SIEMENS

SpeedStream®

Residential Family User's Guide

5450 Four-Port Router

Part No. 007-0980-001

Siemens Subscriber Networks – End User Software License and Limited Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY SIEMENS SUBSCRIBER NETWORKS (SIEMENS) CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS OF THE FOLLOWING SOFTWARE LICENSE AND LIMITED WARRANTY. IF YOU DO NOT ACCEPT THESE TERMS, PLEASE RETURN THE HARDWARE AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE STORE OR OTHER VENDOR FROM WHICH YOU PURCHASED IT FOR A FULL REFUND OF THE PURCHASE PRICE.

The following describes your license to use the software (the "Software") that has been provided with your SIEMENS DSL customer premises equipment ("Hardware") and the limited warranty that SIEMENS provides on its Software and Hardware.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. Accordingly, while you own the media (CD ROM or floppy disk) on which the Software is recorded, SIEMENS retains ownership of the Software itself.

1. **Grant of License**. You may install and use one (and only one) copy of the Software on the computer on which the Hardware is being installed. If the Hardware is being installed on a network, you may install the Software on the network server or other server-side device on which the Hardware is being installed and onto the client-side devices connected to the network as necessary.

2. **Restrictions**. The license granted is a limited license. You may NOT:

sublicense, assign, or distribute copies of the Software to others; decompile, reverse engineer, disassemble or otherwise reduce the Software or any part thereof to a human perceivable form; modify, adapt, translate or create derivative works based upon the Software or any part thereof; or rent, lease, loan or otherwise operate for profit the Software.

3. **Transfer**. You may transfer the Software only where you are also transferring the Hardware. In such cases, you must remove all copies of the Software from any devices onto which you have installed it, and must ensure that the party to whom you transfer the Hardware receives this License Agreement and Limited Warranty.

4. **Upgrades Covered**. This license covers the Software originally provided to you with the Hardware, and any additional software that you may receive from SIEMENS, whether delivered via tangible media (CD ROM or floppy disk), down loaded from SIEMENS or delivered through customer support. Any such additional software shall be considered "Software" for all purposes under this License.

5. **Export Law Assurance**. You acknowledge that the Software may be subject to export control laws and regulations of the U.S.A. You confirm that you will not export or re-export the Software to any countries that are subject to export restrictions.

6. **No Other Rights Granted**. Other than the limited license expressly granted herein, no license, whether express or implied, by estoppel or otherwise, is granted to any copyright, patent, trademark, trade secret, or other proprietary rights of SIEMENS.

7. **Termination**. Without limiting SIEMENS's other rights, SIEMENS may terminate this license if you fail to comply with any of these provisions. Upon termination, you must destroy the Software and all copies thereof.

Limited Warranty

The following limited warranties provided by SIEMENS extend to the original end user of the Hardware/licensee of the Software and are not assignable or transferable to any subsequent purchaser/licensee.

1. **Hardware**. SIEMENS warrants that the Hardware will be free from defects in materials and workmanship and will perform substantially in compliance with the user documentation relating to the Hardware for a period of one year from the date the original end user received the Hardware.

2. **Software**. SIEMENS warrants that the Software will perform substantially in compliance with the end user documentation provided with the Hardware and Software for a period of ninety days from the date the original end user received the Hardware and Software. The end user is responsible for the selection of hardware and software used in the end user's systems. Given the wide range of third-party hardware and applications, SIEMENS does not warrant the compatibility or uninterrupted or error free operation of our Software with the end user's system.

3. **Exclusive Remedy**. Your exclusive remedy and SIEMENS's exclusive obligation for breach of this limited warranty is, in SIEMENS's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty (30) days, which ever is longer.

4. **Warranty Procedures**. If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:

A. Prior to returning a product under this warranty, the end user must first call SIEMENS at (888) 286-9375, or send an email to SIEMENS at support@efficient.com to obtain a return materials authorization (RMA) number. RMAs are issued between 8:00 a.m. and 5:00 p.m. Central Time, excluding weekends and holidays. The end user must provide the serial number(s) of the products in order to obtain an RMA.

B. After receiving an RMA, the end user shall ship the product, including power supplies and cable, where applicable, freight or postage prepaid and insured, to SIEMENS at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from SIEMENS, the end user shall provide SIEMENS with any missing items or, at SIEMENS's sole option, SIEMENS will either (a) replace missing items and charge the end user or (b) return the product to the end user freight collect. The end user shall include a return address, daytime telephone number and/or fax. The RMA number must be clearly marked on the outside of the package.

C. Returned Products will be tested upon receipt by SIEMENS. Products that pass all functional tests will be returned to the end user.

D. SIEMENS will return the repaired or replacement Product to the end user at the address provided by the end user at SIEMENS's expense. For Products shipped within the United States of America, SIEMENS will use reasonable efforts to ensure delivery within five (5) business days from the date received by SIEMENS. Expedited service is available at additional cost to the end user.

E. Upon request from SIEMENS, the end user must prove the date of the original purchase of the product by a dated bill of sale or dated itemized receipt.

5.**Limitations**.

The end user shall have no coverage or benefits under this limited warranty if the product has been subject to abnormal use, abnormal conditions, improper storage, exposure to moisture or dampness, unauthorized modifications, unauthorized repair, misuse, neglect, abuse, accident, alteration, improper installation, or other acts which are not the fault of SIEMENS, including acts of nature and damage caused by shipping.

SIEMENS will not honor, and will consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with; (2) the Product's case has been opened; or (3) there has been any attempted or actual repair or modification of the Product by anyone other than an SIEMENS authorized service provider.

The limited warranty does not cover defects in appearance, cosmetic, decorative or structural items, including framing, and any non-operative parts.

SIEMENS's limit of liability under the limited warranty shall be the actual cash value of the product at the time the end user returns the product for repair, determined by the price paid by the end user for the product less a reasonable amount for usage. SIEMENS shall not be liable for any other losses or damages.

The end user will be billed for any parts or labor charges not covered by this limited warranty. The end user will be responsible for any expenses related to reinstallation of the product.

THIS LIMITED WARRANTY IS THE ONLY WARRANTY SIEMENS MAKES FOR THE PRODUCT AND SOFTWARE. TO THE EXTENT ALLOWED BY LAW, NO OTHER WARRANTY APPLIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. **Out of Warranty Repair**. Out of warranty repair is available for fixed fee. Please contact SIEMENS at the numbers provided above to determine the current out of warranty repair rate. End users seeking out of warranty repair should contact SIEMENS as described above to obtain an RMA and to arrange for payment of the repair charge. All shipping charges will be billed to the end user.

General Provisions

The following general provisions apply to the foregoing Software License and Limited Warranty:

1. **No Modification**. The foregoing limited warranty is the end user's sole and exclusive remedy and is in lieu of all other warranties, express or implied. No oral or written information or advice given by SIEMENS or its dealers, distributors, employees or agents shall in any way extend, modify or add to the foregoing Software License and Limited Warranty. This Software License and Limited Warranty constitutes the entire agreement between SIEMENS and the end user, and supersedes all prior and contemporaneous representation, agreements or understandings, oral or written. This Software License and Limited Warranty may not be changed or amended except by a written instrument executed by a duly authorized officer of SIEMENS.

SIEMENS neither assumes nor authorizes any authorized service center or any other person or entity to assume for it any other obligation or liability beyond that which is expressly provided for in this limited warranty including the provider or seller of any extended warranty or service agreement.

The limited warranty period for SIEMENS supplied attachments and accessories is specifically defined within their own warranty cards and packaging.

2. **EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES**. TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL SIEMENS BE LIABLE, WHETHER UNDER CONTRACT, WARRANTY, TORT OR ANY OTHER THEORY OF LAW FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, PERSONAL INJURY, LOSS OR IMPAIRMENT OF DATA OR BUSINESS INFORMATION, EVEN IF SIEMENS HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. SIEMENS'S LIABILITY TO YOU (IF ANY) FOR ACTUAL DIRECT DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION, WILL BE LIMITED TO, AND SHALL NOT EXCEED, THE AMOUNT PAID FOR THE HARDWARE/SOFTWARE.

3. **General**. This Software License and Limited Warranty will be covered by and construed in accordance with the laws of the State of Texas, United States (excluding conflicts of laws rules), and shall inure to the benefit of SIEMENS and its successor, assignees and legal representatives. If any provision of this Software License and Limited Warranty is held by a court of competent jurisdiction to be invalid or unenforceable to any extent under applicable law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this Software License and Limited Warranty will remain in full force and effect. Any notices or other communications to be sent to SIEMENS must be mailed by certified mail to the following address:

Siemens Subscriber Networks

4849 Alpha Road

Dallas, TX 75244

U.S.A.

Attn: Customer Service

Contents

Chapter 1

Introduction

This chapter provides an overview of the router's features and capabilities.

Congratulations on the purchase of your new SpeedStream 5450 four-port router. The 5450 four-port router is a multi-function device providing the following services:

- Built-in DSL Modem that provides shared Internet access for multiple users.
- Four-port 10/100 Ethernet Switch for 10Base-T or 100Base-T connections.
- Custom Controls that allow you to configure the router to best meet your specific security and Internet-sharing needs.

Features of the 5450 Router

The 5450 router incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Network (LAN) Features

- **Four-Port 10/100 Ethernet Switch**
  The router incorporates a four-port 10/100 Ethernet switch, making it easy to create or extend your network. Optionally, you can configure the fourth port as a WAN port for connection to another broadband device.
- **DHCP Server Support**
  Dynamic Host Configuration Protocol (DHCP) provides a dynamic, "upon request," IP address to computers and other networked devices. Your router can act as a DHCP Server for devices on your local network.
- **Network Status and Statistics**
  Using these diagnostic tools, you can easily monitor the status of each network connection and evaluate network performance.

Security Features

- **Password Protected Configuration**
  Password protection is provided to prevent unauthorized users from modifying the router's configuration data and settings.
- **NAT Protection**
  An intrinsic side affect of NAT (Network Address Translation) technology is that by allowing all your network users to share a single IP address, the location and even the existence of each computer is hidden. From the external viewpoint, there is no network, only a single device.
- **Stateful Inspection Firewall**
  All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Attack Protection System**
  Attacks can flood your Internet connection with invalid data packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The router incorporates protection against these types of attacks as well as other common hacker attacks.

Configuration & Management

- **Easy Setup**
  Use your Web browser for quick and easy configuration.
- **UPnP Support**
  Universal Plug and Play (UPnP) allows automatic discovery and configuration of the SpeedStream Router. UPnP is supported by Windows Me, XP, or later, operating systems.

Advanced Router Functions

- **DMZ**
  One computer on your local network can be configured to allow unrestricted two-way communication with servers or individual users on the Internet. This provides the ability to run programs that are incompatible with firewalls.
- **Firewall "Snooze"**
  Temporarily disable firewall protection to limit interference with games and other applications incompatible with firewalls.
- **Content Filter**
  Use the Content Filter to block individual user access to undesirable Web sites. Content filtering can be defined differently for each user.
- **Time of Day Use Restrictions**
  Limit the time of day during which individual users have access to the Internet. Time limitations can be defined differently for each user.

Minimum System Requirements

At a minimum, your computer must be equipped with the following to successfully install the router. Your Internet Service Provider may have additional requirements for use of their service.

- A network interface card (NIC) that supports 10/100 Ethernet
- Operating system that supports TCP/IP
- Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later

Package Contents

If any of the items are damaged or missing, please contact your Internet Service Provider for assistance.

- Model 5450 Router
- Power adapter
- CAT-5 Ethernet cable for LAN connections
- RJ11 cable for DSL connection
- Quick Start Guide
- CD-ROM containing user documentation

Physical Details

Familiarize yourself with the router before installing.

Front Panel LEDs

The front panel contains the following LEDs:

Power	**Off**	Power is off.
	Green	Power is on.
	Flashing	Flash write in progress.
	Red	The Power LED briefly shows red during power-up. This indicates that the SpeedStream is conducting the POST (Power-On Self Test) that is run each time the SpeedStream is powered on. Post error occurred if persistent.
DSL Port	**On**	DSL connection is active.
	Off	No active DSL connection.
Ethernet	**On**	One or more Ethernet LAN ports are active.
	Off	No active Ethernet LAN port connection.
Activity	**Off**	No data being transmitted or received.
	Flashing	Data is being transmitted or received.
Internet	**Off**	No power or bridge mode or no DSL link.
	Green	DLS link is up + WAN interface + WAN interface has IP address.

Example Front Panel

Rear Panel

DSL Port (RJ11)	Connect the RJ11 DSL cable (looks like a telephone cord) here to use your DSL connection through an existing phone line.
Four 10/100 Ethernet Ports	Connect the RJ45 Ethernet cable here to connect your computers, hubs, or switches to the router. You can configure port #4 as either a LAN or WAN port.
Power Adapter Port	Connect the supplied power adapter provided with the router here.

Example Rear Panel

Power Button	Push this button to power the router on and off.

General Safety Guidelines

When using the 5450 router, observe the following safety guidelines:

- Never install telephone wiring during a storm.
- Avoid using a telephone during an electrical storm. Lightening increases the risk of electrical shock.
- Do not install telephone jacks in wet locations and never use the product near water.
- Do not exceed the maximum power load ratings for the product; otherwise, you risk dangerous overloading of the power circuit.

Chapter 2

Installation

This chapter covers the physical installation of the router.

Minimum System Requirements

- DSL service and an Internet access account from an Internet Service Provider (ISP).
- Network cables for each device you intend to connect to the router.
- TCP/IP network protocol must be installed on all computers.

Note: Your configuration may vary slightly from the instructions and illustrations in this chapter. Refer to your service provider's documentation, or contact them with questions regarding your specific configuration.

Hardware Installation

You may position the router at any convenient location in your office or home. No special wiring or cooling requirements are needed; however, you should comply with the safety guidelines specified in the General Safety Guidelines section.

Basic Installation Procedure

1. Install line filters if necessary.
2. Connect the cables.
3. Configure network settings on your computer.
4. Configure the Router via the Web-based management interface.
5. Reboot the computer if prompted. Whenever you are required to reboot the router, allow five seconds between turning off the unit and powering it back on.

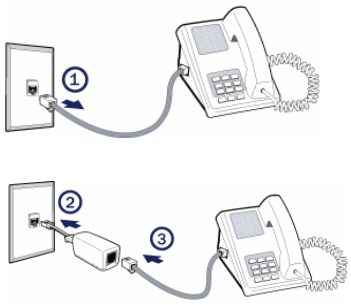
Installing Line Filters

Because DSL shares your telephone line, you may need to separate the two signals so they do not interfere with each other. A line filter (may be included with some models) prevents DSL traffic from disrupting the voice signal on the telephone line, and vice versa. Follow the procedures below to install line filters on any device (telephones, fax machines, caller ID boxes) that shares the same telephone line with your DSL. (Note, this section may not apply to you. Consult your provider if you are unsure.)

There are two types of filters to connect between the telephone and the wall plate:

- *In-line filter:* For use with standard desktop telephones.
- *Wall-mount filter*: For use with wall-mounted telephones.

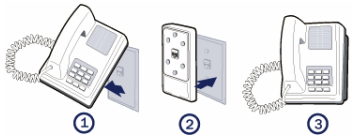
DSL performance may be significantly degraded if the line filters are not installed in the correct direction, as illustrated below.



In-Line Filter

For each device sharing the same telephone line:

1. Unplug the device's cord from the telephone jack.
2. Plug the filter into the telephone jack.
3. Plug the telephone cord (or other device cord) into the filter.



Wall-Mount Filter

For a wall-mounted telephone, install a wall mount filter:

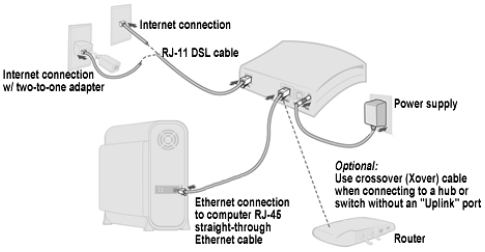
1. Remove the telephone.
2. Connect the wall mount filter to the wall plate.
3. Reconnect the telephone.

Connecting Cables to Ethernet

The router provides four ports for Ethernet connection to your primary computer. Follow the step-by-step instructions below to connect your computer to the router.

To connect the router via the Ethernet interface, your computer must have an Ethernet adapter (also called a network interface card, or "NIC") installed.

If your computer does not have this adapter, install it before proceeding further. Refer to your Ethernet adapter documentation for complete installation instructions.



1. Connect the Ethernet cable(s)

1) With your computer powered off, connect the Ethernet cable to an Ethernet port (1-4) on the router.

2) Connect the other end of the Ethernet cable to the Ethernet port on your computer.

3) If desired, use standard 10/100 CAT5 Ethernet cables to connect additional computers to the remaining Ethernet ports on the router.

2. Connect the DSL cable

1) Connect the DSL cable (resembles a telephone cord) to the DSL port on the router.

2) Plug the other end of the DSL cable into the phone jack.

3. Connect the power

1) Connect the power adapter to the rear of the router.

2) Plug the power adapter into the electrical wall outlet.

3) Flip the power switch to power on the router.

4) Power on all connected computers.

4. Check the LEDs

1) For each active Ethernet connection, the LAN Link LED for the corresponding port number should be lit.

2) The DSL and Power LEDs should be lit. (For more information, refer to the LEDs section in Chapter 1.)

When using the Ethernet installation method, you do not have to install any software. Refer to your Internet Service Provider's instructions for installing their software and/or connecting to the Internet. You can now configure the TCP/IP settings as detailed in the next chapter.

Chapter 3

Operating System Configuration

This chapter explains how to configure each computer on your network to work with the router.

To access the Internet through the router, the TCP/IP protocol must be installed on your computer. If TCP/IP is not already installed on your computer, install it. Refer to your system documentation or online help for instructions.

- Once TCP/IP is installed on your computer, you should check the TCP/IP protocol settings to make sure they are correct for use with the router.
- Once TCP/IP configuration is verified, the next step is to configure your computer to use the router for internet access so your PC will use the router when connecting to the Internet and not Dial-Up Networking.

The operating system on each computer in your network must have the TCP/IP network settings and Internet access settings configured.

Check TCP/IP Protocol Settings

Because the router uses the TCP/IP network protocol for all functions, it is essential that the TCP/IP protocol be installed and configured properly.

The default network settings for the router are:

IP Address:	192.168.254.254
Subnet Mask:	255.255.255.0

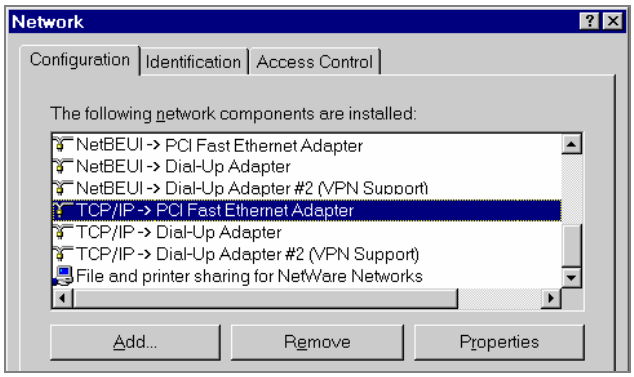
By default, the router will act as a DHCP server, automatically providing a suitable IP address and related information to each computer when the computer boots up. For all non-server versions of Windows, the TCP/IP setting defaults to act as a DHCP client. If using the default router settings and the default Windows TCP/IP settings, you do not need to make any changes.

The instructions to check TCP/IP protocol settings differ between operating system. Check the settings using the instructions for your operating system:

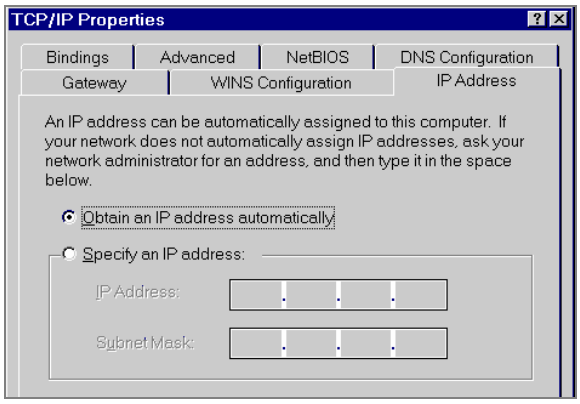
- Windows 9x/ME
- Windows 2000
- Windows XP
- MAC OS 8.6 through 9.x
- MAC OSX

Checking TCP/IP Settings (Windows 9x/ME)

1. Select **Start>Control Panel >Network**. This displays the **Configuration** tab on the "Network" window.



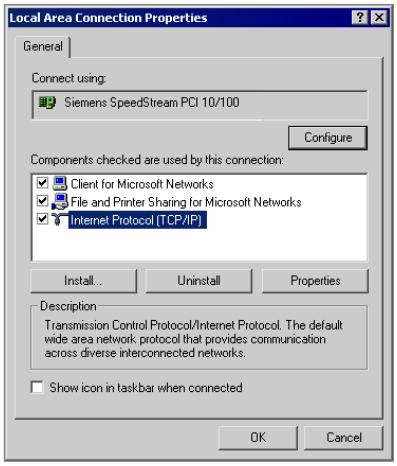
2. Select the TCP/IP protocol for your network card.
3. Click **Properties**. This displays the "TCP/IP Properties" window.



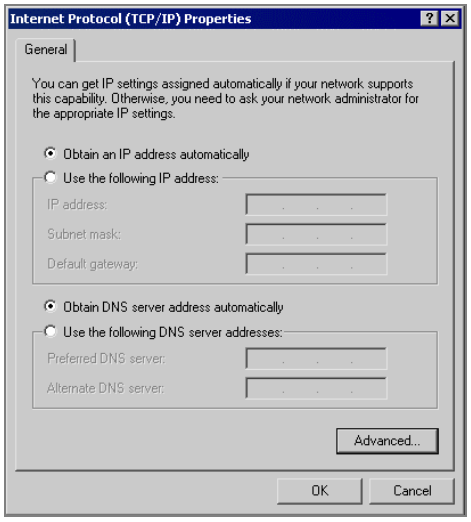
4. Click the **IP Address** tab.
5. Ensure that the **Obtain an IP address automatically** option is selected. This is the default Windows settings.
6. Close this window.
7. Restart your computer to ensure it obtains an IP address from the router.
8. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (Windows 2000)

1. On the Windows taskbar click **Start>Settings>Control Panel**. This displays the "Control Panel" window.
2. Double-click **Network and Dial-up Connections**. This displays the "Network and Dial-up Connections" window.
3. Right-click **Local Area Connection** and select Properties. This displays the "Local Area Connections Properties" window.



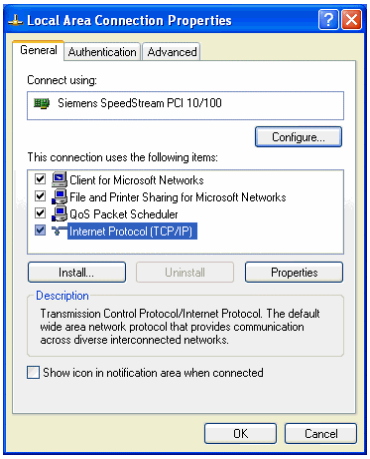
4. Select the TCP/IP protocol for your network card.
5. Click **Properties**. This displays the "Internet Protocol (TCP/IP) Properties" window.

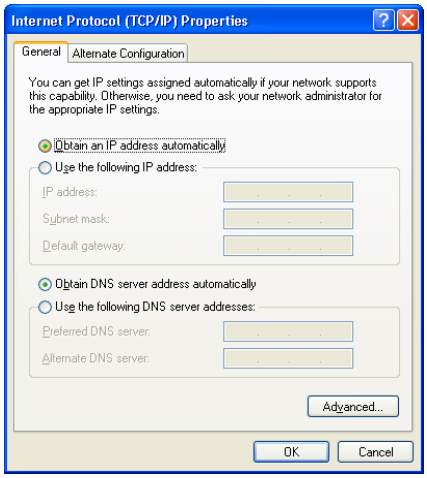


6. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** options. Exit back to the Control Panel.
7. Restart your computer to ensure it obtains an IP address from the router.
8. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (Windows XP)

1. On the Windows taskbar click **Start>Control Panel**. This displays the "Control Panel" window.
2. Double-click the **Network Connection** icon. This displays the "Network Connections" window.
3. Right-click **Local Area Connection**, then click **Properties**. This displays the "Local Area Connection Properties" window.
4. Select the TCP/IP protocol for your network card.
5. Click **Properties**. This displays the "Internet Protocol (TCP/IP) Properties" window.

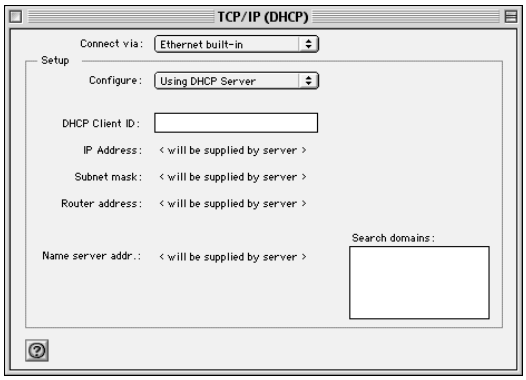




6. Ensure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
7. Exit back to the Control Panel.
8. Restart the computer to ensure it obtains an IP address from the router.
9. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (MAC OS 8.6 through 9.x)

1. Select **Apple >Control Panel >TCP/IP**. This displays the "TCP/IP" window.



2. Select **Ethernet** or **Ethernet built-in** from the **Connect via** drop-down menu.
3. Select **Using DHCP Server** from the **Configure** drop-down menu.
4. Close the "TCP/IP window" and click **Save**.
5. Reboot when configuration is saved. Once rebooted, the computer will pull an IP address from the DHCP server on the router.
6. Configure the router using the procedure described in the next chapter.

Checking TCP/IP Settings (MAC OSX)

1. Click **Apple -> System Preferences**. This displays the "System Preferences" window.

2. Double-click the **Network** icon under the **Internet & Network** section. This displays the "Network" window.

3. Select **Built-in Ethernet** from the **Show** drop-down menu:
4. Select **Using DHCP Server** from the **Configure IPv4** drop-down menu.
5. Click **Apply Now** and quit window.
6. Configure the router using the procedure described in the next chapter.

Internet Access Configuration

Windows users must configure their computers to use the router for Internet access. Ensure that the router is installed correctly and the DSL line is functional. Then follow the appropriate procedure below to configure your Web browser to access the Internet via the LAN, rather than by a dial-up connection.

For Windows 9x/2000

1. Select **Start>Settings>Control Panel** to display the Control Panel.
2. Double-click the **Internet Options** icon. This displays the "Internet Properties" window.
3. Click the **Connections** tab.
4. Click **Setup**.
5. Click **I want to set up my Internet connection manually**, or **I want to connect through a local area network (LAN)**, then click **Next**. This displays the "Internet Connection Wizard" window.
6. Click **I connect through a local area network (LAN)**, then click **Next**. This displays the "Local Area Network Internet Configuration" window.
7. Ensure all the boxes are deselected, then click **Next**. This displays the "Set Up your Internet Mail Account" window.
8. Click **No**, then click **Next**. This displays the "Completing the Internet Connection Wizard" window.
9. Click **Finish** to close the Internet Connection Wizard. Setup is now complete.
10. Configure the router using the procedure described in the next chapter.

For Windows XP

1. Select **Start>Control Panel**.
2. Double-click the **Internet Options** icon. This displays the "Internet Options" window.
3. Click the **Connections** tab.
4. Click **Setup**. This starts the **New Connection Wizard**.
5. Click **Next**.
6. Select **Connect to the Internet**, then click **Next**.
7. Select **Setup my connection manually**, then click **Next**.
8. Select **Connect using a broadband connection that is always on**, then click **Next**.
9. Click **Finish**.
10. Configure the router using the procedure described in the next chapter.

Chapter 4

SpeedStream Router Setup

This chapter describes how to connect to and setup your router configuration.

This chapter describes the steps to set up the router configuration using the Setup Wizard. Other configuration may also be required on the router, depending on which features and functions of the router you wish to use. Use the table below to locate detailed instructions for the required functions.

To do this	Refer to
Configure users and devices on the router.	Chapter 5, Configuring Users and Devices
Configure router advance options such as ISP connections, networking options, and security.	Chapter 6, Configuring Advanced Features
Monitor the health of the router.	Chapter 7, Monitoring Router Health

Before Configuring the Router

Before attempting to configure the router, please ensure that:

- Your computer can establish a physical connection to the router. The computer and the router must be directly connected using Ethernet ports on the router.
- The router is installed correctly and powered on.
- The TCP/IP protocol is installed on all computers on your network. (If you need to install TCP/IP, refer to your system documentation or Windows Help.)
- The network settings on each computer are correctly configured.

From this point on, you will perform all configuration of the router from your computer using the Web browser-based setup program.

Connecting to the Router

You can connect to the Gateway using UPnP (if it is enabled on your computer) or through the Web browser.

Using UPnP (Windows XP and Me)

If your Windows operating system supports UPnP (Universal Plug and Play) and UPnP is enabled, an icon for the Gateway appears in the system tray near the time display, notifying you that a new network device has been found and offering to create a new desktop shortcut to the newly discovered device.

Note: You must be logged in as administrator or be a user with administrative rights for Windows 2000 and XP to be able to install the drivers for the Gateway.

4. Unless you intend to change the IP address of the Gateway, you can accept the desktop shortcut. Whether you accept the desktop shortcut or not, you can find UPnP devices in **My Network Places** (previously called Network Neighborhood).
5. Double-click the icon for the Gateway (either on the desktop or in **My Network Places**) to access the Gateway's configuration program.
6. Refer to the Setup Wizard section for details of the initial configuration process.

Using your Web Browser

The SpeedStream Gateway contains an HTTP server that allows you to connect to the Gateway and configure it from your Web browser (Microsoft Internet Explorer or Netscape Navigator, versions 5.0 or later).

To establish a connection from your computer to the Gateway:

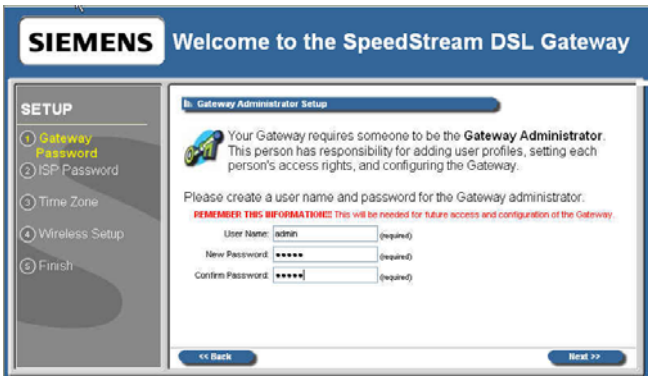
1. After installing the router, start your computer. If your computer is already running, reboot it.
2. Open your Internet Explorer or Netscape Navigator Web browser.
3. In the **Address** bar, type **http://speedstream** and press the **Enter** key. This displays the "Setup" window.
4. Refer to the Setup Wizard section for details of the initial configuration process.

Router Setup Wizard

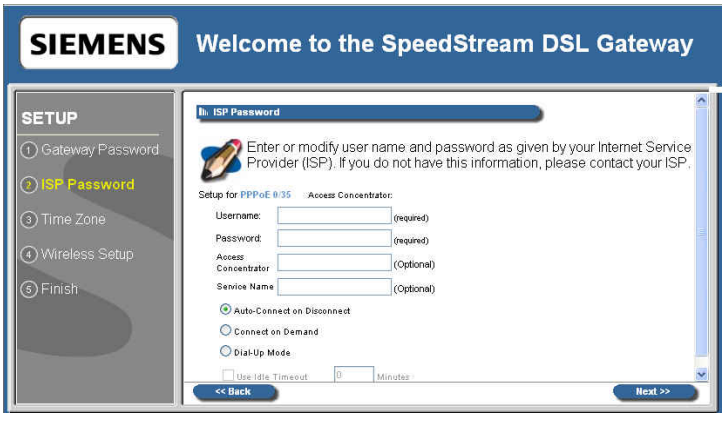
The first time you connect to the router, the Setup Wizard runs automatically. (The Setup Wizard also runs if the router's default settings are restored.) Proceed through the entire Setup Wizard to ensure accuracy of the installation.

You will need to know the username and password for Internet service provided by your ISP. Check the information supplied by your ISP for details.

1. The first window of the Setup Wizard is the "**Welcome"** window. Click **Next** on the "Welcome" window to begin setup. This displays the "Gateway Administrator Setup" window.

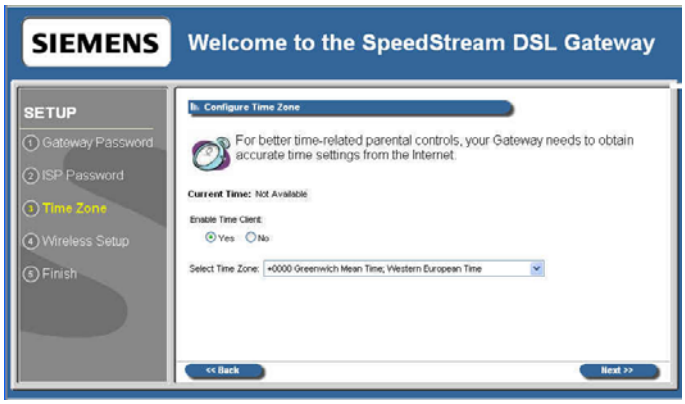


2. An administrator account has access rights to the router configuration windows. Optionally, change the "admin" user name to a different administrative name by typing the new administrative name in **User Name**. If you wish, simply leave the "admin" user name in **User Name**.
3. Type a password in **New Password** and re-type it in **Confirm Password**.
4. Click **Next**. This displays the "ISP Password" window.



5. Enter information as specified by your ISP.

6. Click **Next**. This displays the "Configure Time Zone" window.



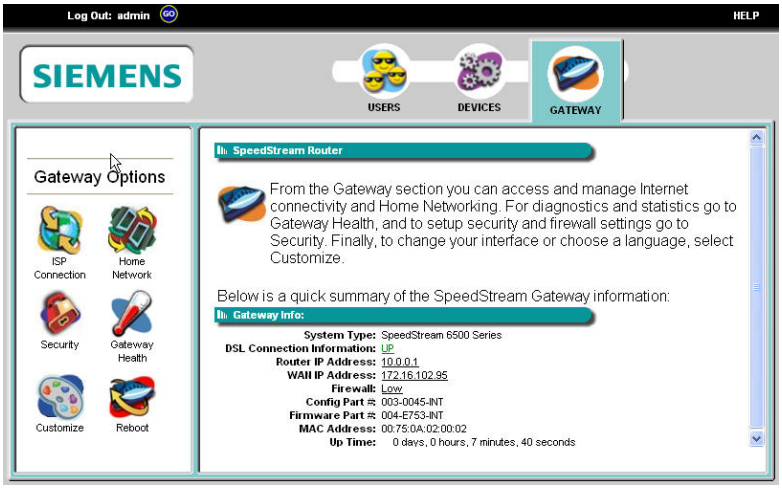
Optionally set the time zone of the area of the world in which you live on the "Configure Time Zone" window. This option must be enabled to define time of day restrictions for users.

7. To set the time zone, select the **Yes** option for **Enable Time Client**.
8. Select your time zone from the **Select Time Zone** drop-down menu, then click **Next**. This displays the "Finish" window.
9. On the "Finish" window, click **Finish**. This displays the "What do I do now?" window. From this window you may click one of the following:

   - **Surf Now**
     Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the router's configuration interface at anytime should you choose to further configure the router.
   - **Continue**
     Displays the "Home" window where you can create usage profiles/rules for different users, change the level or type of security used on the router, or define/configure your network to be managed by the router.

Home Window

After finishing the Setup Wizard and clicking **Configure**, the Home window appears. This window also appears from now on when connecting to the router.



After finishing the Setup Wizard and clicking **Configure**, the "Home" window is displayed. This window is also displayed from now on when connecting to the router. At the top of this window is the MenuBar that contains the login/logout drop-down menu and Help menu.

Below the Menu Bar is a Toolbar that contains a set of buttons to access various configuration and information windows on the router: Users, Devices, Gateway. In the left navigation pane there are configuration options for the selected Toolbar button. These options differ depending on how a user is logged into the system. An administrator has full configuration rights (shown above), while a user has limited configuration rights. To Home window displays basic networking attributes of the modem including IP address and default router specifications.

Pay special attention to **Login** in the top left-hand corner of the window to ensure that you are logged in to access all available features.

Menu Bar

The only two items on the menu bar are the **Log in** drop-down menu and the **Help** menu option. The **Log In** drop-down menu is used to log in a user or administrator. The **Help** option is used to display a help system for the router.

Toolbar

The router has three primary toolbar buttons: Users, Devices, and Gateway. The options for all the toolbar buttons differ depending on the user login. The administrator has the most authority with all options enabled, while the user has limited options based on the user profile for the login. Please see the table below for more information.

	Users Button: This button provides access to user profiles and the User Profile Wizard. This wizard guides you through the steps required to set up and configure individual user profiles. Once configured, you can use this option to view a user's profile.
	Devices Button: This button provides Access to network devices connected to the router. You can use this option to view shared files and resources on other computers if they are shared via Windows File Sharing.
	Gateway Button: This button provides access to all router configuration options, security settings, router health monitoring, and Internet connection and network details. The settings available may differ depending upon your service provider.

Logging into the Router

There are two types of primary users that log into the router: administrators and users. Administrators have rights to all of the configuration options available on the router. Users have limited access based on what is set by the administrator for each user.

To log on to the router:

1. Select a user from the **Log In** drop-down menu in the upper-left corner of the "Home" window.
2. Select a user from the **Username** drop-down menu.
3. Type the user password in **Password**.
4. Click **Go**. This displays the "Home" window.

Logging out of the Router

To log out of the router:

1. Click **GO** next to **Log Out**. The system responds by displaying the "Home" window.

Chapter 5

Configuring Users and Devices

This chapter explains how to configure users and devices on the router.

This chapter contains details for configuring users and devices on the router. This chapter is organized into two parts corresponding to the buttons in the toolbar: Users and Devices. Refer to Chapter 6, Configuring Router Options for details on configuring the features on the router.

Configuring Users

Users are added and maintained from the “User Profiles” window accessed by clicking **Users** button on the toolbar. The “User Profiles” window provides details about all active user profiles if **Enable User Profiling** is selected.

The **Enable User Profiling** option must be selected on the “User Profiles” window for the content filtering option to be operational.

Adding a User

This section describes how to add users to the router to restrict their access to router functions and to the Internet. You **MUST** be logged in as the administrator to add a user.

To add a user:

1. From the “Users Profile” window, click the **Add New User** button in the left navigation pane. This displays the “Profile User Information” window.

2. Type a user name in **Username**.
3. Type a password in **Password**.
4. Re-type the password in **Confirm**.
5. Click **Next**. This displays the "Profile Content Filtering" window. (At any time during user configuration, you can click **Finish** to complete the user profile and accept the defaults for this user.)

Content filtering restricts access to undesirable Web sites and Web content. The **Enable User Profiling** option must be selected on the "User Profiles" window for the content filtering option to be operational.

6. Select one of the following content filtering options:
   - **Disable all Content Filtering**
     User has access to all Internet content without restrictions.
   - **Allow access only to website addresses containing the following words**
     User has access only to the specified Web addresses or to addresses containing specified word entries defined in the Website word/name table.
   - **Deny all access to website addresses containing the following words**
     User is denied access to all Web addresses specified as well as addresses that contain any words specified in the Website word/name table.
7. If the **Allow access only…** or **Deny all access…** option is selected, type a word or Web address in the box under the Website word/name table, then click **Add Entry**. The system responds by adding the word or Web address to the Website word/name table.

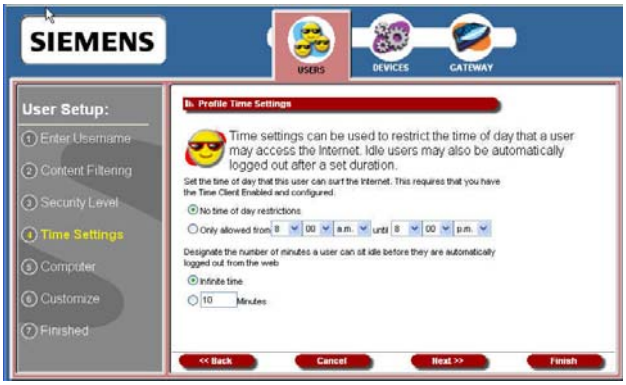
   Note: The entries in the Website word/name table may be either modified or deleted at any time by clicking either **Edit** or **Delete** next to the corresponding word or Web address.
8. Click **Next**. This displays the "Profile Configuration Access" window.

Profile configuration access defines the access permission for a user controlling what functions and features are available to that user.

9. Select one of the following profiles and click.

   - **Administrator**
     User has access to the Internet and all of the configuration tools on the router.
   - **Gamer**
     User has access to the Internet as well as the router's commonly used tools for gamers, including Port Configuration and DMZ.
   - **Web Surfer**
     Use has access only to the Internet, not to the router's configuration.

10. Click **Next**. This displays the "Profile Time Setting" window.



Profile time settings are used to limit a user's ability to use the Internet during certain times of the day or night. You can also define the amount of time a user stays logged on to the Internet without Web surfing activity (Idle Time). To use the time of day restrictions, you must have the Time Client enabled. Please see the Setup Wizard section for more information.

11. Select one of the following time of day options to control the time of day a user can access the internet:

    - **No time of day restrictions**
      The user can access the Internet at any time.
    - **Only allowed from**
      The user can only access the Internet at the time range set in the time drop-down menus. Be sure to specify the **from** and **until** times the user can access the Internet.

12. Select one of the following options to designate the number of minutes a user can sit idle before they are automatically logged out from the web:

    - **Infinite Time**
      The user is never automatically logged out of the Internet.
    - **Minutes**
      Type a time interval in minutes in **Minutes**. This time represents how long a user may be idle before automatically being logged out of the Internet.

13. Click **Next**. This displays the "Associated Computer/Connected Device" window.

Some users consistently use a particular computer to surf the Internet. To simplify logging in for these users, you can use the Associated Computer option to automatically log a particular user into the router with their username and password when they access the Internet from the specified computer.

14. Select one of the following:

    - A specific device to associate with the profile. All computers and devices currently on the network, powered on, and detected by the router are displayed in the computer list.
    - **None.** The user can log in from any device.

15. Click **Next**. This displays the "Customized Profile Icon" window.

All user profiles have an icon that displays in the left navigation pane of the "User Profiles" window. You may customize the color of this icon using the "Customized Profile Icon" window.

16. To select a color, do one of the following:

    - Select a color from the drop-down menu.
    - Type a numeric color value in the box next to the color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. **Note**: If you are entering a numeric value for the color, ensure that the "#" is in front of your numeric value.

17. Click **Finish**. This displays the "User Profile" window. The icon of the user you just created is displayed in the left navigation pane.

Editing A User Profile

This section describes how to edit a user profile. You must be logged in as the administrator to edit a user profile.

To edit a user profile:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to edit. This displays the "Profile Monitor" window.

2. Click **Edit Profile**. This displays the "Profile Content Filtering" window with the **User Setup** pane in the left navigation pane.

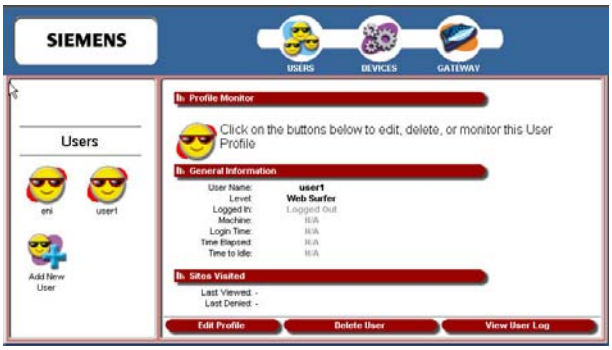
3. Click on any item in the **User Setup** list to display the appropriate window.
4. Make any changes.
5. Once you have made all the changes you want, click **Finish**.

Deleting a User

This section describes how to delete a user. You must be logged in as the administrator to delete a user.

To delete a user:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.



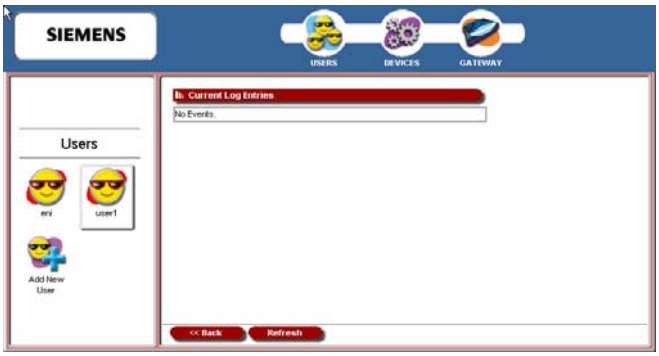
2. Click **Delete User**.

Viewing User Logs

User logs provide time stamped information about the activity of the user over the network.

To view user logs:

1. From the "Users Profile" window, click the button in the left navigation pane corresponding to the user you want to delete. This displays the "Profile Monitor" window.
2. Click **View User Log**. This displays the "Current Log Entries" window displaying all the log information about the user.

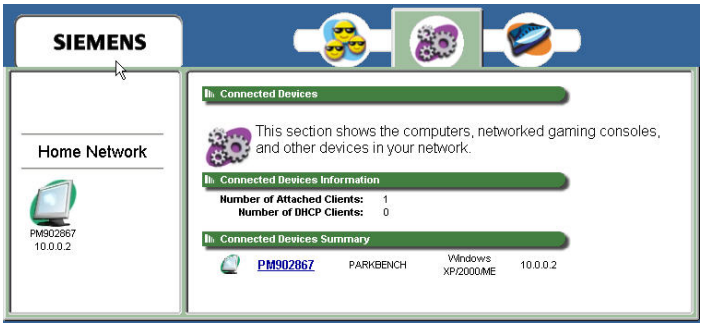


Configuring Devices

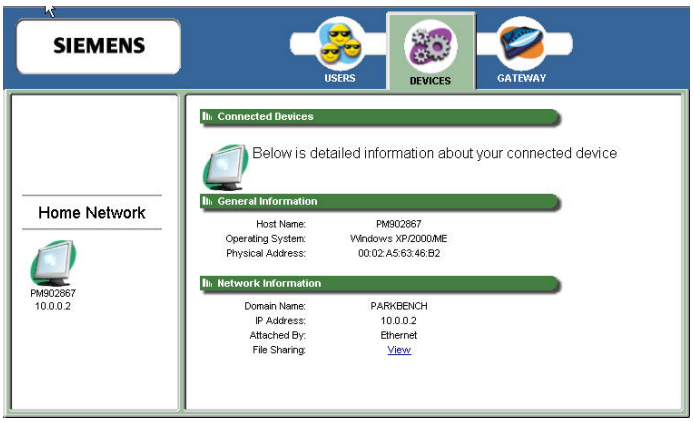
The Devices option allows you to view devices connected to your router. If you are logged in as the administrator, you can view all the connected devices to the router. If you are logged in as a specific user, you can only view devices associated with that user logon.

To use the Devices option:

1. Click **Devices** in the toolbar. This displays the "Connected Devices" window displaying general information about devices on your network.



2. Click the icon of a connected device in the left navigation pane, or click the device hyperlink under **Connected Devices Summary**. This displays the "Connected Devices" window, which displays both general and network information about the selected device.



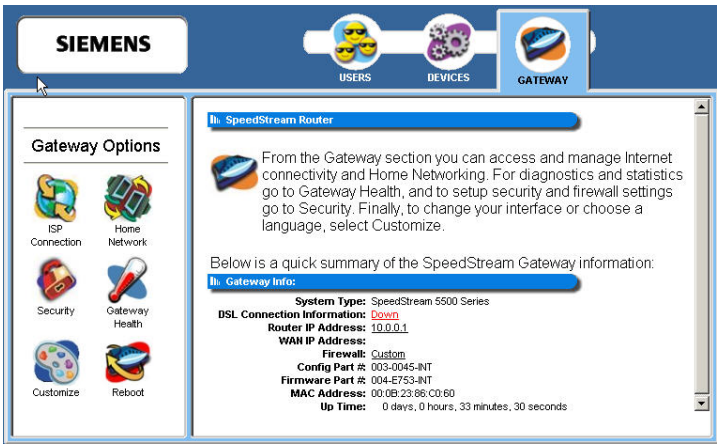
Chapter 6

Configuring Advanced Features

This chapter explains how to configure advanced features on the router.

This chapter contains details for configuring the many advanced features available with your router. Some of the features described below require at least a mid-level understanding of networking principles. These features are provided to allow configuration flexibility for advanced users.

These advanced features are accessed through the **Gateway** button available on the toolbar on the "Main" window. The options that display under the **Gateway Options** pane in the left navigation pane are based on how you logged into the system. If you logged in as the administrator, all options are turned on and enabled. If you logged in as a user, only the Gateway Health, Customize, and Reboot options are enabled.



Gateway Options discussed in this chapter

This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.

Get information about ISP connections. You can also use this option to set ISP configuration parameters. This should only be done when instructed by your ISP.

View network-related information

Configure security for the router.

Reboot the router.

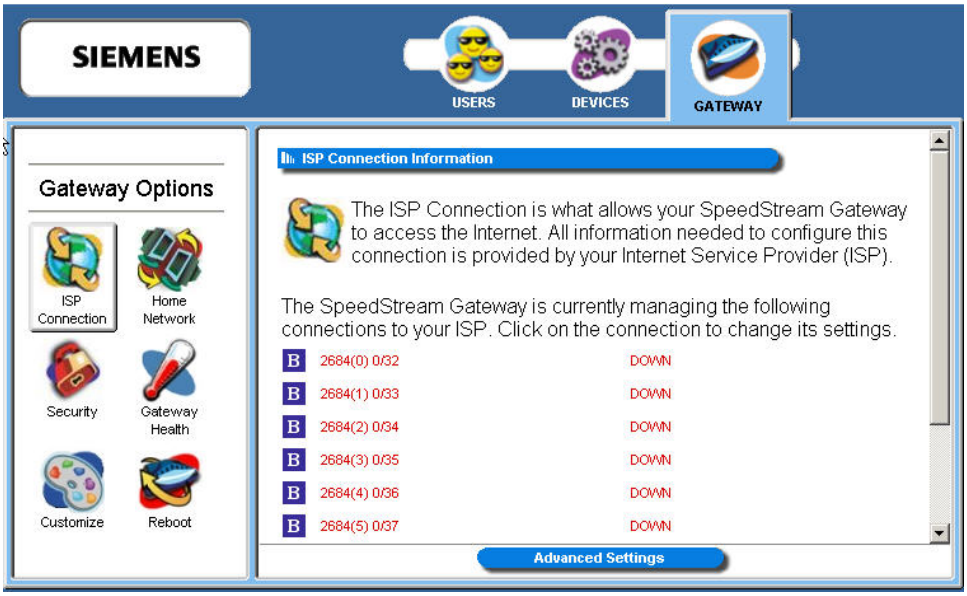
ISP Connection

The **ISP Connection** option displays all active and available Internet connections. Many of the settings for this option are intended for use only by advanced users. This option may not be available depending on your ISP. You must be logged in as an administrator to use this option.

WARNING: If this feature is not properly configured your Internet connection may terminate.

To use the ISP connection function:

1. Click the **ISP Connection** button in the left navigation pane. This displays the "ISP Connection Information" window listing all the ISP connections being managed by the router.

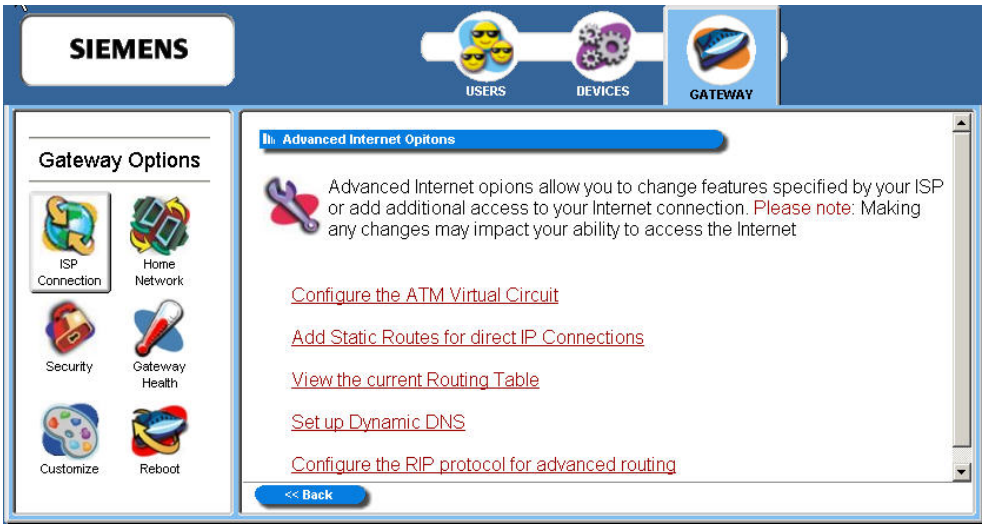


2. Click one of the ISP connections (in red) to reconfigure that connection. Please check with your ISP for the information required to reconfigure a connection.
3. Optionally refer to the section titled Advanced Settings for details on configuring advanced ISP connection settings.

Advanced ISP Settings

The router provides access to additional, advanced ISP configuration settings. All the options in this section should only be configured with the help and guidance of your ISP. Incorrect changes to any of these options could result in the failure of your Internet connection.

To access the advanced settings, click **Advanced Settings** from the "ISP Connection Information" window. This displays the "Advanced Internet Options" window.



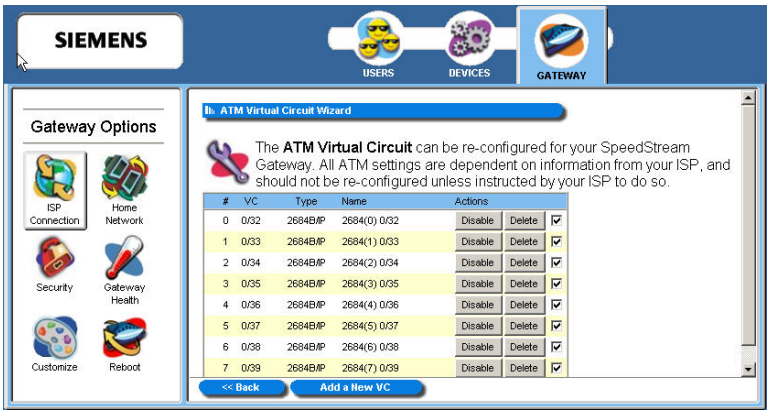
The advanced options are listed below. To access one of these options, click its link on the "Advanced Internet Options" window.

Configure the ATM Virtual Circuit	Create and configure a PVC (Permanent Virtual Circuit) across a network. A PVC is used to maintain a permanent connection between two points on a network.
Add Static Routes for direct ISP Connections	Configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data.
View the Current Routing Table	View a table of routing information of all static and dynamic routes for network devices.
Set up Dynamic DNS	Set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names.
Configure the RIP protocol for advanced routing	Configure the protocol that allows the router to determine the shortest path between two points on the network.

ATM Virtual Circuits

Use the ATM virtual circuit advanced option to create and configure a Permanent Virtual Circuit (PVC). A PVC is used to maintain a permanent connection between two points on a network. Changes to ATM settings should not be made unless you are advised to do so by your Internet Service Provider.

To access the ATM virtual circuit option, click the **Configure ATM Virtual Circuit** hyperlink on the "Advanced Internet Options" window. This displays the "ATM Virtual Circuit Wizard" window.



Make any modifications advised by your ISP.

Static Routes

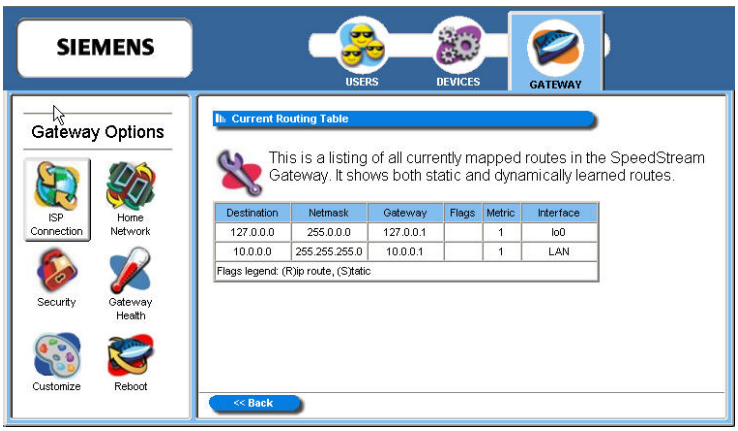
Use the static routes advanced option to configure static routes to remote equipment. Static routing allows a pre-defined route to be set for the transmission of data. Static routes take precedence over all dynamic routing options and also provide enhanced security over dynamic routing.

To configure the static routes:

1. Click the **Add Static Routes for Direct IP Connections** hyperlink from the "Advanced Internet Options" window. This displays the "Static Routes" window.

2. Type the IP address of the destination device in **Destination**.
3. Type the net mask of the destination device in **Net Mask**.
4. Optionally, type the IP address of a destination Gateway in **Next Hop**.
5. Select a connection type from the **Interface** drop-down menu.
6. Click **Apply**. The system responds by adding your new route to the routing table.

To view the current routing table, click the **View the current routing table** hyperlink. This displays a table of routing information including destination IP address, subnet mask, flags, Gateway, metric and interface of all static and dynamic routes for network devices.



Dynamic DNS

Use the dynamic DNS advanced option to set up dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names. For example, an IP address of 333.136.249.80 could be translated into siemens.com. To use the DDNS service, you must register for the service. You can register from the following web page: www.dydns.org/services/dydns.

Once registered, you must set up your DNS data on the router. Once this is done users can connect to your servers (or DMZ computer) from the Internet using your Domain name. Refer to the section in this document titled DMZ for more information on DMZs.

To set up Dynamic DNS on the router:

1. Click the **Set up Dynamic DNS** hyperlink from the "Advanced Internet Options" window. This displays the "Set Up Dynamic DNS" window.

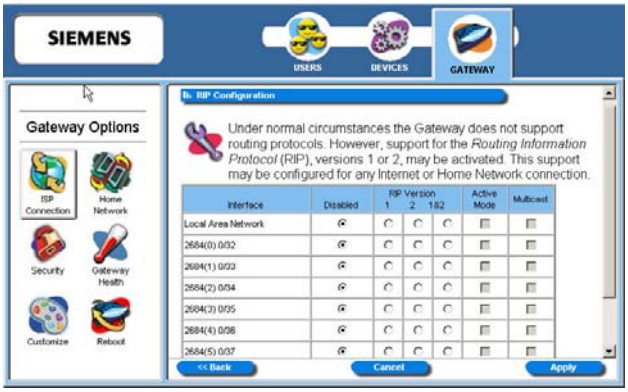
2. Select the **Enable** option.
3. Type the name provided to you by www.dydns.org in **Service Username**.
4. Type your www.dydns.org password in **Password**.
5. Type the domain or host name provided by www.dydns.org in **Host Name 1**.
6. Optionally, if you have more than one domain or host name, type it in **Host Name 2**.
7. Click **Apply**. The system responds by registering your domain or host name to www.dydns.org.

RIP (Routing Information Protocol)

Using RIP, the router is able to determine the shortest distance between two points on the network based on the addresses of the originating devices. RIP (Routing Information Protocol) is based on distance algorithms to calculate the shortest path. The shortest path is based on the number of hops between two points.

To use the RIP option:

1. Click the **Configure the RIP protocol for advanced routing** hyperlink from the "Advanced Internet Options" window. This displays the "RIP Configuration" window.

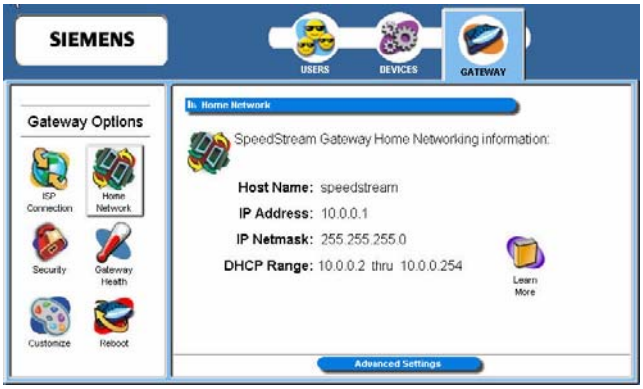


2. Select one of the following options from under the **RIP Version** heading next to the connection of your choice:
   - **1:** Provides essential RIP packet formatting for routing information packets.
   - **2:** Provides enhanced packet formatting for routing information packets by providing the following: IP address, subnet mask, next hop, and metric (shows how many routers the routing packet crossed to its destination.
   - **1&2:** A combination of both types of RIP packets.
3. Select an **Active Mode** checkbox next to a corresponding connection to enable it.
4. Click **Apply**. This displays the "Your Settings Have Been Saved" window.
5. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your router.

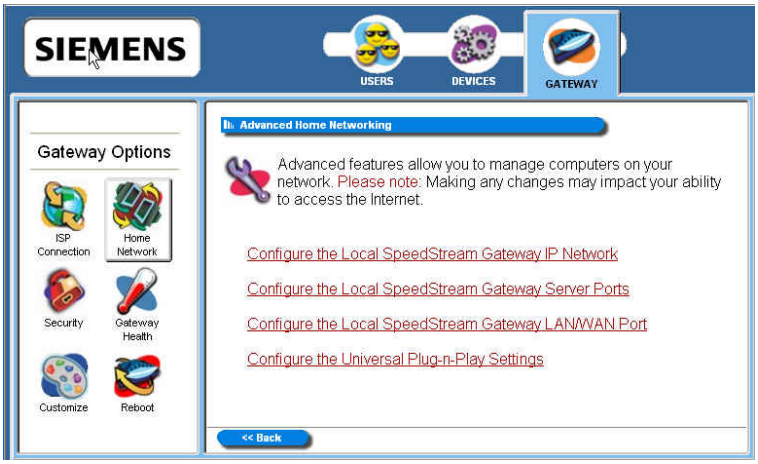
Home Network

The Home Network option displays all network-related information. You must be logged in as the administrator to access this option. To use the Home Network option:

1. Click the **Home Network** button on the **Gateway Options** pane. This displays the "Home Network" window containing information about the home network.



2. Optionally, click **Advanced Settings** to display a list of advanced features that allow you to manage the computers on your network. This displays the "Advanced Home Networking" window.



The advanced options are listed below. To access one of these options, click its link on the "Advanced Home Networking" window.

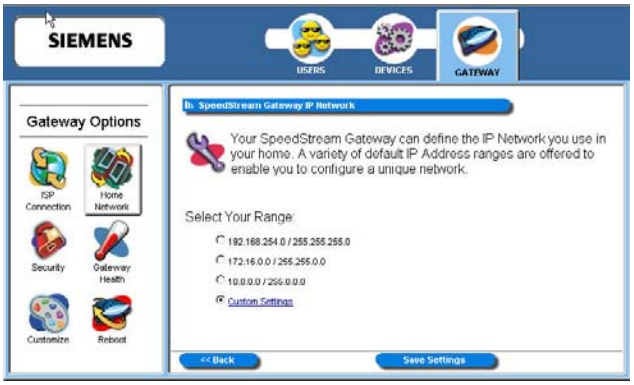
IP Network	Define the range for assigning IP addresses.
Server Ports	Specify the ports used by common applications such as HTTP, FTP, and Telnet.
LAN/WAN Port	Configure Ethernet port #4 as either a LAN (network) port or as a WAN (Internet connection) port.
UPnP	Configure UPnP. UPnP allows the Gateway to communicate directly with certain Windows operating systems.

IP Network

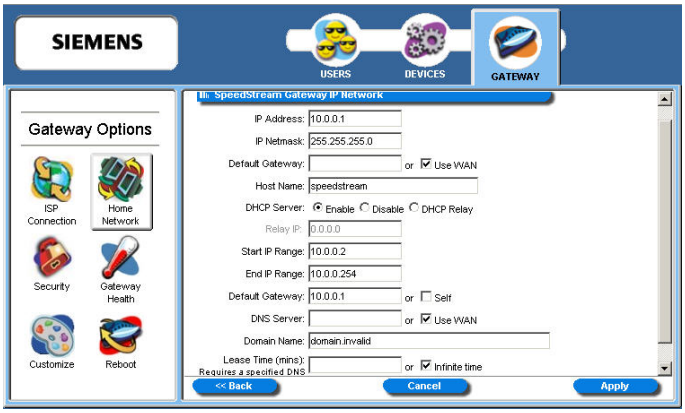
The router provides the flexibility to use different ranges of IP addresses to be assigned by the DHCP Server housed in the router. DHCP (Dynamic Host Configuration Protocol) allows computers to obtain either permanent or temporary IP addresses from a central server.

To configure the IP network option:

1. Click the **Configure the local SpeedStream Gateway IP Network** hyperlink. This displays the "SpeedStream Gateway IP Network" window.



2. Select a range from the displayed options and click **Save Settings**. Be sure to select an IP address range that is not in conflict with any existing devices.
3. Optionally, click the **Custom Settings** hyperlink for advanced configuration. Please contact your ISP for more information on configuring the options for custom settings.

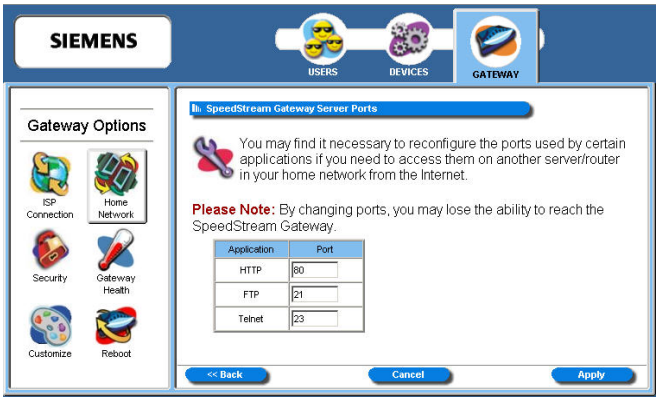


Server Ports

Common applications such as HTTP (Web site traffic), FTP, and Telnet use pre-defined incoming port numbers for compatibility with other services. If you wish to change the ports used by these applications you may do so using this option. This feature is recommended for use by advanced users only.

To configure the server port option:

1. Click the **Configure the Local SpeedStream Gateway Server Ports** hyperlink. This displays the "SpeedStream Gateway Server Ports" window.



2. Optionally, type a port number in **HTTP**. The default port for this field is 80.
3. Optionally, type a port number in **FTP**. The default port for this field is 21.
4. Optionally, type a port number in **Telnet**. The default port for this field is 23.
5. Click **Apply**. This displays the "Your settings have been saved" window.
6. Optionally, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your router.

LAN/WAN Port

Your router contains four Ethernet ports, Ethernet port #4 can be used as either a LAN (network) port or as a WAN (Internet connection) port. Select the appropriate option to define whether the port is used as a fourth local network port or as a connection for another broadband device.

Note: For configuration of the port as a WAN port, you may be required to consult your Internet Service Provider for the appropriate settings.

To configure the LAN/WAN port:

1. Click the **Configure the Local SpeedStream Gateway LAN/WAN Port** hyperlink. This displays the "SpeedStream Gateway LAN/WAN Port" window.

2. Select one of the following options:

   - **LAN** (Local Area Network)
     Use the port as a connection to the network located in your home or premises.
   - **WAN** (Wide Area Network)
     Use the port as a connection to a large connected network such as the Internet that is spread over a large geographic area. If you select the WAN option, please contact your ISP for instructions on how to configure this option.

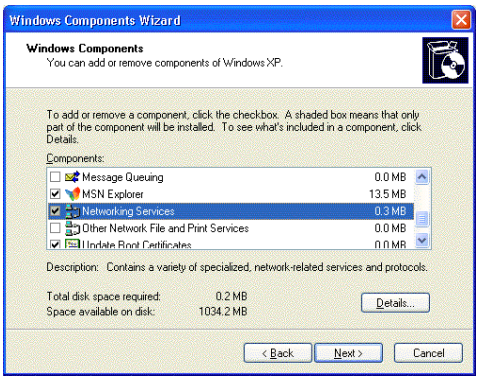
3. Click **Apply**.

UPnP (Universal Plug and Play)

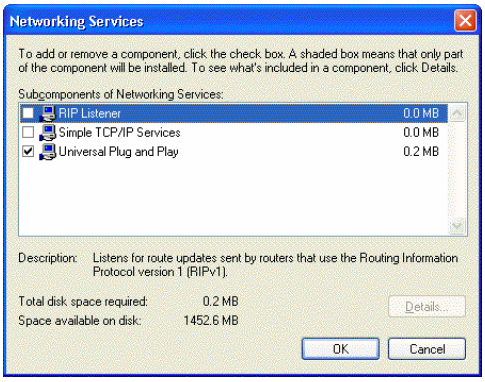
Microsoft UPnP allows the Gateway to communicate directly with certain Windows operating systems to trade information about the special needs of certain applications (such as messaging programs and interactive games) as well as provide information about other devices on the network. This communication between the operating system and Gateway greatly reduces the amount of manual configuration required to use new applications and devices.

Only certain versions of Windows XP and computer support the UPnP (Universal Plug and Play) function. Before configuring this option, make sure that UPnP is installed on your computer and enabled. Follow the steps below for installing UPnP components.

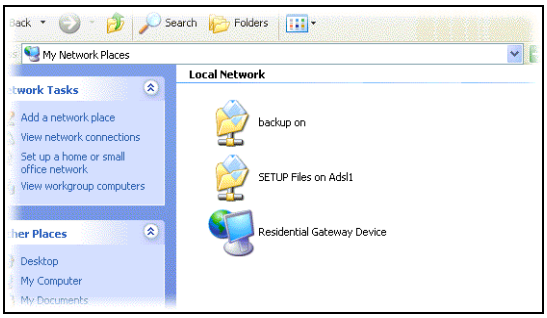
1. Select **Start>Control Panel**.
2. Select **Add or Remove Programs>Add/Remove Windows Components** to open the "Windows Components Wizard" window**.**



3. Select **Network Services** and click **Details**. This displays the "Networking Services" window.



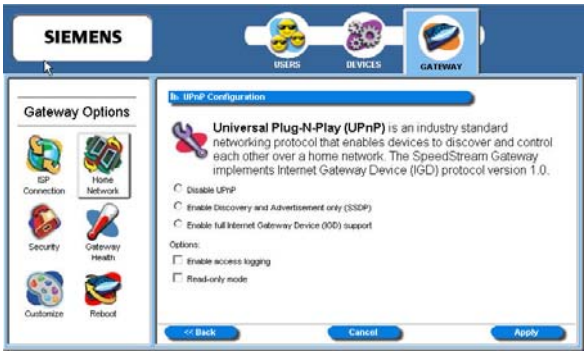
4. Select **Universal Plug and Play**.
5. Click **OK**. The system installs the UPnP components automatically.
6. After finishing the installation, go to **My Network Places**. You will find an icon for the UPnP function called Residential Gateway Device.



7. Double-click the icon. The Gateway will open another Web page for UPnP functions. Now, NAT functionality is available. The Gateway will create virtual servers automatically when it detects the computer running Internet applications that require this configuration.

Now you can configure the Gateway for UPnP. To configure UPnP on the Gateway:

8. Click **Configure the Universal Plug and Play Settings** link to display the "UPnP Configuration" window:



9. Select one of the following operating modes to enable or disable UPnP.

   - **Disable UPnP**
     Prevents the Gateway from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
   - **Enable Discovery and Advertisement only (SSDP)**
     Sends information about new devices (hardware) detected only. No information concerning software applications or services is transmitted.
   - **Enable full Internet Gateway Device (IGD) support**
     Allows the Gateway to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required.

10. Select one of the following control options.

    - **Enable Access Logging**
      Logs UPnP transactions to the system log.
    - **Read Only Mode**
      Can read configuration information from a device; cannot modify the device configuration.

11. Click **Apply** to accept the settings. This displays the UPnP finish window.

12. Click **Reboot**.

Security

Your router provides broad security measures against unwanted users. Security also allows for the configuration of the router firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration.

To use the security option, click the **Security** button on the **Gateway Options** pane. This displays the "Security Options" window containing icons to access the security features.

This section is organized into parts that correspond to the following buttons shown in the **Gateway Option**s pane.

Configure the network firewall. A firewall is a system designed to prevent unauthorized access to or from a private network.

Change administrative password.

Configure address translation. Address translation hides individual users/computers behind a single outward-facing address. Hiding internal addresses allows greater security for your network.

Firewall Settings

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall window provides a listing of options to be enabled or disabled as well as links to configure the more complex details of each feature.

To configure the firewall:

1. From the "Security Options" window, click **Firewall Settings**. This displays the "Firewall Settings" window.

2. Select the checkboxes for all **Security** options you wish to enable. This can be any of the following:

   - **Level**
     Enable security level access is from the router to the Internet or other networks. Click **Configure** to configure Security Level feature. This displays the "Firewall Level Configuration" window.
   - **Attack Detection**
     Enable protection from common hacker attacks to your computer/network from the Internet. Click **Configure** to configure the Attack Detection feature. This displays the "Attack Detection Configuration" window.
   - **IP Filtering**
     Configure inbound and outbound filter rules if your firewall Level setting is Custom. Click **Configure** to configure IP filter rules. This displays the "Firewall IP Filter Configuration Wizard" window.

3. Select **DMZ** for the **Gaming** option if you want to enable DMZ. Click **Configure** to configure firewall DMZ option. This displays the "Firewall DMZ Configuration" window.

4. Select the checkboxes for all **Support** options you wish to enable. This can be any of the following:

   - **Firewall Snooze Control**
     Bypass the firewall for a set amount of time so outside support personnel can access your router or network or so you can run an application that conflicts with the firewall. Click **Configure** to configure the snooze control. This displays the "Firewall Snooze Control" window.

Security Level

Security level refers to how much access is permitted from your router to the Internet or other networks.

To enable and configure the security level feature:

1. Select **Level** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Level**. This displays the "Firewall Level Configuration" window.

3. Select the firewall security level from the **Select Firewall Level** drop-down menu. This can be one of the following:

   - **Off**
     No firewall protection. Data can move freely both in and out of the router.
   - **Low**
     Provides basic firewall protection. Attack detection is enabled and only ports well known to the router can allow the flow of data.
   - **High**
     Provides maximum firewall protection. Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. (ICSA 3.0a Compliant.)
   - **Custom**
     Set your own rules for firewall protection. This option should be used by advanced users only. If you select this option, you must set customized rules for both inbound and outbound traffic using the IP Filtering option.

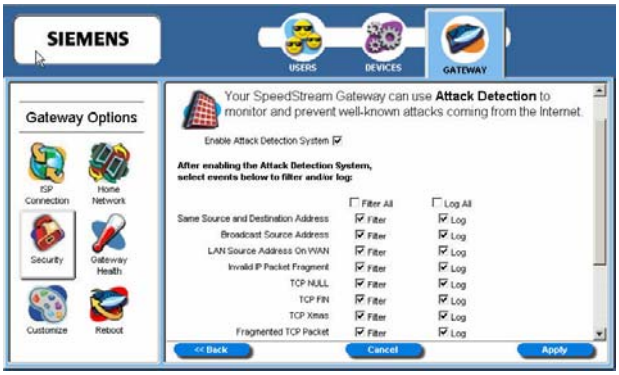
4. Click **Apply**.

Attack Detection

If the Attack Detection System is enabled, the router provides protection against the most common hacker attacks that attempt to access your computer/network from the Internet. Intrusion attempts can also be logged to provide a record of attempts and their source (when available).

To enable and configure the attack detection feature:

1. Select **Attack Detection** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Attack Detection** option. This displays the "Attack Detection Configuration" window.



3. Select **Enable Attack Detection**.
4. Select **Filter** for each event in the list you want to filter or, if you want to filter all events, select **Filter All**. This provides maximum protection against malicious intrusion from outside your network.
5. Select **Log** for each event in the list you want to log or, if you want to log all events, select **Log All**.
6. Click **Apply**.

Below is a description of each event that can be monitored.

- **Same Source and Destination Address**
  An outside device can send a SYN (synchronize) packet to a host with the same source and destination address (including port) causing the system to hang. When the receiving host tries to respond to the source address in the packet, it ends up just sending it back to itself. This packet could ping-pong back and forth over 200 times (consuming CPU resources) before being discarded.
- **Broadcast Source Address**
  An outside device can send a ping to your router broadcast address using a forged source address. When your system responds to these pings, it is brought down by echo replies.
- **LAN Source Address on LAN**
  An outside device can send a forged source address in an incoming IP packet to block trace back.
- **Invalid IP Packet Fragment**
  An outside device can send fragmented data packets that can bring down your system. IP packets can be fairly large in size. If a link between two hosts transporting a packet can only handle smaller packets, the large packet may be split (or fragmented) into smaller ones. When the packet fragments get to the destination host, they must be reassembled into the original large packet like pieces of a puzzle. A specially crafted invalid fragment can cause the host to crash
- **TCP NULL**
  An outside device can send an IP packet with the protocol field set to TCP but with an all null TCP header and data section. If your router responds to this attack, it will bring down your system.

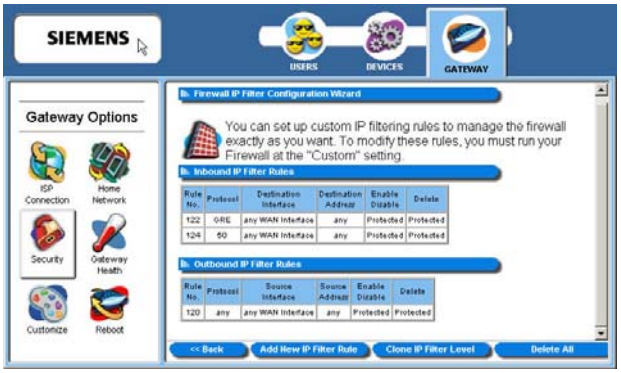
- **TCP FIN**
  An outside device can send an attack using TCP FIN. This attack never allows a data packet to finish transmitting and brings down your system.
- **TCP XMAS**
  An outside device can send an attack using TCP packets with all the flags set. This causes your system to slow to a halt.
- **Fragmented TCP Packet**
  An outside device can send an attack using fragmented packets to allow an outside user Telnet access to a device on your network.
- **Fragmented TCP Header**
  An outside device can send an attack using TCP packets with only a header and no payload. When numerous packets are sent through the router in this manner, your system slows and halts.
- **Fragmented UDP Header**
  An outside device can send an attack using fragmented UDP headers to bring down a device on your network.
- **Fragmented ICMP Header**
  An outside device can send an attack using fragmented ICMP headers to bring down a device on your network.
- **Inconsistent UDP/IP header lengths**
  An outside device can send an attack using inconsistent UDP/IP headers to bring down a device on your network.
- **Inconsistent IP header lengths**
  An outside device can send an attack using changes in the IP header to zero the fragment offset field. This will be treated as a complete packet when received and cause your system to halt.

IP Filtering

Define inbound and outbound IP filter rules using this procedure. IP filtering rules can only be defined if the **Firewall Level** setting is **Custom**. This method of firewall protection is recommended for advanced users only.

To define IP filtering rules:

1. Click the **Configuration** hyperlink next to the **IP Filter** option on the "Firewall Settings" window. This displays the "Firewall IP Filter Configuration Wizard" window.



2. Do one of the following:

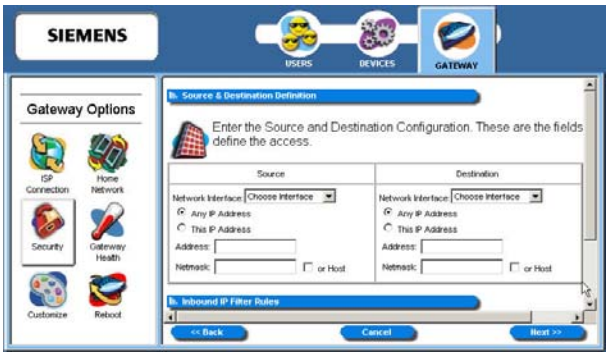
   - Click **Add New IP Filter Rule** to add new IP filter rules. This displays the "Basic Rule Definition" window.
   - Click **Clone IP Filter Level** to clone IP filter rules already defined. This displays the "Clone Rule Definition" window. Once cloned, you can modify the existing rules.

Add New IP Filter Rules

The "Basic Rule Definition" window is displayed when you select **Add New IP Filter Rule** from the "Firewall IP Configuration Wizard" window. Using this option, you can define both inbound and outbound rules. Each rule defined is added to the Rule Definition table.

To add a new rule:

1. Type up to a five digit numeric value in **Rule No** to uniquely identify the rule.
2. Select either **Permit** or **Deny** from the **Access** drop-down menu. Select **Permit** to allow the rule and **Deny** to prohibit the rule.
3. Select either **Inbound** or **Outbound** from the **Direction** drop-down menu. **Inbound** refers to data coming into the router, while **Outbound** refers to data transmitted from the router.
4. Optionally, select **Disable stateful inspection for packets matching this rule**.
5. Optionally, select **Create a log entry for packets matching this rule**. When selected, an entry is placed in the log file when packets match this rule.
6. Click **Next**. This displays the "Source and Destination Definition" window.



7. Under the **Source** heading, select a network connection from the **Network Interface** drop-down menu.
8. Select one of the following options:

   - **Any IP Address**
     Select this option if this rule applies to any IP address from the source.
   - **This IP Address**
     Select this option if a rule applies to a specific IP address from the source.

9. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
   - Enter a netmask in the **Netmask** field.
   - Select **or Host** to use your router netmask as the source netmask.
10. Under the **Destination** heading, select a network connection from the **Network Interface** drop-down menu.
11. Select one of the following options:
    - **Any IP Address**
      Select this option if this rule applies to any IP address of the destination.
    - **This IP Address**
      Select this option if a rule applies to a specific IP address of the destination.
12. If you selected **This IP Address**, enter an IP address in the **IP Address** field and do one of the following:
    - Enter a netmask in the **Netmask** field.
    - Select **or Host** to use your router netmask as the destination netmask.
13. Click **Next**. This displays the "Protocol Definition" window.

14. Do one of the following:
    - Select one of the following protocol options from the **Select by Name** drop-down menu. This defines the types of packets filtered.
      - Any Protocol
      - TCP (Transmission Control Protocol):
        Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users. Click **Next** to display the "TCP/UDP Options" window.
      - UDP (User Datagram Protocol):
        Provides for the exchange of datagrams without acknowledgement or guaranteed delivery. Click **Next** to display the "TCP/UDP Options" window.
      - **ICMP** (Internet Control Message Protocol):
        A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command. Click **Next** to display the "ICMP Options" window.
      - **GRE** (Generic Routing Encapsulation):
        A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
    - Type a protocol number in the **Select by Number** field.
15. Click **Finish**.

TCP/UDP Options Window

The "TCP/UDP Options" window is displayed if you select TCP or UDP protocol from the "Protocol Definition" window. If you selected either of these protocol types, you must identify the source and destination ports.

1. Select one of the following options from the **Source Port Operator** drop-down menu and the **Destination Port Operator** drop-down menu:

   - **any**
     Any port is acceptable as the source/destination port.
   - **less than or equal to**
     A port less than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **equal to**
     A port equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **greater than or equal to**
     a port greater than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **range**
     Any port between the value of the entry in the **Port 1** field and the value in the **Port 2** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** and **Port 2** fields.

2. Optionally, select **Check TCP syn packets** if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
3. Click **Next**.
4. Click **Finish**.

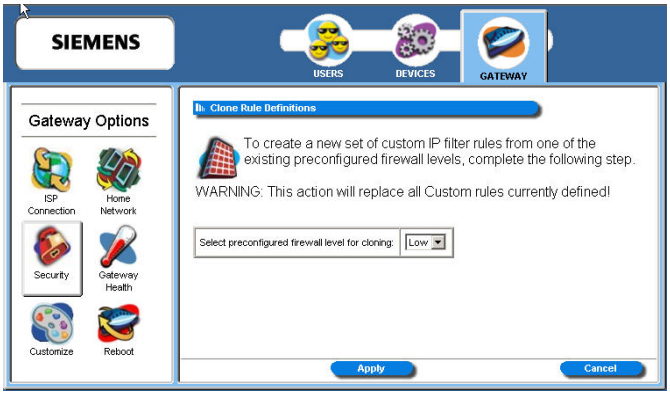
ICMP Options Window

The "ICMP Options" window is displayed if you select ICMP protocol from the "Protocol Definition" window.

1. Do one of the following:
   - Select any of the ICMP options you wish to filter.
   - Select **All Types** to filter all options.
2. Click **Next**.
3. Click **Finish**.

Clone IP Filter Rules

The "Clone Rule Definitions" window is displayed when you select **Clone IP Filter Level** from the "Firewall IP Configuration Wizard" window. Using this option, you can clone either high or low level rules and modify them according to your needs. If you choose to clone IP filter rules, the rules already defined in the Rule Definition table are discarded.



To clone IP filter rules:

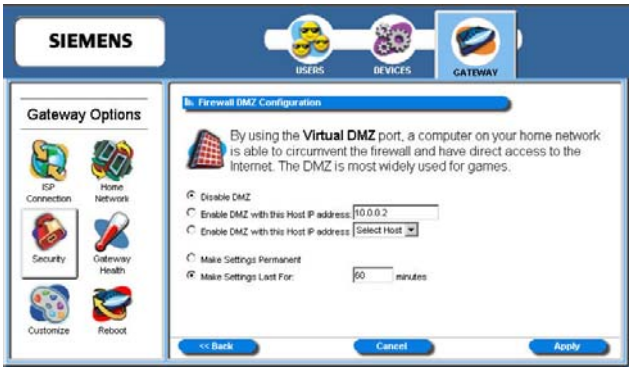
1. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
   - **Low**
     Clones low-level IP filter rules.
   - **High**
     Clones high-level IP filter rules.
2. Click **Apply**. This displays the "Firewall IP Filter Configuration Wizard" window with the selected rule set showing in the Rule Definition table.
3. Disable or delete any rule as desired.

DMZ

The DMZ feature allows a computer on your home network to circumvent the firewall and have direct access to the internet. This feature is primarily used for gaming. The router allows you to configure a temporary or permanent DMZ (Demilitarized Zone) to bypass the firewall for network or Internet gaming. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host. This function is recommended for use only when you require this special level of unrestricted access as it leaves your router and network exposed to the Internet with no firewall protection.

To enable and configure the DMZ:

1. Select **DMZ** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **DMZ**. This displays the "Firewall DMZ Configuration" window.



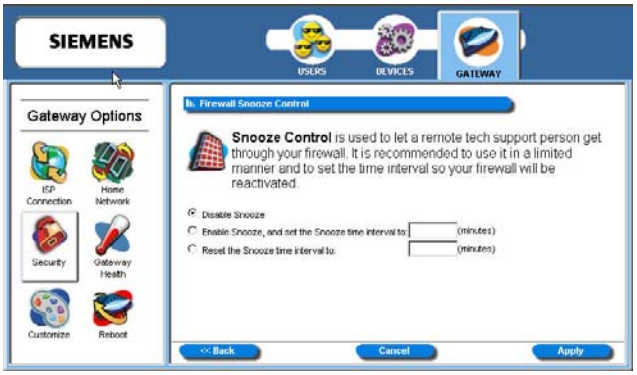
3. Select one of the following DMZ enable options:
   - **Disable DMZ**
     The firewall is not bypassed.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address typed in the box next to this field.
   - **Enable DMZ with this Host IP address**
     The firewall is bypassed through an IP address that is selected from the **Select Host** drop-down menu next to this field. Select the desired host from the drop down.
4. Select one of the following time element options:
   - **Make Settings Permanent**
     DMZ settings are permanent unless changed by the administrator.
   - **Make Settings Last for**
     DMZ settings last for only the time (in minutes) entered in the box next to this option.
5. Click **Apply**.

Firewall Snooze Control

The snooze feature allows you to bypass the firewall for a set amount of time so outside support personnel can access your router or network, or so you can run an application that conflicts with the firewall. This function is recommended for use only when you require this special level of unrestricted access as it leaves your router and network exposed to the Internet with no firewall protection.

To enable and configure snooze control:

1. Select **Firewall Snooze Control** from the "Firewall Settings" window.
2. Click the **Configure** hyperlink next to **Firewall Snooze Control**. This displays the "Firewall Snooze Control" window.



3. Select one of the following options:
   - **Disable Snooze**
     Disables all snooze control. In this mode, the firewall is not bypassed.
   - **Enable Snooze, and set the Snooze time interval to**
     Enables snooze for a specified time period. Be sure to enter the number of minutes to define how long the firewall should be disabled.
   - **Reset the Snooze time interval to**
     Reset the snooze control time period. Use this option if you need a time extension for an open snooze session. Be sure to specify the additional amount of time (minutes) the firewall should be disabled.
4. Click **Apply**.

Administrator Password

You may change the router's administrator password at any time if you have administrative rights to the router. To change the administrator password:

1. From the "Security Options" window, click the **Admin Password** button. This displays the "Enter Network Password" window.
2. Provide the administrator log on ID and password, then click **OK**. This displays the router Administrator Setup window.

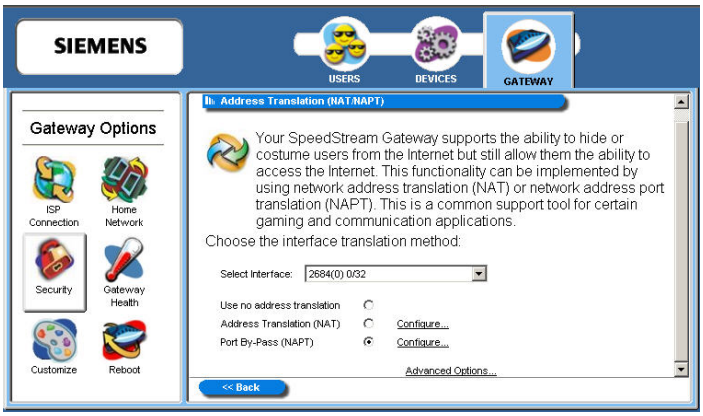
3. Make any desired changes to the **User Name**, **New Password**, and **Confirm Password**.
4. Click **Save Settings**.

Address Translation

The Address Translation feature provides different methods of keeping individual users/computers hidden behind a single outward-facing address, while still allowing them to access the Internet and related applications. If you have more than one available Internet connection interface, they will all be displayed in the drop-down menu for ease of selection.

To enable and configure the address translation feature:

1. From the "Security Options" window, select the **Address Translation** button. This displays the "Address Translation (NAT/NAPT)" window.



2. Select an interface from the **Select Interface** drop-down menu.
3. Select one of the following options:

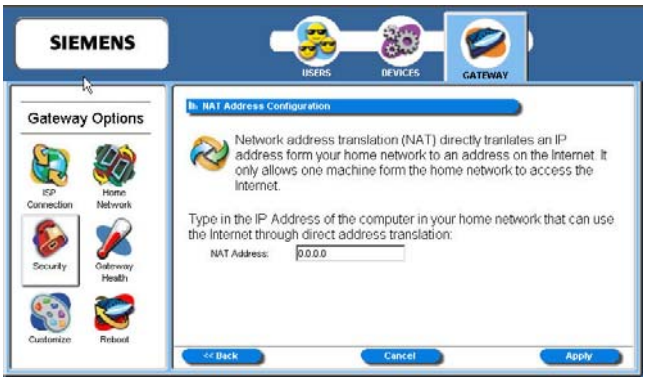
   - **Use no address translation**
     Disables address translation.
   - **Address Translation (NAT)**
     Uses NAT for address translation. NAT is an Internet standard that allows a LAN to use one set of IP addresses for internal traffic and a second set for external traffic. This displays the "NAT Address Configuration" window.
   - **Port By-Pass (NAPT)**
     Uses NAPT for address translation. Only TCP, UDP, and ICMP protocols support NAPT. NAPT allows many devices connected to the router access to the Internet while masking the identification of the internal IP addresses. This displays the "Port By-Bass Configuration" window.

Address Translation With NAT

Network Address Translation (NAT) translates an IP address from your home network to an address on the Internet. It allows only one machine to access the Internet.

To enable and configure NAT address translation:

1. Select **Address Translation (NAT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Address Translation (NAT)**. This displays the "NAT Address Configuration" window.



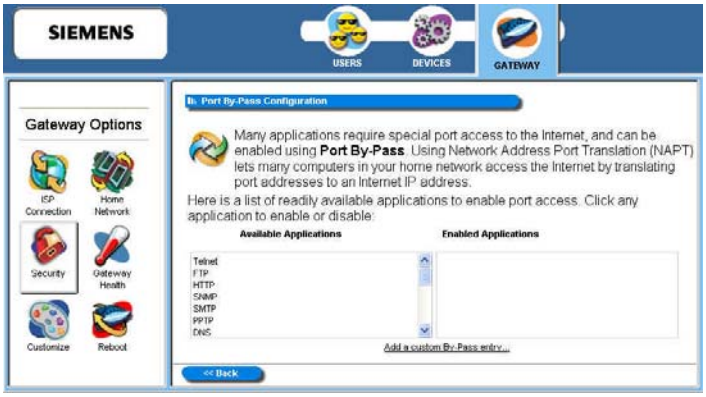
3. Type the IP address of the one computer in your network that you wish to have access to the Internet.
4. Click **Apply**.

Address Translation With NAPT

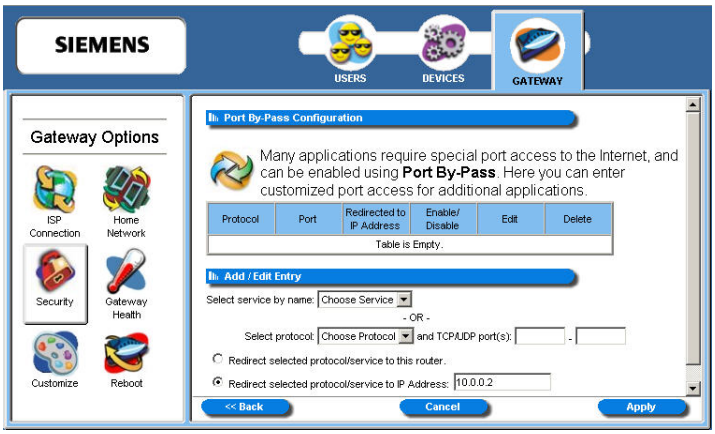
Many applications require special port access to the Internet in order to function. By enabling Network Address Port Translation (NAPT), multiple computers in your home network have access to the Internet by translating port addresses to an Internet IP address while masking their IP addresses from outside users. Only TCP, UDP, and ICMP protocols support NAPT.

To enable and configure NAPT address translation:

1. Select **Port By-Pass (NAPT)** from the "Address Translation (NAT/NAPT)" window.
2. Click the **Configure** hyperlink next to **Port By-Pass (NAPT)**. This displays the "Port-By-Pass Configuration" window.



3. To enable an application for NAPT, click the desired application from the **Available Applications** list. The application is moved to the **Enabled Applications** list.
4. Optionally, click the **Add a custom bypass entry** hyperlink. This displays the advanced features on the Port By-Pass Configuration" window. The advanced option allows you to configure special port access to the Internet.



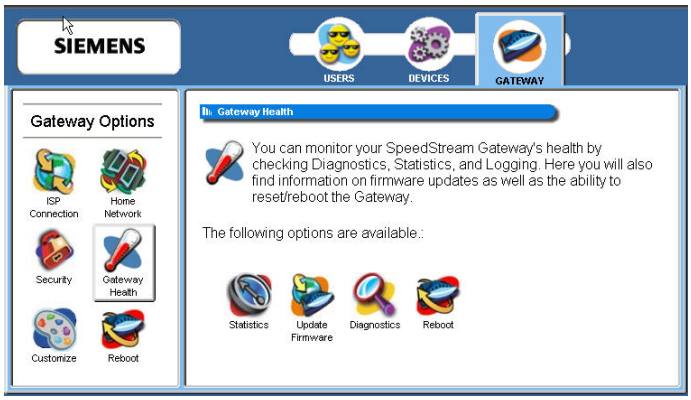
5. Do one of the following:
   - Select one of the following services from the **Select service by name** drop-down menu.
     - **Telnet**
       Telnet is a program that allows you to connect to other computers over the Internet. This options uses port 23.
     - **FTP** (File Transfer Protocol)
       FTP is used to transfer files in both ASCI and Binary format between local and remote devices. This option uses port 21.
     - **HTTP** (Hyper Text Transfer Protocol)
       HTTP is the standard method of transferring all types of information over the Internet. This option uses port 80.
     - **SNMP** (Signaling Network Management Protocol)
       SNMP is a protocol used by network management applications to help manage a network. This option uses port 161.
     - **SMTP** (Simple Mail Transfer Protocol)
       SMTP is used for sending email between servers. This port uses port 25.
     - **PPTP** (Point-to-Point Tunneling Protocol)
       PPTP is a protocol that allows VPN (Virtual Private Network) applications. This option uses port 1723.
     - **Domain**
       Domain is used for DNS options. This option uses port 53.
   - Select a protocol from the **Select Protocol** drop-down menu. This can be one of the following:
     - **TCP** (Transmission Control Protocol)
       Provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user.
     - **UDP** (User Datagram Protocol)
       A connectionless mode protocol that provides the delivery of packets to a remote or local user.
     - **ICMP** (Internet Control Message Protocol)
       A method by which IP software on a host or router can communicate to pass information to other machines.
     - **GRE** (Generic Routing Encapsulation)
       This protocol is used to provide tunneling for a VPN connection.
6. If you selected a protocol, type the range of UDP or TCP ports in the appropriate boxes
7. Select one of the following options:
   - **Redirect selected protocol/service to this router**
     The protocol or service that you select is directed to your router.
   - **Redirect selected protocol/service to IP Address**
     The protocol or service that you select is directed to an IP address on your LAN that you type in the box next to this field.
8. Click **Apply**.

Chapter 7

Monitoring Router Health

This chapter explains how to monitor the health of the router.

This chapter describes how to monitor the health of the router. The router health options are used to gauge the various measures of router's health. To use the router health options, click the **Gateway Health** button from the **Gateway Options** pane. This displays the "Gateway Health" window.



Gateway Health options discussed in this chapter:

This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Health** pane.


Statistics

Used to measure the Internet stats, home networking stats, security stats, and the different router log files.


Update Firmware

Updates the firmware of your router through the Internet or from a device connected to your router. (Not all routers will have this option.)


Diagnostics

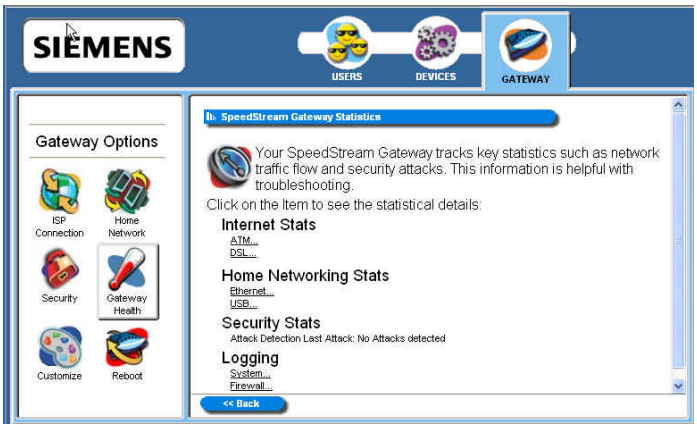
Runs a diagnostic program against a selected connection on your router.


Reboot

Reboots the system or resets all settings to router factory defaults.

Statistics

You can display statistics for the Internet, Home Networking, Security, and Logging. To display any of these statistics, click the **Statistics** button from the "Gateway Health" window. This displays the "SpeedStream Gateway Statistics" window.



Click the hyperlink for the type of statistics you wish to view. These fall into four categories:

- **Internet Stats**
  Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.
- **Home Networking Stats**
  Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the router. (USB connection is not available on this model.)
- **Security Stats**
  Security breach attempts are shown for any firewall rules or attack detection services you have defined on the Firewall customization window.
- **Logging**
  Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

Internet Stats

Internet statistics are commonly used by your Internet Service provider to diagnose service-related issues. Internet statistics include either ATM or DSL statistics.

ATM Statistics

View status and statistical information for the WAN-side Asynchronous Transfer Mode (ATM) network connection. WAN-side connection to the service provider is based on an Asynchronous Transfer Mode (ATM) network connection. In addition, statistical information is provided for each Virtual Circuit (VC) configured under the ATM Adaptation Layer (AAL).

To view ATM statistics, click the **ATM** hyperlink under **Internet Stats**.

DSL Statistics

View status and statistical information for the Digital Subscriber Line (DSL) when the physical WAN-side connection to the service provider is achieved through a DSL line. Statistical information is accumulated over periodic intervals and may be displayed for up to a 24 hour period.

To view DSL statistics, click the **DSL** hyperlink under **Internet Stats**

Ethernet Home Networking Stats

Home Networking statistics are helpful for troubleshooting issues on your home network. These statistics are displayed for each physical interface connected to the router.

View status and statistical information for LAN-side Ethernet connectivity.

Pay special attention to the status (up or down) reported for each Ethernet port to verify that each cable is connected properly and detected by the router.

Logging

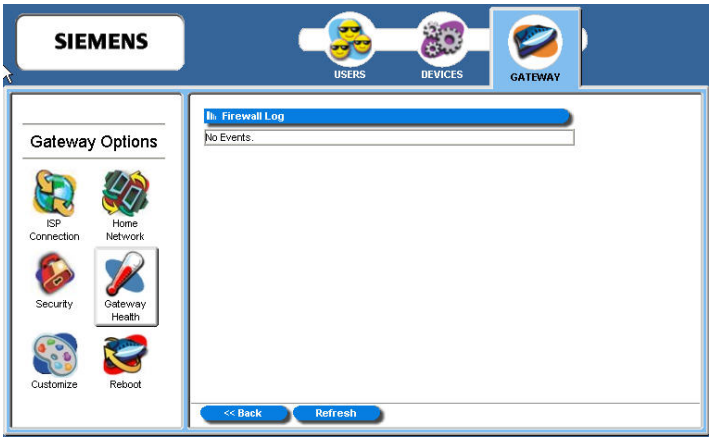
Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available: System, Firewall, and User Access.

System Logging

System logging displays router status, user login, interfaces accessed, etc. Activity displayed in the system log is defined using the checkboxes provided at the bottom of the window. Click **Apply** after making any changes. The system log can be cleared or saved to a text file using the appropriate buttons, Clear Log or Save Log.

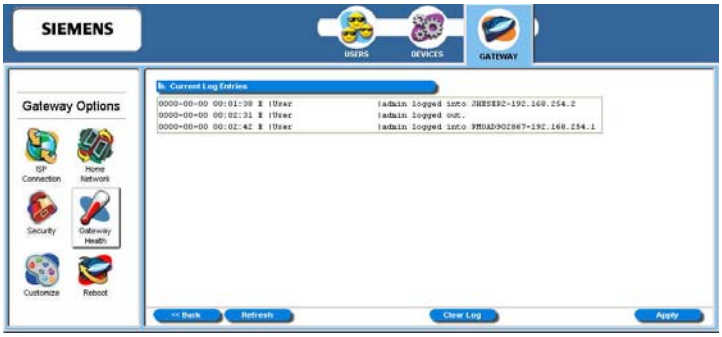
Firewall Logging

Firewall Logging displays attempts (both failures and successes) to access data through the firewall. Firewall log entries are defined on the **Firewall Settings Configuration** window found under the **Security** menu.



User Access

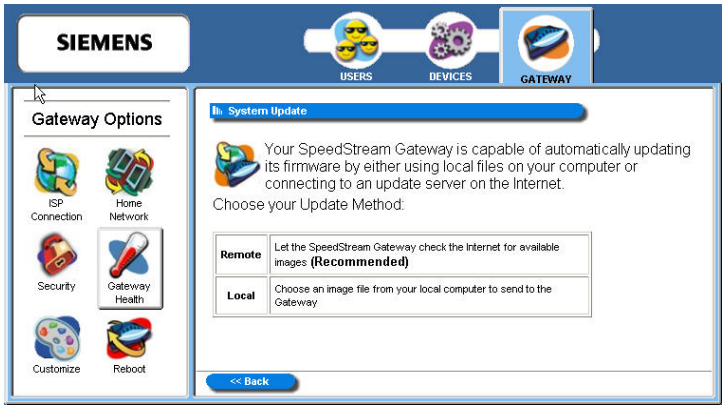
User Access logging displays activity related to users logging in or out of the router. Both successful and unsuccessful attempts by username are recorded.



Update Firmware

This feature updates the firmware of your router through the Internet or from a device connected to your router. This option may not be available on your router configuration. If available, you must be logged in as the router Administrator to access the utility.

To access this feature, click the **Update Firmware** button from your "Gateway Health" window. This displays the "System Update" window.



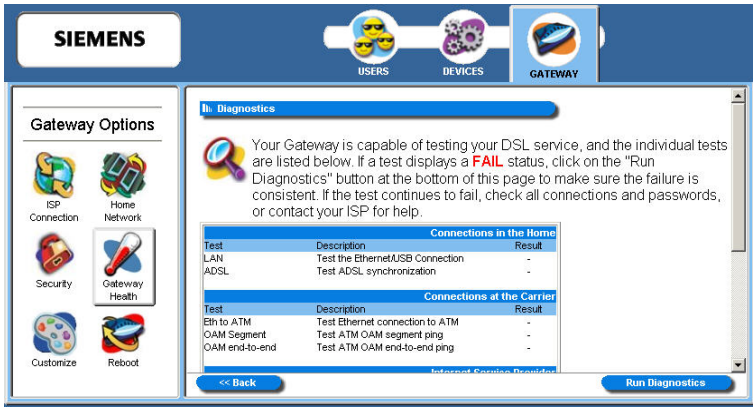
Select one of the following download options to start the download process.

- **Remote**
  Checks the Internet for the appropriate upgrade file. This is the recommended method.
- **Local**
  Download the firmware update from a location on your network and select the upgrade file. Before doing this, you must download the upgrade file to your computer.

Important: Do not turn off or interrupt the router during a firmware upgrade session. The router could be rendered inoperable!

Diagnostics

The router provides diagnostic tests and data for each interface. This data is commonly requested by technical support to assist in troubleshooting. To access this feature, click the **Diagnostics** button from your "Gateway Health" window. This displays the "Diagnostics" window.



To use the diagnostic option:

1. Select a connection to test from the **Connection to Test** drop-down menu. You must move all the way to the bottom of this window to display this drop-down menu.
2. Click **Run Diagnostics**. The system responds by displaying the results in the different tables. Pay special attention to any tests that report a failing condition and check the connections for these interfaces before running the diagnostics again.
3. Click **Apply**.

Chapter 8

Miscellaneous Router Options

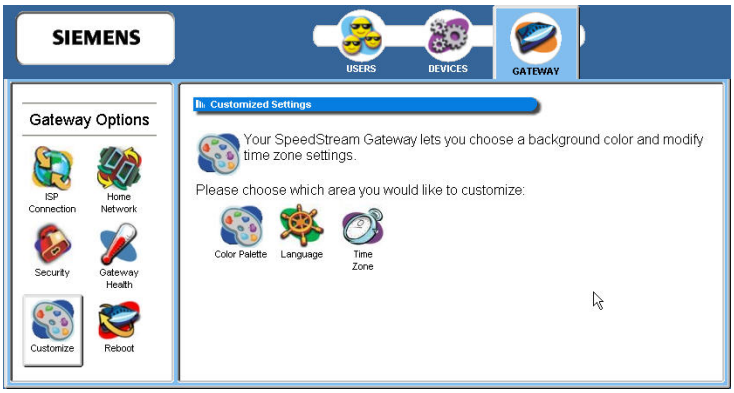
This chapter explains how to customize the appearance of the configuration program and to reboot the router. This chapter is organized into parts that correspond to the following buttons shown in the **Gateway Options** pane.

Customize the router's display.

Reboot the router.

Customize

You are able to control the background color, language, and time zone settings of your router using customization options. To access the customization options, click the **Customization** button from the **Gateway Options** pane. This displays the "Customized Settings" window.



Customization options discussed in this chapter:

Customize the appearance of the configuration interface/program.

Select language to display in text. (Not all routers will have this option.)

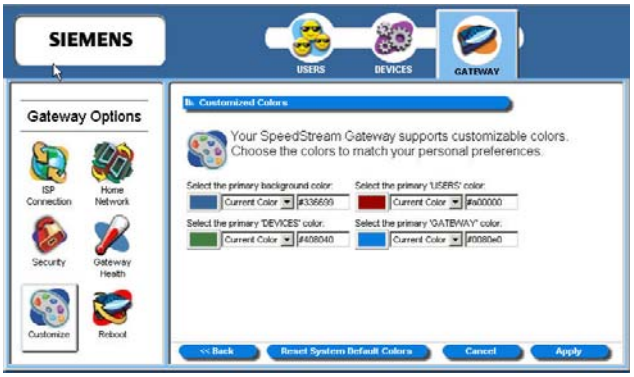
Configure time parameters to automatically synchronize the router's internal date and time settings with those of your selected time zone.

Color Palette

Multiple color selections are available to customize the appearance of the configuration interface/program.

To configure the color palette:

1. From the "Customized Settings" window, click the **Color Palette** button. This displays the "Customized Colors" window.



2. Using the color drop-down menus from the different display options, select the colors you wish to use in the system.
3. Optionally, type a numeric color value in the box next to the particular color drop-down menu. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. If you are entering a numeric value for the color, ensure that the "#" is in front of your numeric value.

   Click **Reset System Default Colors** if you want to reset all system color schemes to the factory settings.
4. Click **Apply**.

Language

Multiple languages may be available for displaying text in the configuration interface/program. This option may not be available on your router configuration.

To set the language used on the router windows:

1. From the "Customized Settings" window, click the **Language** button. This displays the "Customized Language" window.

2. Select your desired language.
3. Click **Apply**.

Time Zone

Using this option, you can configure the time parameters to automatically synchronize the router's internal date and time settings with those of your selected time zone. This time will be used to control time restrictions you may set for users as well as in entries in the system log.

To enable and configure the time zone feature:

1. From the "Customized Settings" window, click the **Time Zone** button. This displays the "Configure Time Zone" window.

2. Select **Yes** for **Enable Time Client**.
3. Select a time zone from the **Select Time Zone** drop-down menu.

   Note: The router's time server is unable to determine whether your time zone is currently observing daylight savings time. If you are currently observing daylight savings time, select an alternate time zone that matches your time settings during daylight savings time observation periods.
4. Click **Apply**.

Reboot

You can reboot the router using the Reboot option, or you can reset the router to factory defaults using the reset option. Reboot should be used when the router needs to be restarted. The router can also be rebooted using the power switch on the rear panel of the router. This option can be used at either the user or administrator level.

To reboot or reset factory defaults on the router:

1. Click the **Reboot** button from the **Gateway Options** pane. This displays the "System Reboot" window.

2. If you want the factory default settings to be reset, click **Reset to Factory Defaults**. Reset should be used when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the router does not appear to be working properly. This option resets all custom settings, users, and passwords on your router. You must be logged on as the administrator to use this option.
3. Click **Reboot**.

Appendix A

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the router and some possible solutions to them. If you follow the suggested steps and the router still does not function properly, contact your Internet Service Provider or Technical Support for assistance.

General Issues

Problem: **Can't connect to the router to configure it.**

Solution: Check the following:

- The router is properly installed, connections are OK, and it is powered ON. Check the LEDs for Ethernet port status.
- Ensure that your computer and the router are on the same network segment.
- If your computer is set to "Obtain an IP Address automatically" (DHCP client), restart your computer.

Internet Access

Problem : **When I enter a Web site address or IP address I get a time out error.**

Solution: A number of things could be causing this. Try the following troubleshooting steps.

- Verify that other computers work. If they do, ensure that your computer's IP settings are correct. If using a fixed (static) IP address, check the network mask, default router and DNS settings as well as the IP address.
- If the computers are configured correctly, but still not working, check the router. Ensure that it is connected and on. Connect to it and check its settings. (If you cannot connect to it, check the Ethernet and power connections.)

Problem: **Some applications do not run properly when using the router.**

Solution: The router processes the data passing through it, so it is not transparent.

- If you are running a supported Windows operating system, ensure that the UPnP feature is enabled.
- If this does not solve the problem or your operating system does not support UPnP you can use the *DMZ* function. This should work with almost every application, but:

  - It is a security risk, since the firewall is disabled for the DMZ computer.

  - Only one (1) computer can use this feature.
- Another option is to use the Firewall Snooze Control feature to temporarily disable the firewall to allow the application to function unimpeded.

Contacting Technical Support

Before contacting technical support, please refer to the previous troubleshooting information. For issues concerning DSL service or connectivity, contact your Internet Service Provider (ISP) directly. If you are still unable to resolve the problem, be prepared to provide the following information:

- Internet Service Provider and service type (DSL, cable)
- Product model number (SpeedStream 5450)
- Date of purchase or installation
- Description of problem

Technical Support services are available via the Internet, e-mail and telephone:

Telephone: (972) 852-1000
Fax: (972) 852-1001
Email: infor.ssn@siemens.com
Internet: http://www.icn.siemens.com/subscriber

Appendix B

Specifications

Media Interface:	RJ-11 DSL WAN connection (5) 10/100Base-T RJ-45 Ethernet LAN connections (Auto-MDI/MDI-X) DB-9 RS-232 Serial console port
Diagnostic LEDs:	Power, Status, Link and Activity for DSL, and Ethernet
Management:	Intuitive, Web-based management Comprehensive hardware diagnostics SNMPv1 support UPnP IGD-NAT traversal support XML Management Scheme, DSL Forum 2002-281
Security:	PAP (RFC 1334), CHAP (RFC 1994) Password Authentication Access Control list Stateful Inspection Firewall with Denial of Service (DoS) protection Pre-configured firewall levels for ease of use with “Custom” level for advanced users Filter on source and/or destination IP address Filter on transport protocol and/or port number Firewall logging with Network Time Protocol support and Syslog support DMZ support and Firewall “Snooze” feature Content filtering ICSA compliancy mode
Standards Compliance:	IEEE 802.1d, 802.11g, 802.3, and 802.3u T1.413 issue 2 G.992.1 (G.DMT) G.992.2 (G.Lite)

Routing:	DHCP server and DNS agent Network Address Port Translation (NAPT) Network Address Translation (NAT) Packet filtering RFC 2364 Point-to-Point Protocol over ATM PVCs (PPPoA) RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE) RFC 2684 (formerly 1483) Bridged Ethernet and routed encapsulation RFC 2225 (formerly 1577) Classical IP over ATM PPPoE Relay/Bridging Configurable PAP and CHAP authentication TCP/IP with RIP1 and RIP2 or static routing on the LAN and/or WAN Dynamic DNS Support IP QoS (depending on configuration)
Bridging:	IEEE 802.1.d Transparent Learning Bridge (dynamic learning of up to 255 addresses) RFC 2684 (formerly 1483) Bridged Ethernet over ATM PVCs Spanning Tree support
AAL and ATM Support:	Up to 8 active VCCs across VPI 0-255, VCI 0-65535 address range ATM Forum UNI3.1/4.0 PVC ATM Traffic class: UBR, CBR, VBRnrt, VBRrt OAM F5
Power:	12V power supply included 1000mA max. output
Certifications:	FCC Part 15, Class B FCC Part 68 UL Listed CE certification CSA Industry Canada WHQL

Siemens Subscriber Network
4849 Alpha Road
Dallas, TX 75244 USA
(972) 852-1000 Tel
(972) 852-1001 Fax
info.ssn@siemens.com
http://www.icn.siemens.com/subscriber