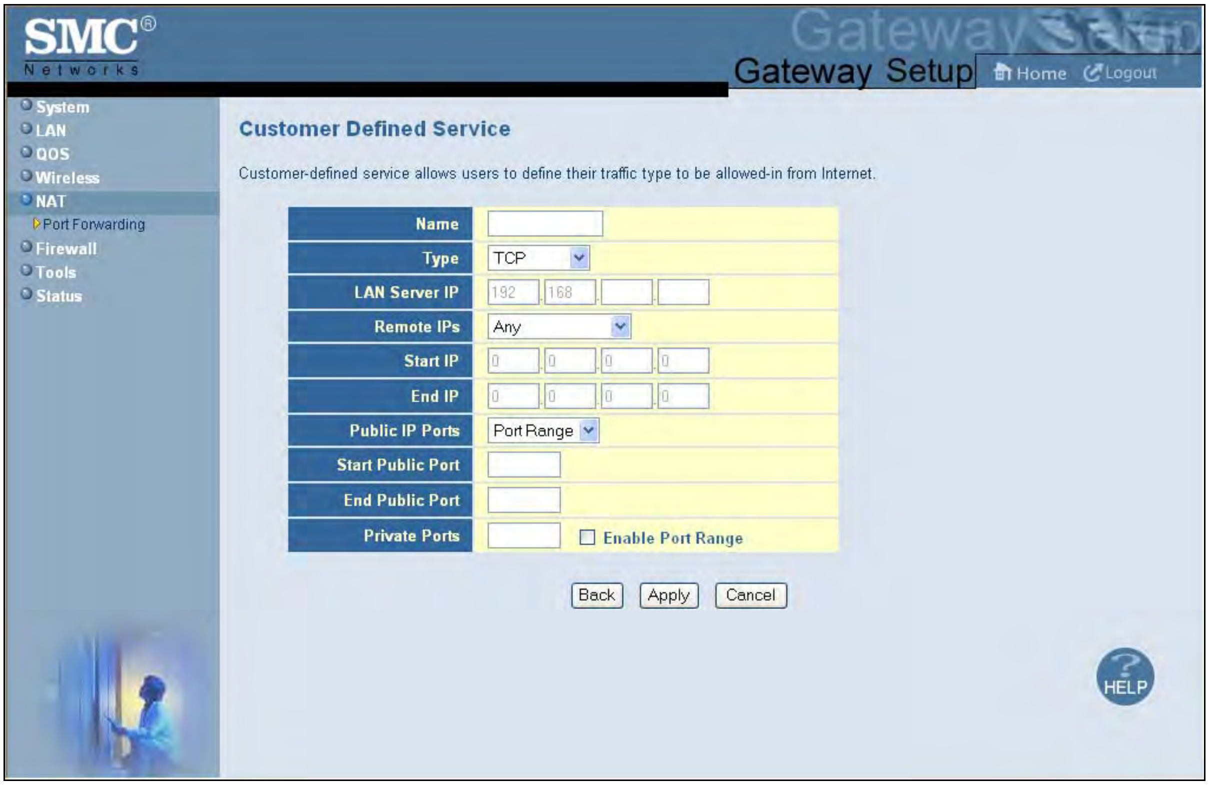
Using the following procedure, you can define special application services you want to provide to the Internet. The following example shows how to set port forwarding for a Web server on an Internet connection, where port 80 is blocked from the WAN side, but port 8000 is available.

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, uncheck **Disable Port Forwarding Function** if it is checked.
2. Click the **Add** button below the **Customer Defined Service Table**. The Customer Defined Service menu appears (see Figure 40).
3. Complete the fields in the Customer Defined Service menu (see Table 17).
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 2 through 4.
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 17) 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.



Customer Defined Service

Customer-defined service allows users to define their traffic type to be allowed-in from Internet.

Name	
Type	TCP
LAN Server IP	192 . 168 . .
Remote IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0
Public IP Ports	Port Range
Start Public Port	
End Public Port	
Private Ports	□ Enable Port Range

Figure 40. Customer Defined Service Menu

Table 17. 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. • 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: • 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. • 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).

Security Settings (Firewall) Menu

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

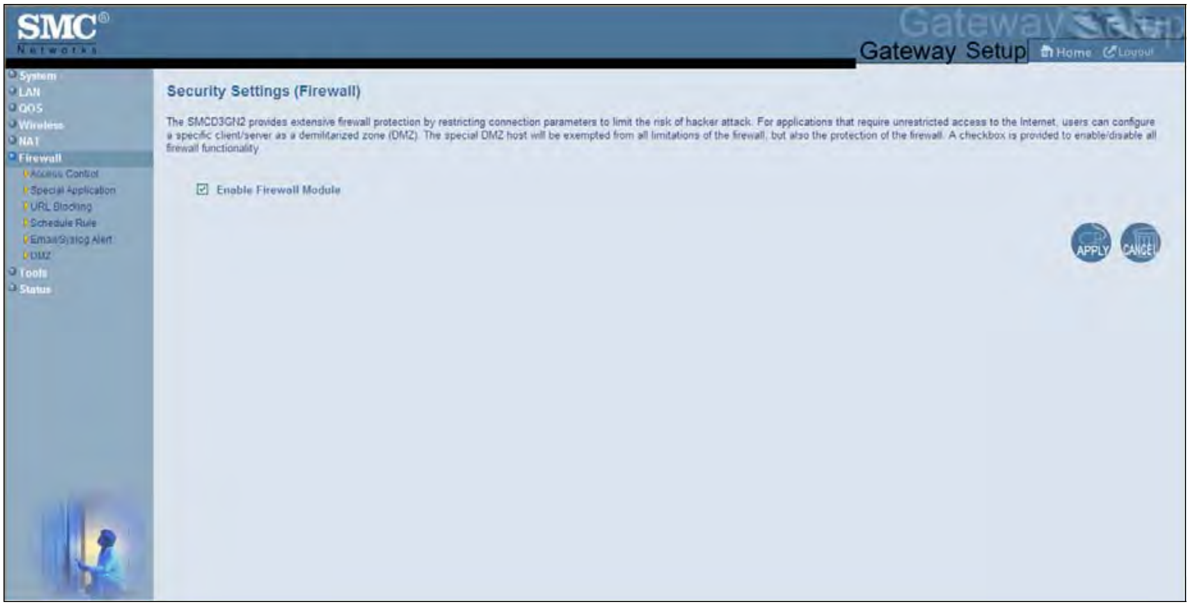
If you enable the Gateway firewall module, the following submenus appear in the menu bar:

- Configure access control settings — see page 74
- Configure the Gateway for special applications — see page 76
- Set up URL blocking — see page 90
- Schedule rules — see page 92
- Receive email or syslog alert notifications — see page 93
- Configure a local client computer as a local DMZ for unrestricted two-way Internet access — see page 97

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 41 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.



Security Settings (Firewall)

The SMCD3GN2 provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack. For applications that require unrestricted access to the Internet, users can configure a specific client/server as a demilitarized zone (DMZ). The special DMZ host will be exempted from all limitations of the firewall, but also the protection of the firewall. A checkbox is provided to enable/disable all firewall functionality

☑ Enable Firewall Module

Figure 41. Security Settings (Firewall) Menu

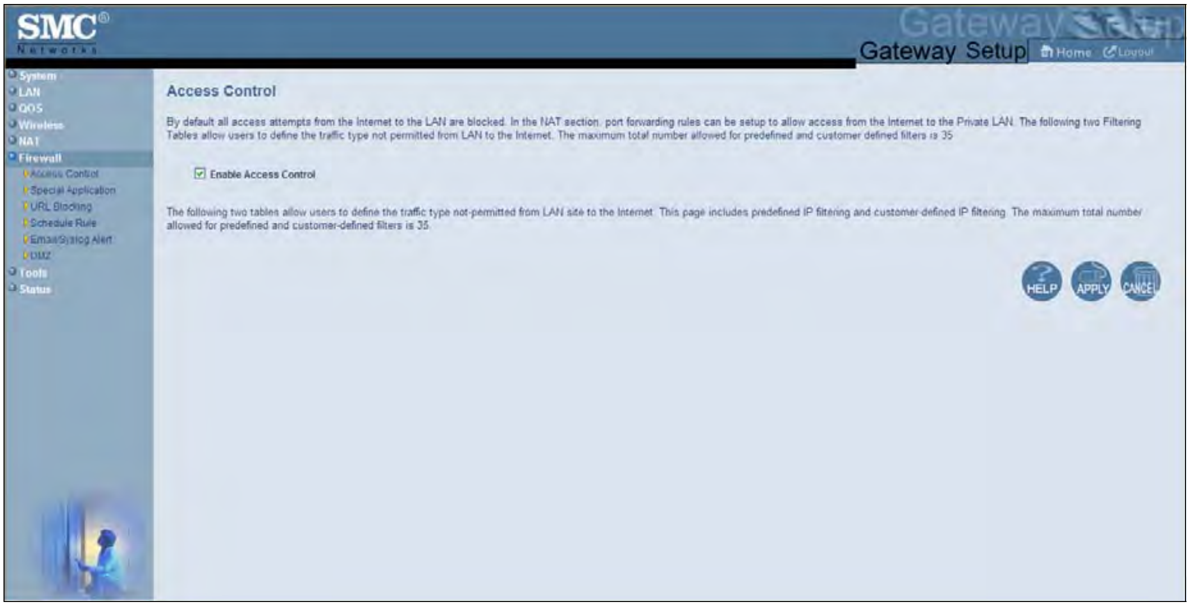
Configuring Access Control

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 73).

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.

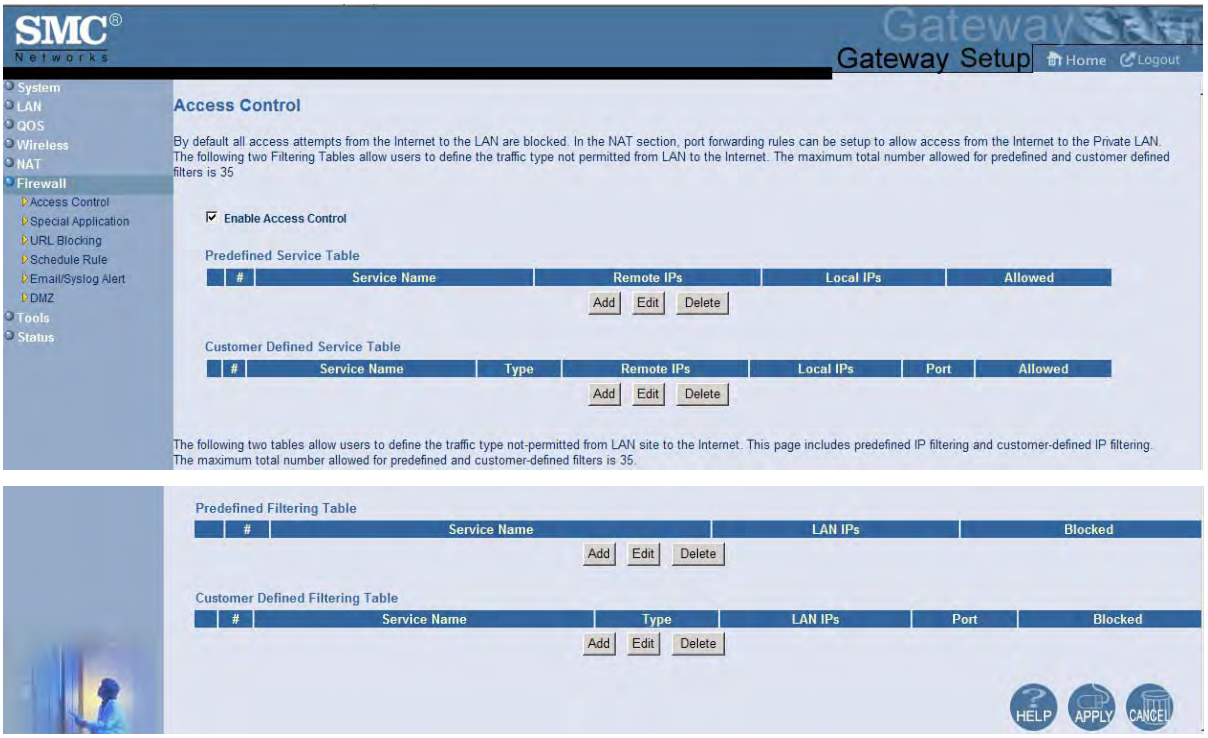


Access Control

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. 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

☑ Enable Access Control

The following two tables allow users to define the traffic type not-permitted from LAN site to the Internet. This page includes predefined IP filtering and customer-defined IP filtering. The maximum total number allowed for predefined and customer-defined filters is 35.



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. 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

☑ Enable Access Control

Predefined Service Table

	#	Service Name	Remote IPs	Local IPs	Allowed

Customer Defined Service Table

	#	Service Name	Type	Remote IPs	Local IPs	Port	Allowed

The following two tables allow users to define the traffic type not-permitted from LAN site to the Internet. This page includes predefined IP filtering and customer-defined IP filtering. The maximum total number allowed for predefined and customer-defined filters is 35.

Predefined Filtering Table

	#	Service Name	LAN IPs	Blocked

Customer Defined Filtering Table

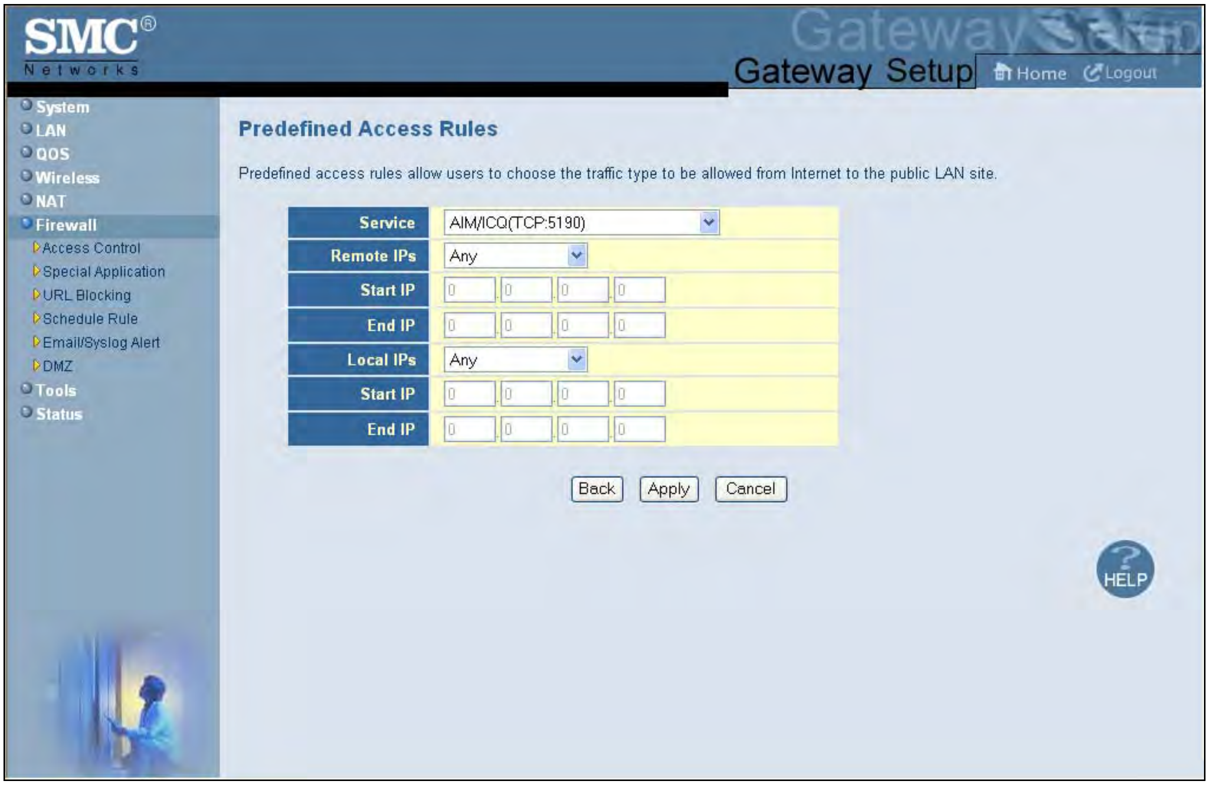
	#	Service Name	Type	LAN IPs	Port	Blocked

Figure 42. 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 43).
3. Complete the fields in the Predefined Access Rules menu (see Table 18).
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 2 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 18) 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.



Predefined Access Rules

Predefined access rules allow users to choose the traffic type to be allowed from Internet to the public LAN site.

Service	AIM/ICQ(TCP:5190)
Remote IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0
Local IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0

Figure 43. Predefined Access Rules Menu

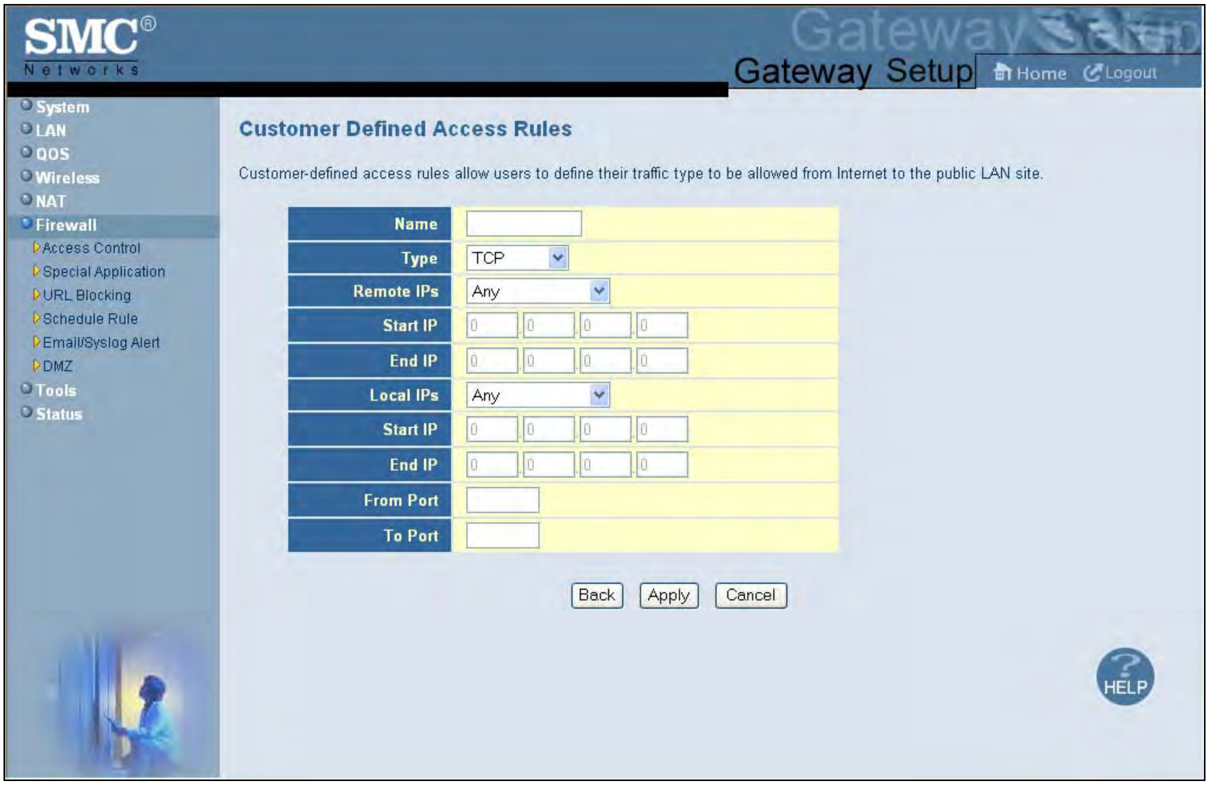
Table 18. Predefined Access Rules Menu Options

Option	Description
Service	List of predefined services from which you can choose.
Remote IPs	Allows access to any remote IP address, one remote IP address, or a range of remote IP addresses. • 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: • 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.
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. • 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: • 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.

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 44).
3. Complete the fields in the Customer Defined Access Rules menu (see Table 19).
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 2 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 19) 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.



Customer Defined Access Rules

Customer-defined access rules allow users to define their traffic type to be allowed from Internet to the public LAN site.

Name	
Type	TCP
Remote IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0
Local IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0
From Port	
To Port	

Figure 44. Customer Defined Access Rules Menu

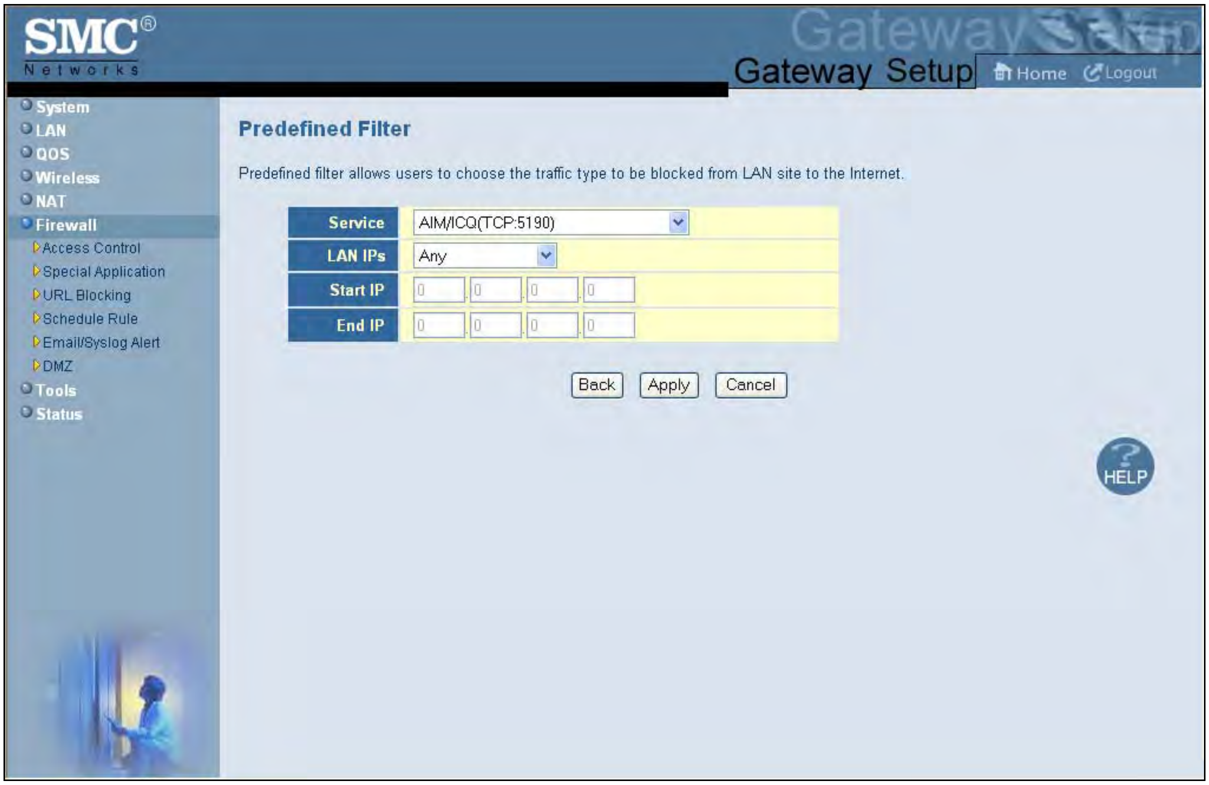
Table 19. Customer Defined Access Rules Menu Options

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. • 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: • 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. • 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: • 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 45).
3. Complete the fields in the Predefined Filter menu (see Table 20).
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 2 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 20) 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.



Predefined Filter

Predefined filter allows users to choose the traffic type to be blocked from LAN site to the Internet.

Service	AIM/ICQ(TCP:5190)
LAN IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0

Figure 45. Predefined Filter Menu

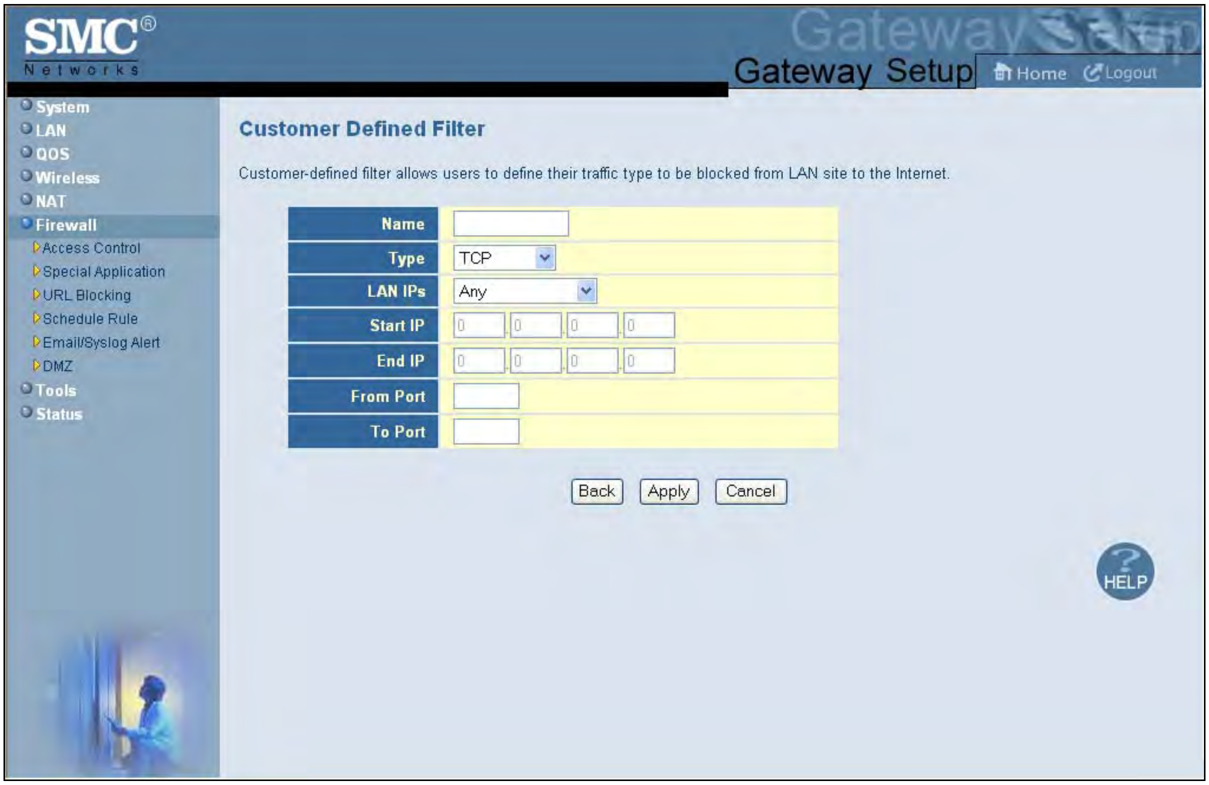
Table 20. Predefined Filter Menu Options

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. • 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: • 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 46).
3. Complete the fields in the Customer Defined Filter menu (see Table 21).
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 2 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 21) 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.



Customer Defined Filter

Customer-defined filter allows users to define their traffic type to be blocked from LAN site to the Internet.

Name	
Type	TCP
LAN IPs	Any
Start IP	0 . 0 . 0 . 0
End IP	0 . 0 . 0 . 0
From Port	
To Port	

Back Apply Cancel

Figure 46. Customer Defined Filter Menu

Table 21. 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. • 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: • 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.

Configuring Special Applications

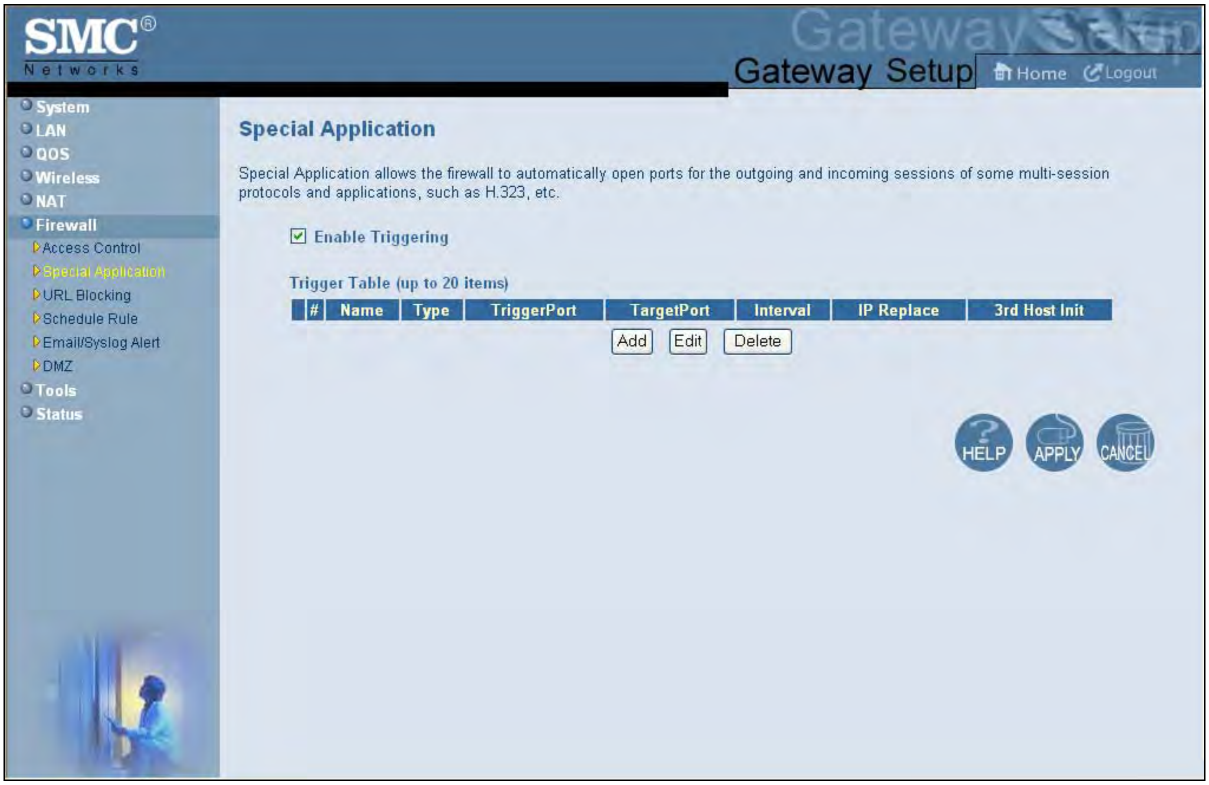
Using the Special Application menu, you can configure the Gateway to detect port triggers for detect multiple-session applications and allow them to pass the firewall. For special applications, besides the initial communication session, there are multiple related sessions created during the protocol 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 47 shows an example of the menu.

The maximum number of allowed triggers is 20. 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 73).



Special Application

Special Application allows the firewall to automatically open ports for the outgoing and incoming sessions of some multi-session protocols and applications, such as H.323, etc.

☑ Enable Triggering

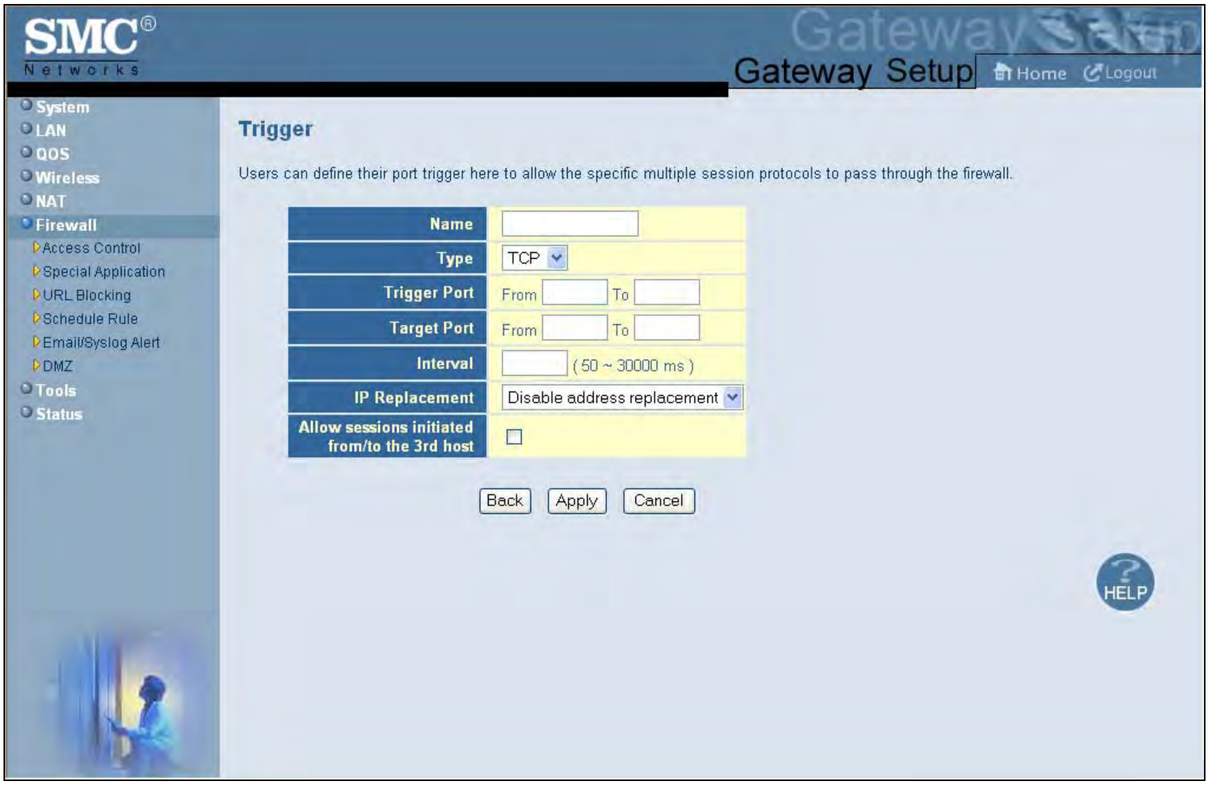
Trigger Table (up to 20 items)

#	Name	Type	TriggerPort	TargetPort	Interval	IP Replace	3rd Host Init

Figure 47. 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 48).
3. Complete the fields in fields Trigger menu (see Table 22).
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 22) 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.



Trigger

Users can define their port trigger here to allow the specific multiple session protocols to pass through the firewall.

Name	
Type	TCP
Trigger Port	From ___ To ___
Target Port	From ___ To ___
Interval	(50 ~ 30000 ms)
IP Replacement	Disable address replacement
Allow sessions initiated from/to the 3rd host	☐

Figure 48. Trigger Menu

Table 22. 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 3rd 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

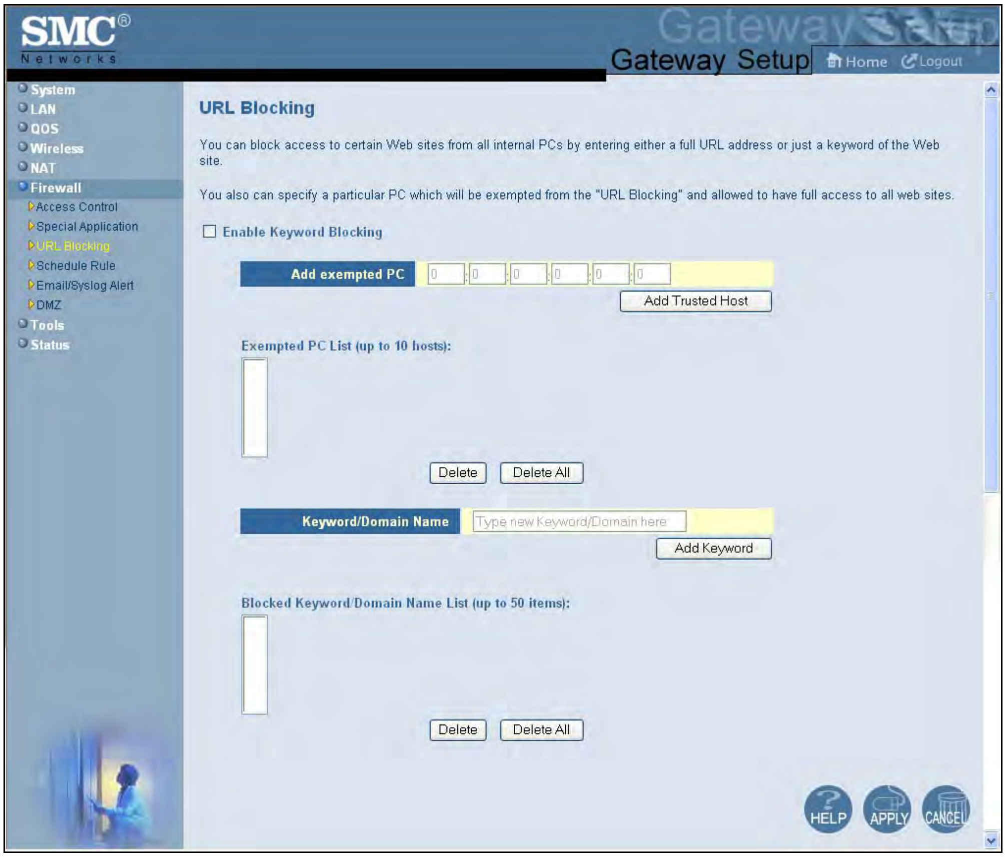
Using the URL Blocking menu, you can configure the Gateway to block access to certain Web sites from local computers by entering either a full URL address or keywords of the Web site. the Gateway examines all the HTTP packets to block the access to those particular sites. This feature can be used to 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 49 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 73).

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 92.



URL Blocking

You can block access to certain Web sites from all internal PCs by entering either a full URL address or just a keyword of the Web site.

You also can specify a particular PC which will be exempted from the "URL Blocking" and allowed to have full access to all web sites.

□ Enable Keyword Blocking

Add exempted PC: 0 . 0 . 0 . 0 . 0 . 0

Add Trusted Host

Exempted PC List (up to 10 hosts):

Delete | Delete All

Keyword/Domain Name: Type new Keyword/Domain here

Add Keyword

Blocked Keyword/Domain Name List (up to 50 items):

Delete | Delete All

Figure 49. URL Blocking Menu

To enable URL blocking:

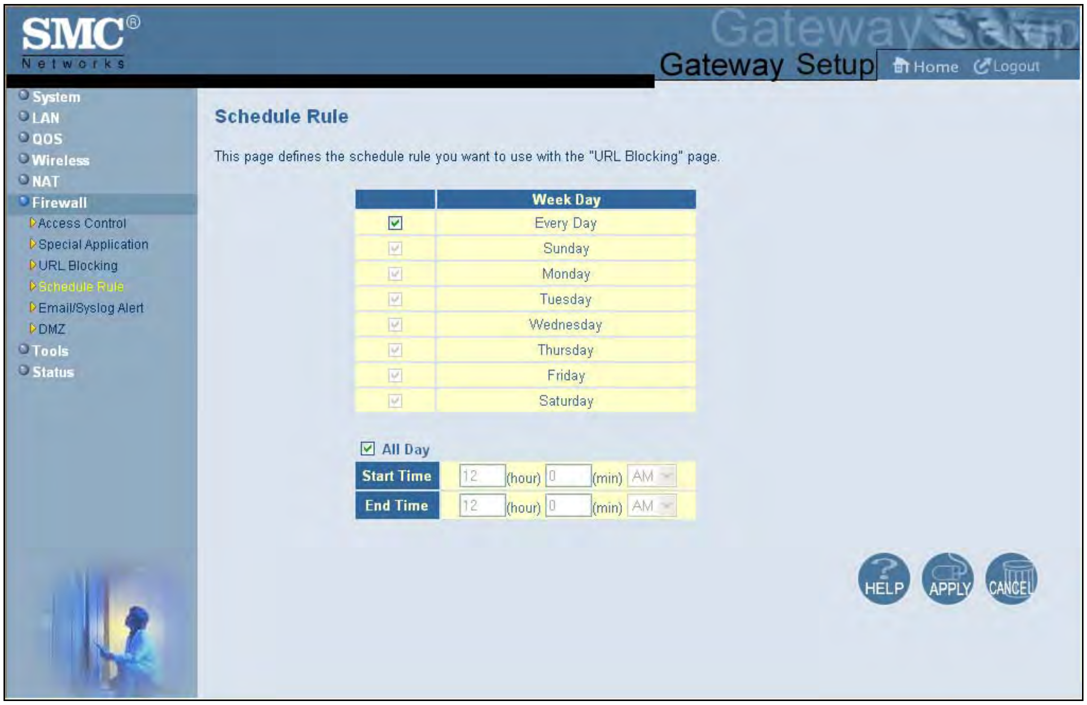
1. In the URL Blocking menu, check **Enable Keyword Blocking** if it is not checked and click **Apply**.
2. To exempt a computer from URL blocking, enter the computer's MAC address in the **Add exempted PC** field and click the **Add Trusted Host** button. The MAC address you entered appears in the **Exempted 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 90) 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 50 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 73).



Schedule Rule

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

	Week Day
☑	Every Day
☑	Sunday
☑	Monday
☑	Tuesday
☑	Wednesday
☑	Thursday
☑	Friday
☑	Saturday

☑ All Day

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

Figure 50. 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:

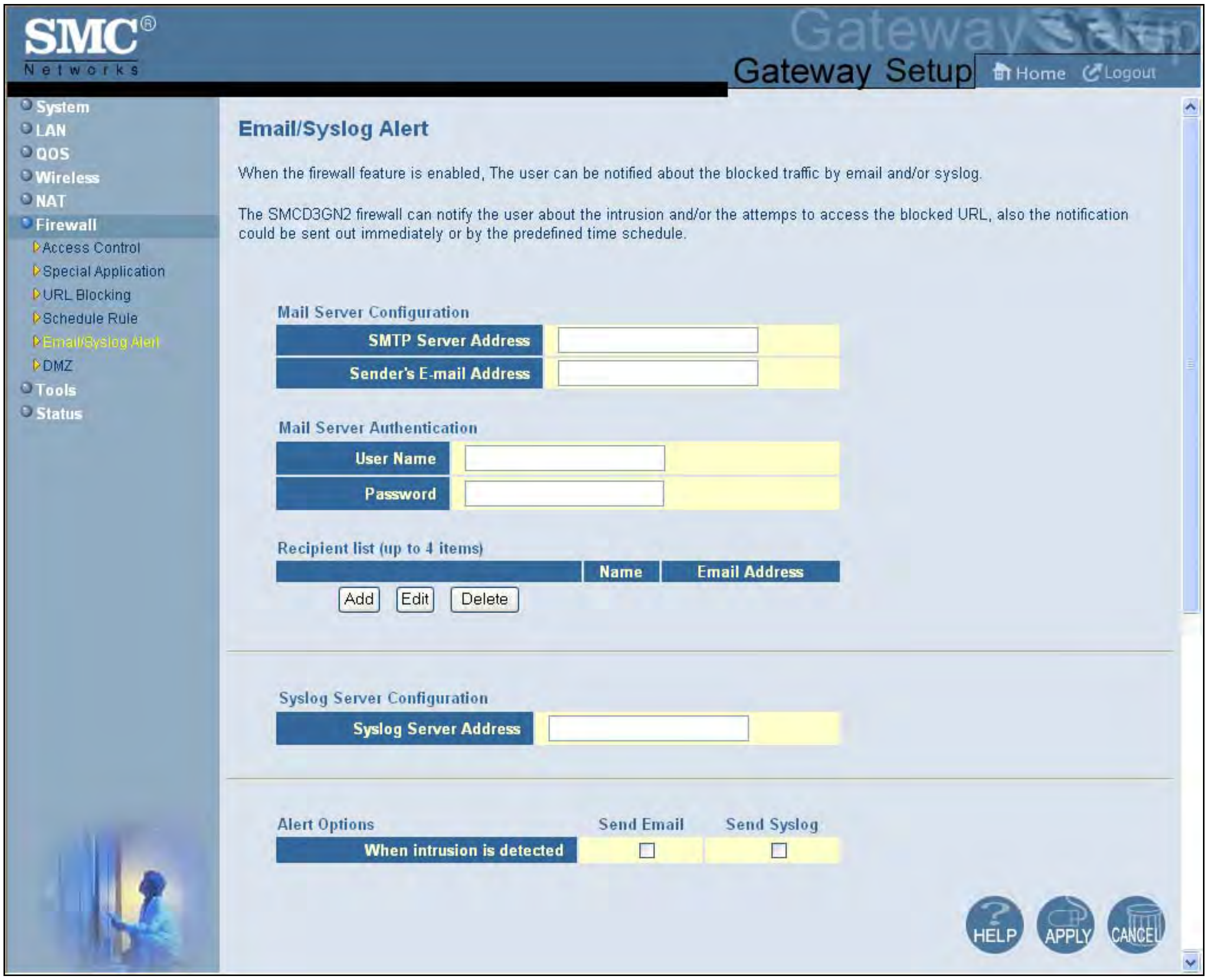
- Traffic is blocked
- Attempts are made to intrude onto the network
- Local computers try to access block URLs

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. Figure 51 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.

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 73).



Email/Syslog Alert

When the firewall feature is enabled, The user can be notified about the blocked traffic by email and/or syslog.

The SMCD3GN2 firewall can notify the user about the intrusion and/or the attemps to access the blocked URL, also the notification could be sent out immediately or by the predefined time schedule.

Mail Server Configuration

SMTP Server Address	
Sender's E-mail Address	

Mail Server Authentication

User Name	
Password	

Recipient list (up to 4 items)

	Name	Email Address

Syslog Server Configuration

Syslog Server Address	

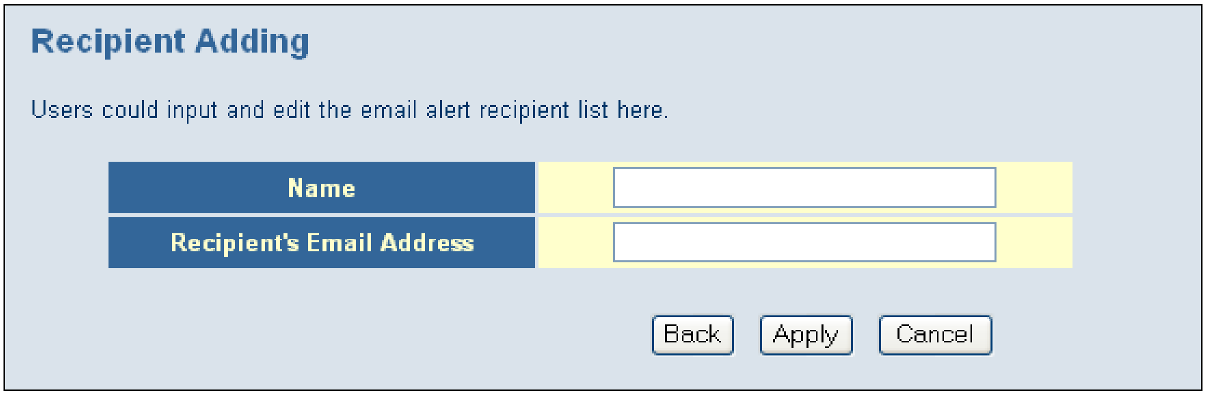
Alert Options	Send Email	Send Syslog
When intrusion is detected	□	□

Figure 51. 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 52), 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	
Recipient's Email Address	

Figure 52. 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 blocked 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 95.
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:

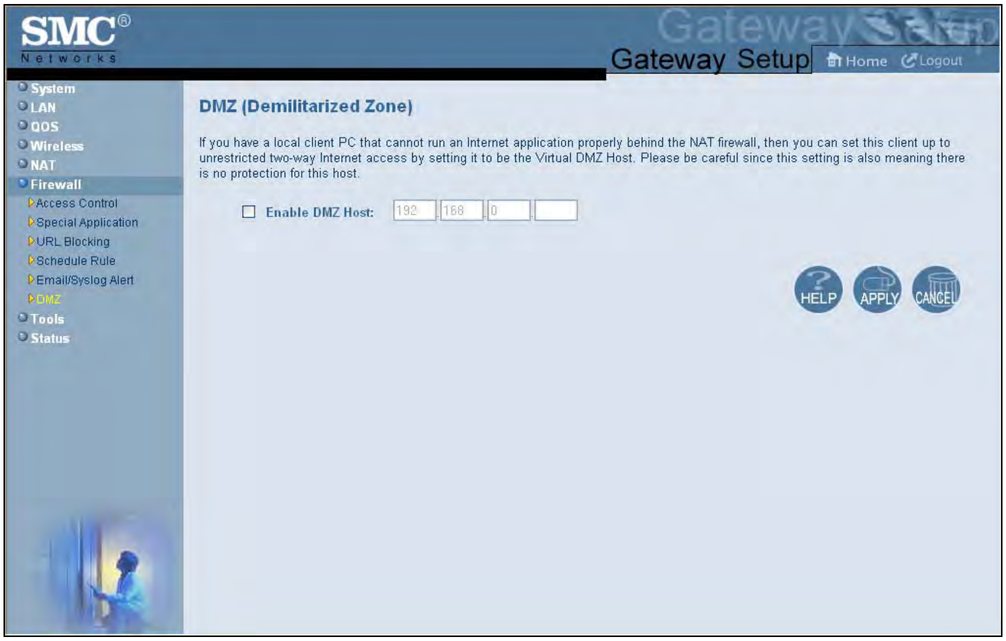
1. Perform step 1 under “Configuring Syslog Entries” on page 96.
2. Under **Alert Options**, check **Send Syslog** next to **When intrusion is detected**.
4. Click **Apply**.

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 53 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 73).



DMZ (Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly behind the NAT firewall, then you can set this client up to unrestricted two-way Internet access by setting it to be the Virtual DMZ Host. Please be careful since this setting is also meaning there is no protection for this host.

☐ Enable DMZ Host: 192 . 168 . 0 .

Figure 53. DMZ (Demilitarized Zone) Menu

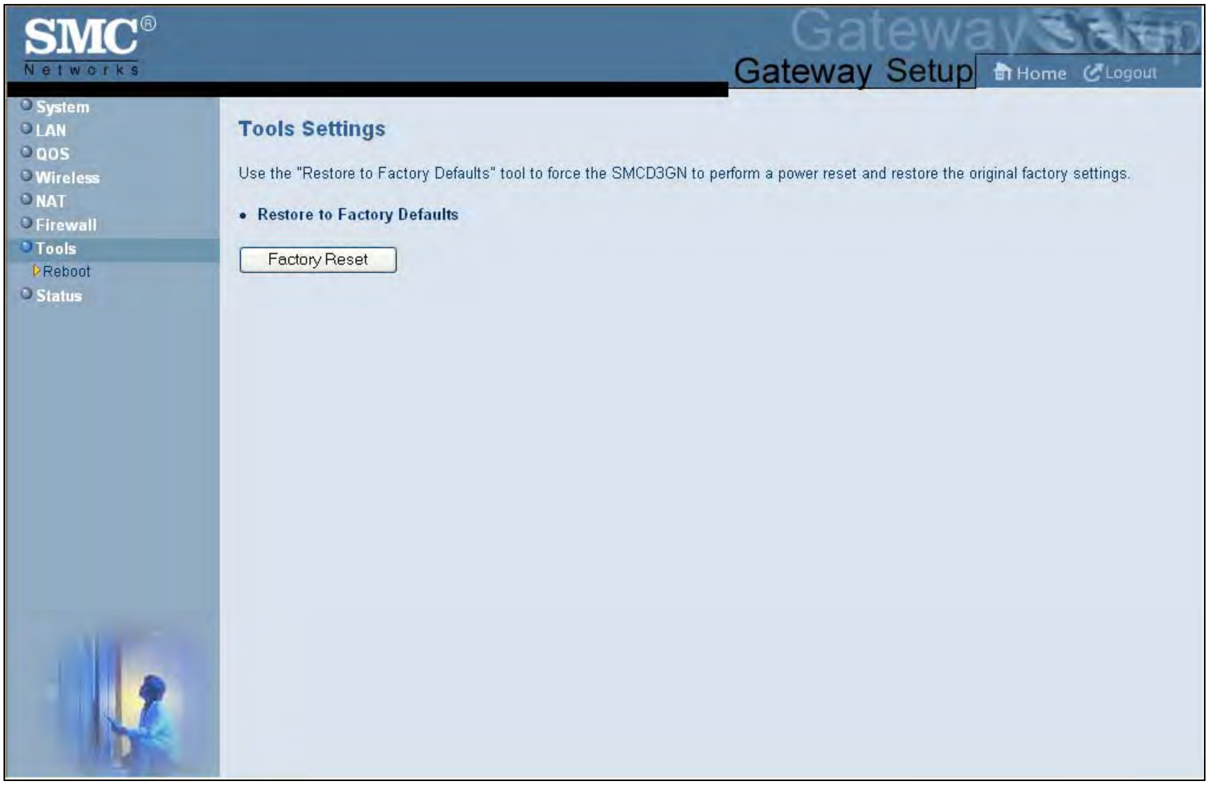
To configure DMZ settings:

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 Tools Settings Menu

Using the **Tools Settings** menu, you can reset the Gateway and restore the device's factory default settings. To access the Tools Settings menu, click **Tools** in the menu bar. Figure 54 shows an example of the menu.

Note: To reboot the Gateway and retain any customized settings, use the Reboot menu (see "Using the Reboot Menu to Reboot the Gateway" on page 99).



Tools Settings

Use the "Restore to Factory Defaults" tool to force the SMCD3GN to perform a power reset and restore the original factory settings.

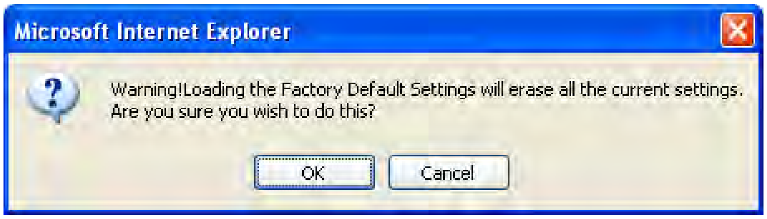
- Restore to Factory Defaults

Factory Reset

Figure 54. Tools Settings Menu

To reset the Gateway and restore its factory default settings:

1. Click **Factory Reset**. The warning message in Figure 55 appears.
2. Click **OK** to restore the Gateway's factory default settings or click **Cancel** to retain the Gateway's current settings.

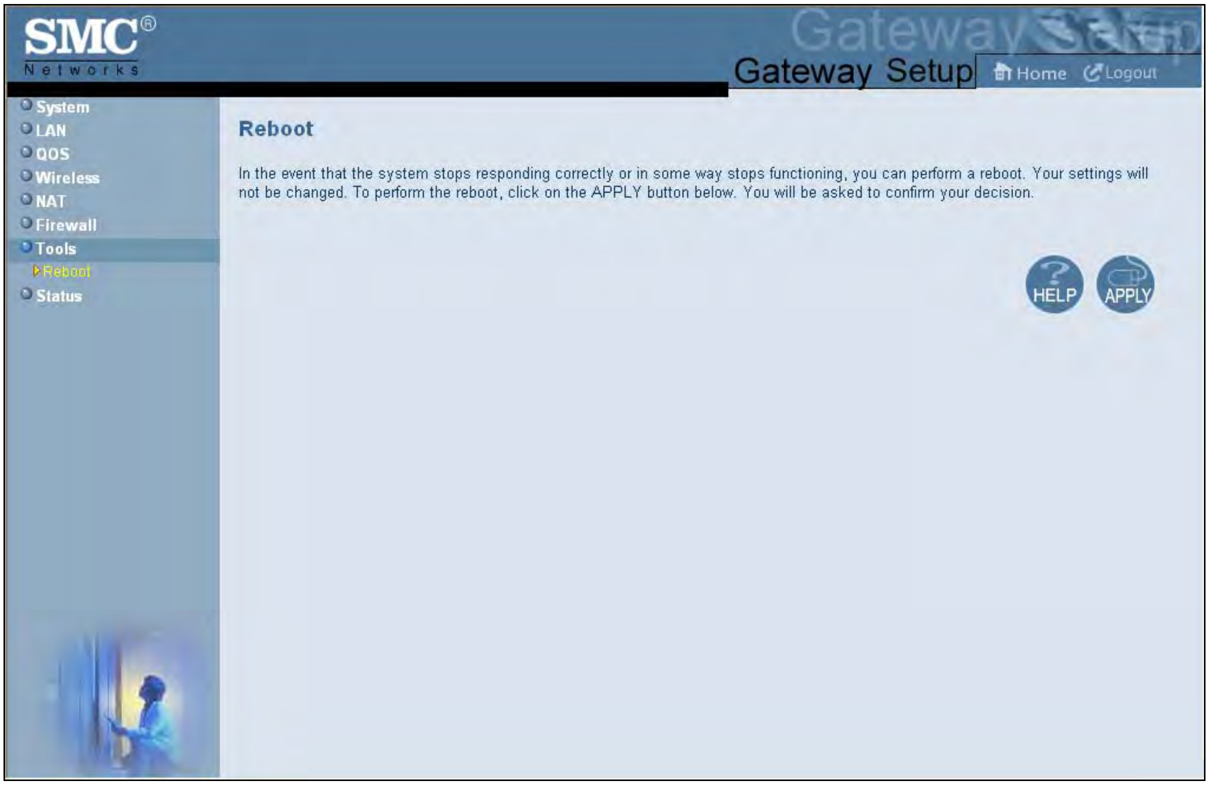


Warning!Loading the Factory Default Settings will erase all the current settings.
Are you sure you wish to do this?

Figure 55. 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 56 shows an example of the menu.



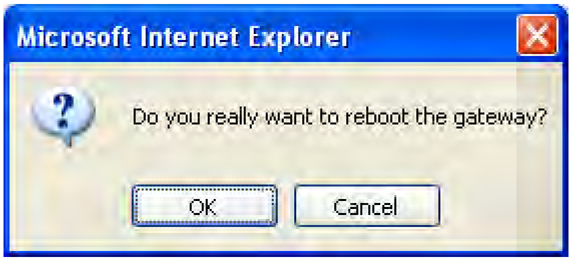
Reboot

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reboot. Your settings will not be changed. To perform the reboot, click on the APPLY button below. You will be asked to confirm your decision.

Figure 56. 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 57 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.



Microsoft Internet Explorer

Do you really want to reboot the gateway?

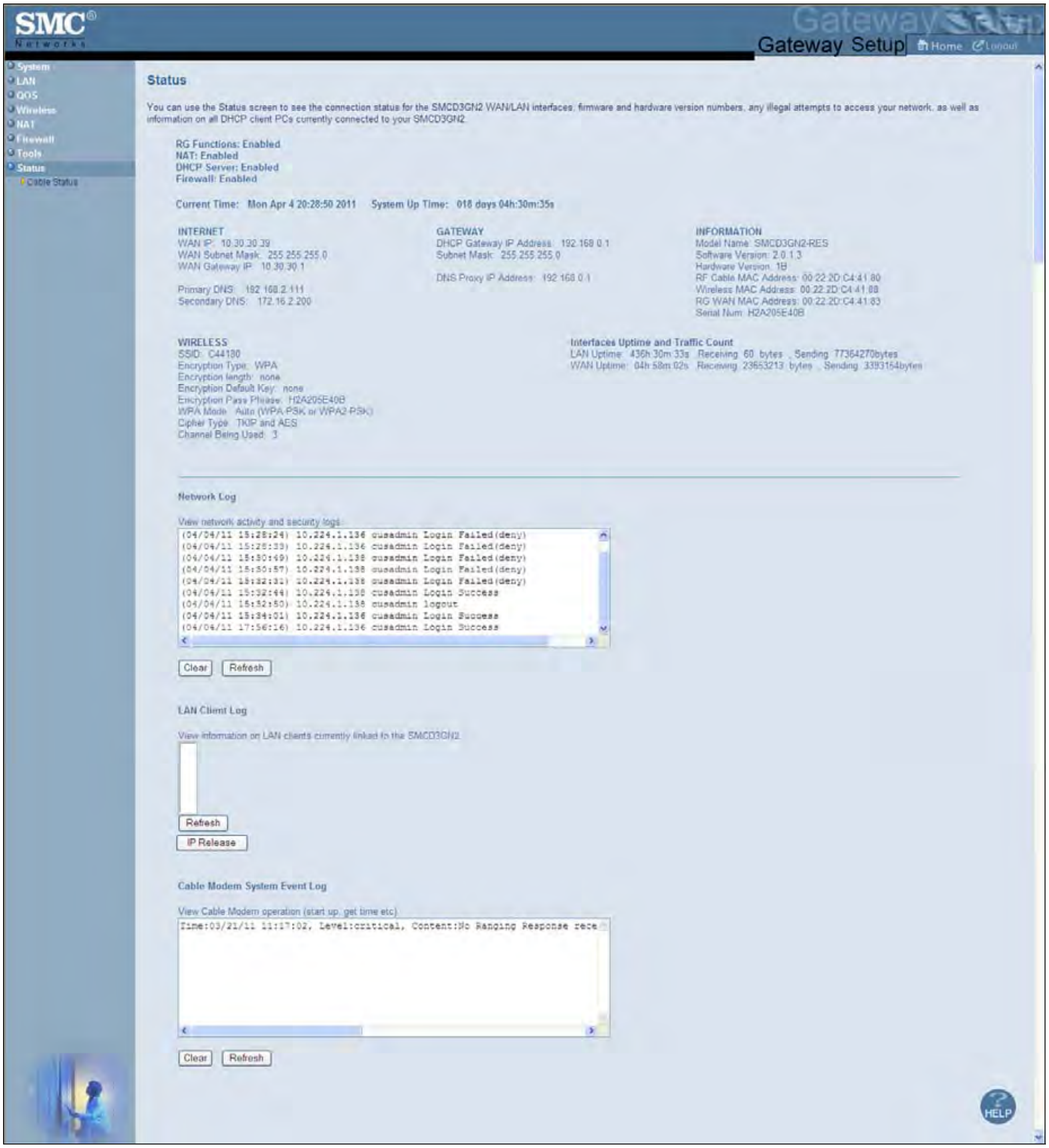
Figure 57. Precautionary Message When Rebooting the Gateway

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, LAN client, and cable modem system event logs, with buttons for clearing or refreshing the logs and releasing the IP
- 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. Figure 58 shows an example of the status information shown.



Status

You can use the Status screen to see the connection status for the SMCD3GN2 WAN/LAN 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: Mon Apr 4 20:28:50 2011 System Up Time: 018 days 04h:30m:35s

INTERNET
WAN IP: 10.30.30.39
WAN Subnet Mask: 255.255.255.0
WAN Gateway IP: 10.30.30.1

Primary DNS: 192.168.2.111
Secondary DNS: 172.16.2.200

GATEWAY
DHCP Gateway IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

DNS Proxy IP Address: 192.168.0.1

INFORMATION
Model Name: SMCD3GN2-RES
Software Version: 2.0.1.3
Hardware Version: 1B
RF Cable MAC Address: 00:22:2D:C4:41:80
Wireless MAC Address: 00:22:2D:C4:41:88
RG WAN MAC Address: 00:22:2D:C4:41:83
Serial Num: H2A205E40B

WIRELESS
SSID: C44180
Encryption Type: WPA
Encryption length: none
Encryption Default Key: none
Encryption Pass Phrase: H2A205E40B
WPA Mode: Auto (WPA-PSK or WPA2-PSK)
Cipher Type: TKIP and AES
Channel Being Used: 3

Interfaces Uptime and Traffic Count
LAN Uptime: 436h:30m:33s , Receiving: 60 bytes , Sending: 77364270bytes
WAN Uptime: 04h:58m:02s , Receiving: 23653213 bytes , Sending: 3393154bytes

Network Log

View network activity and security logs

```
(04/04/11 15:28:24) 10.224.1.136 cusadmin Login Failed(deny)
(04/04/11 15:28:33) 10.224.1.136 cusadmin Login Failed(deny)
(04/04/11 15:30:49) 10.224.1.138 cusadmin Login Failed(deny)
(04/04/11 15:30:57) 10.224.1.138 cusadmin Login Failed(deny)
(04/04/11 15:32:31) 10.224.1.138 cusadmin Login Failed(deny)
(04/04/11 15:32:44) 10.224.1.138 cusadmin Login Success
(04/04/11 15:32:50) 10.224.1.138 cusadmin logout
(04/04/11 15:34:01) 10.224.1.136 cusadmin Login Success
(04/04/11 17:56:16) 10.224.1.136 cusadmin Login Success
```

LAN Client Log

View information on LAN clients currently linked to the SMCD3GN2

Cable Modem System Event Log

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

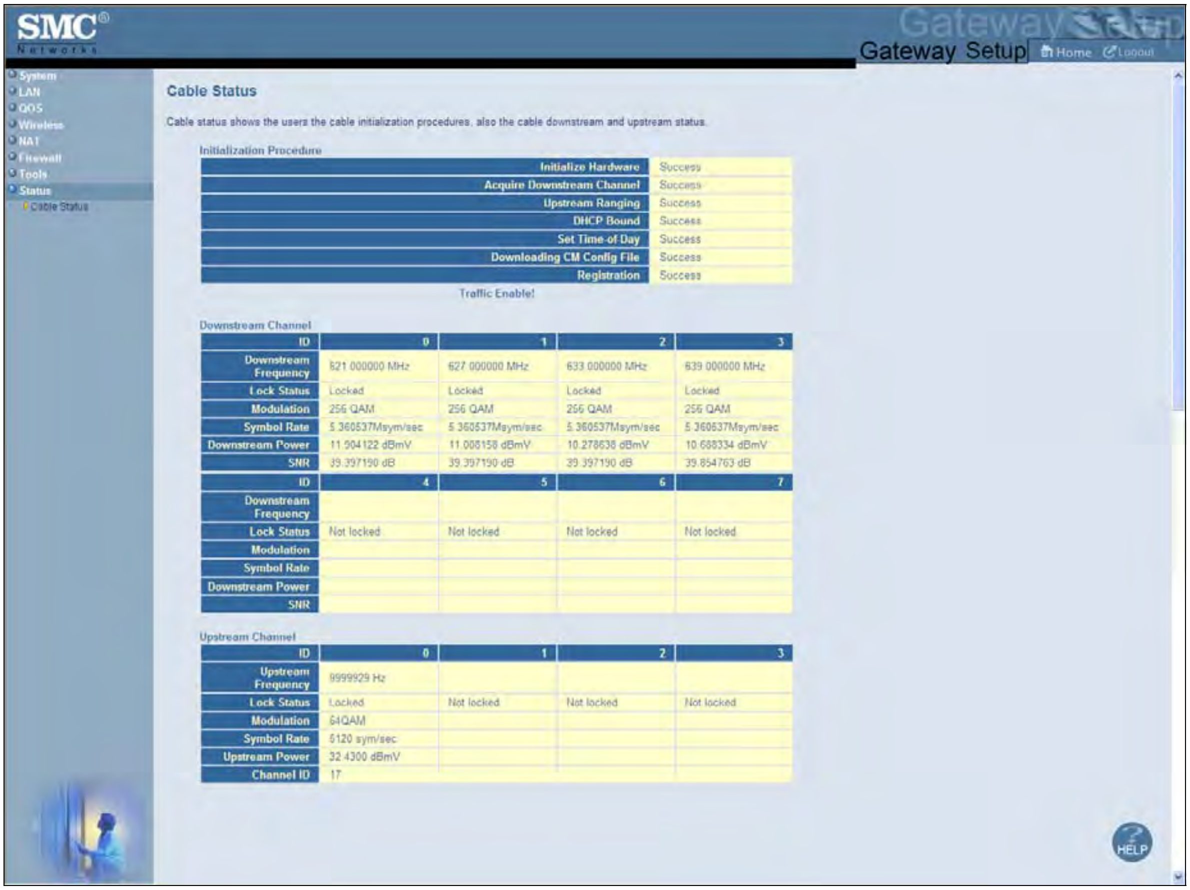
```
Time:03/21/11 11:17:02, Level:critical, Content:No Ranging Response rece
```

Figure 58. Example of Status Page

Viewing Cable Status Information

The Cable Status page is a read-only screen that shows your 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 59 shows an example of the cable status information shown.



Cable Status

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

Initialization Procedure

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	621.000000 MHz	627.000000 MHz	633.000000 MHz	639.000000 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	11.904122 dBmV	11.008158 dBmV	10.278638 dBmV	10.688334 dBmV
SNR	39.397190 dB	39.397190 dB	39.397190 dB	39.854763 dB
ID	4	5	6	7
Downstream Frequency				
Lock Status	Not locked	Not locked	Not locked	Not locked
Modulation				
Symbol Rate				
Downstream Power				
SNR				

Upstream Channel

ID	0	1	2	3
Upstream Frequency	9999929 Hz			
Lock Status	Locked	Not locked	Not locked	Not locked
Modulation	64QAM			
Symbol Rate	5120 sym/sec			
Upstream Power	32.4300 dBmV			
Channel ID	17			

Figure 59. 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 - 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.

Appendix B - Technical 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
- 1 USB 2.0 Host Port

NETWORK INTERFACES

- 4 ports 10/100/1000 MDI/MDIX auto sensing switch
- TR-68 coloring for 1 USB 2.0 Connector Type B
- Cable Interface F type female 75ohm

NETWORKS PROTOCOLS

- Application Layer: DHCP Client/Server; DNS (Proxy & Dynamic), HTTP, FTP, TFTP; SNMPv1/2, Telnet, SSH
- Transport Layer: TCP (TACACS), UDP(RADUIS)
- Network Layer: ARP, ICMP, IPv4, IPv6, IPSec, RIPv1/2
- Data Link Layer: 802.1d transparent bridging, VPN Pass-through, PAT, VLAN, Static Routing; ARP; QoS
- Physical Layer: Ethernet 10/100/1000Base T

SOFTWARE FEATURES

- Full-featured CLI provides enhanced troubleshooting and setup
- DHCP client/server
- IPV6 support coexist IPV4
- RIP v1/v2
- Downloadable configuration files allow for easy setup and installation.
- Universal Plug and Play (UPnP) enabling any UPnP devices seamlessly
- SAMBA for USB Host port connection of USB hard drives
- MIB object that executes any CLI command

- GUI/SNMPv1/2/3/CLI addition to present PHY usage (multiple channels parameters)
- VLAN Tagging (Qin Q; 802.1p/q)
- 8 SSIDs support with full wireless capabilities for each SSID
- Port Forwarding
- 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
- WAN-LAN transparent bridging
- SOAP. HTTP and HNAP
- XML Configuration

SECURITY

- Password protected configuration access
- Stateful Packet Inspection (SPI)
- Network Address Translation (NAT)
  - Many-to-one NAT
  - Many-to-many NAT
- Application Level Gateways (ALG)
- Intrusion Detection
- Denial of Service (DoS) prevention
- Trojan Horse Prevention
- Smart Tracking
- Domain & URL Filtering
- Multiple User Profiles
- Dynamic Address-User Mapping
- Web based authentication
- Comprehensive Logging
- VPN Termination Pass-Through (IPSec, PPTP, L2TP, IKE)
- DMZ

CHANNEL BONDING

- Downstream: Up to 8 channels
- Upstream: Up to 4 channels

RECEIVER

- Demodulation: 64/256QAM
- Bandwidth: 6MHz
- Max. Data Rate per Channel: 30Mbps(64QAM), 43Mbps(256QAM)
- Frequency Range: 88~1002MHz
- Signal Level: -15dbmV to + 15dbmV
- Input Impedance: 75Ω
- Input Return Loss: >6 dB over 88MHz – 1002 MHz

TRANSMITTER

- Modulation:
  - TDMA:QPSK, 8,16,32,64QAM,
  - S-CDMA: QPSK, 8,16,32,64,128QAM
- Bandwidth:
  - TDMA:200, 400, 800, 1600, 3200,6400kHz
  - S-CDMA: 1600, 3200, 6400kHz
- Max. Data Rate per Channel:
  - 320,640,1280,5120,10240kbps (QPSK)
  - 480, 960,1920,3840,7680,15360kbps (8QAM)
  - 640, 1280, 2560,5120,10240,20480kbps (16QAM)
  - 800,1600,3200,6400,12800,25600kbps (32QAM)
  - 960, 1920, 3840, 7680,15360,30720kpbs (64QAM)
  - 8960,17920,35840kbps (128QAM)
- Frequency Range: 5MHz- 42MHz
- Output Signal Level:
  - TDMA: +8 to +54dBmV (32QAM, 64QAM);+8 to +55dBmV (8QAM, 16QAM);+8 to +58dBmV (QPSK)
  - S-CDMA: +8 to +53dBmV(all modulation)

- Output Return Loss: > 6dB

WLAN

- 1T1R/1T2R/2T2R modes
- 300Mbps PHY data rate
- Supports IRRR 802.e WiFi Multimedia (WMM)
- Support 8 SSIDs
- WMM-QoS
- WPS, WPA, WEP (64/128-bit), TKIP,AES, MAC Filtering
- WPS push button for WiFi Protected Setup with PIN
- MAC address Access Control

ENVIRONMENT

- Operating Temperature: 32 °F (0°C) to 104°F (40°C)
- Operating Humidity: 10% to 90%
- Storage Temperature: -40°F (-40°C) to 140°F (80°C)

REGULATORY /STANDARD COMPLIANCE

- FCC Part 15B Class B
- UL/Cul:609650-1
- WiFi 802.11b /g/ n
- DOCSIS 3.0

DIMENSIONS (L x W x H) without packaging

- 9.84x 6.30 x 1.65 in
- 25 x 16 x 4.2 cm

WEIGHT: 508g/1.12lb

LEDs: Power, DS (Downstream), US (Upstream), Online, ETH (4), Wireless, USB

POWER SUPPLY: AC on board; AC power: 90~120V

* Actual speeds will vary based on factors including networks configuration and service tiers.

Index

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

Document number: 20131BIZ4152011