

# **SpeedStream®**

---

## **Router User's Guide**

**Models 4100 and 4200**

Part No. 007-4035-001

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Siemens Subscriber Networks shall not be liable for technical or editorial errors or omissions in this document; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

### Siemens Subscriber Networks – End User Software License and Limited Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY SIEMENS SUBSCRIBER NETWORKS (SSN) 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 SSN DSL customer premises equipment ("Hardware") and the limited warranty that SSN 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, SSN 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 SSN, whether delivered via tangible media (CD ROM or floppy disk), down loaded from SSN 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 SSN.
- 7. Termination.** Without limiting SSN's other rights, SSN 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 SSN 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.** SSN 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.** SSN 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, SSN 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 SSN's exclusive obligation for breach of this limited warranty is, in SSN'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, whichever 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 SSN at (888) 286-9375, or send an email to SSN at support.ssn@siemens.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 SSN at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from SSN, the end user shall provide SSN with any missing items or, at SSN's sole option, SSN 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 SSN. Products that pass all functional tests will be returned to the end user.
  - D.** SSN will return the repaired or replacement Product to the end user at the address provided by the end user at SSN's expense. For Products shipped within the United States of America, SSN will use reasonable efforts to ensure delivery within five (5) business days from the date received by SSN. Expedited service is available at additional cost to the end user.
  - E.** Upon request from SSN, 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 SSN, including acts of nature and damage caused by shipping.

SSN 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 SSN authorized service provider.

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

SSN'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. SSN 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 SSN 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 SSN at the numbers provided above to determine the current out of warranty repair rate. End users seeking out of warranty repair should contact SSN 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 SSN 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 SSN 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 SSN.

SSN 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 SSN 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 SSN 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 SSN HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. SSN'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 SSN 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 SSN 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

<b>INTRODUCTION</b> .....	<b>3</b>
<b>Features of the SpeedStream® Router</b> .....	<b>3</b>
Network (LAN) Features .....	3
Security Features.....	3
Configuration & Management.....	4
Advanced Router Functions .....	4
<b>Minimum System Requirements</b> .....	<b>4</b>
<b>General Safety Guidelines</b> .....	<b>4</b>
<b>PHYSICAL INSTALLATION</b> .....	<b>5</b>
<b>Minimum System Requirements</b> .....	<b>5</b>
<b>Hardware Installation</b> .....	<b>5</b>
Basic Installation Procedure .....	5
Installing Line Filters .....	6
Connecting Cables .....	7
<b>OPERATING SYSTEM CONFIGURATION</b> .....	<b>9</b>
<b>Check TCP/IP Protocol Settings</b> .....	<b>9</b>
Checking TCP/IP Settings (Windows 9x/ME).....	10
Checking TCP/IP Settings (Windows 2000).....	11
Checking TCP/IP Settings (Windows XP) .....	12
Checking TCP/IP Settings (MAC OS 8.6 through 9.x) .....	13
Checking TCP/IP Settings (MAC OSX).....	14
<b>Internet Access Configuration</b> .....	<b>15</b>
For Windows 9x/2000 .....	15
For Windows XP .....	15
<b>SPEEDSTREAM ROUTER SETUP</b> .....	<b>16</b>
<b>Before Configuring the Router</b> .....	<b>16</b>
<b>Connecting to the Router</b> .....	<b>17</b>
Selecting PPP Connection.....	18
PPP Login .....	19
<b>Home Window</b> .....	<b>20</b>
<b>CONFIGURING USER PROFILES</b> .....	<b>21</b>
<b>Add User Profiles</b> .....	<b>21</b>
<b>Editing User Profiles</b> .....	<b>24</b>
<b>Deleting User Profiles</b> .....	<b>24</b>
<b>CONFIGURING ISP CONNECTION SETTINGS</b> .....	<b>25</b>
<b>WAN Interface</b> .....	<b>25</b>
<b>Host</b> .....	<b>26</b>
<b>DHCP</b> .....	<b>27</b>
<b>Static Routes</b> .....	<b>29</b>
<b>RFC2684</b> .....	<b>30</b>
<b>CONFIGURING NETWORK SETTINGS</b> .....	<b>31</b>
RIP (Routing Information Protocol).....	32
Port Forwarding .....	33
UPnP (Universal Plug and Play).....	34
Bridge Mode.....	35
Server Ports .....	36

---

Dynamic DNS .....	37
<b>CONFIGURING SECURITY FEATURES .....</b>	<b>38</b>
Admin User .....	39
<b>Time Client.....</b>	<b>40</b>
<b>NAT/NAPT Server.....</b>	<b>41</b>
<b>Firewall.....</b>	<b>42</b>
Level .....	43
Snooze.....	44
DMZ .....	45
Filter Rules.....	46
<b>Log.....</b>	<b>52</b>
<b>ADS.....</b>	<b>53</b>
<b>MONITORING ROUTER HEALTH.....</b>	<b>55</b>
<b>Status and Statistics.....</b>	<b>55</b>
System Summary .....	56
System Log.....	56
<b>Diagnostics.....</b>	<b>59</b>
<b>Tools.....</b>	<b>60</b>
Interface Map .....	60
Reboot .....	61
Update .....	62
<b>TROUBLESHOOTING.....</b>	<b>63</b>
<b>Basic Troubleshooting Steps .....</b>	<b>63</b>
<b>Interpreting the LED Display.....</b>	<b>64</b>
<b>Resolving Specific Issues.....</b>	<b>65</b>
POST Failure (red <i>pwr</i> LED).....	65
<b>Contacting Technical Support.....</b>	<b>66</b>
<b>FIREWALL SECURITY LEVELS .....</b>	<b>67</b>

---

## Chapter 1

# 1

## Introduction

Congratulations on the purchase of the SpeedStream® Router with SecureRoute™ SpeedStream® Router (Router) is a powerful yet simple communication device for connecting your computer or local area network (LAN) to the Internet. This manual covers the SpeedStream models 4100 and 4200.



SpeedStream 4100 (Ethernet)



SpeedStream 4200 (Ethernet and USB)

## Features of the SpeedStream® Router

Your Router provides high-speed Internet and corporate network access to homes, networked home offices, and small offices. In addition, if you are working from a branch office, the Router provides a fast and effective means of communicating over a remote LAN with the main office. The Router can also be used to connect the corporate LAN to the Internet over the WAN.

### Network (LAN) Features

- **Ethernet Switch**  
Ethernet connectivity (all models) to the Internet or network through a network interface card (NIC), providing full 10/100 megabits per second (Mbps) bandwidth to the port.
- **USB Connection**  
Universal Serial Bus (USB) connection (4200 model) providing added flexibility for connecting your computer via the Ethernet or USB port.
- **Support of G.lite and Full-Rate DsL**  
Ensures compatibility with most DSL networks.

### Security Features

- **Password-protected Configuration**  
Password protection prevents unauthorized users from modifying the Router's configuration settings.
- **Firewall Security**  
Firewall security with four conveniently pre-set standard levels of security (Off, Low, Medium, High), an ICSA-compliant mode, and a custom setting for advanced users.
- **NAT Protection**  
Network Address Port Translation (NAPT) and a secure firewall to protect your data while your computer is connected to the Internet.
- **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.

- **Virtual Private Network**

Virtual Private Network allows remote users to establish a secure connection to a corporate network by setting pass-through of the three most commonly used VPN protocols: PPTP, L2TP, and IPSec.

## 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.

- **Port Forwarding**

Port Forwarding provides flexibility by allowing you to change internal IP addresses without affecting outside access to your network.

- **Session Tracking**

Some protocols, such as FTP, require secondary network connections on ports other than the main control port. These connections are usually made using port numbers in the dynamic range (> 1024). The firewall allows traffic on secondary sessions without manual configuration.

## 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.

- **Ethernet connection method**

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

- **USB connection method**

- 32 MB RAM
- Pentium-compatible 166 MHz processor (or faster).
- 12 MB available hard disk space.
- Windows 98 or later operating system.

## General Safety Guidelines

When using the SpeedStream Router, observe the following safety guidelines:

- Never install telephone wiring during a storm.
- Avoid using a telephone during an electrical storm. Lightning 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.

---

## Chapter 2



# Physical Installation

*This chapter covers the physical installation of the SpeedStream Router.*

## Minimum System Requirements

- DSL service and an Internet access account from an Internet Service Provider (ISP).
- Network cables for the device you intend to connect to the Router. Use standard CAT5 Ethernet cables with RJ45 connectors.
- TCP/IP network protocol must be installed on all computers.
- For USB connection to the Router, the following operating systems are supported (if your Router model supports USB):
  - Windows 98, 98SE
  - Windows 2000
  - Windows ME or XP
  - Mac OS versions 8.6 through 10.2.4

**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 SpeedStream 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. [Install USB drivers if necessary.](#)
4. [Configure network settings on your computer.](#)
5. [Configure the Router via the Web-based management interface.](#)
6. 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.

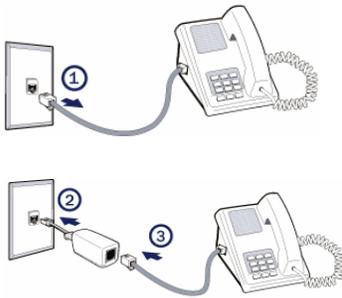
## Installing Line Filters

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.

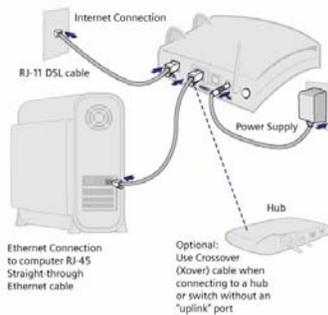
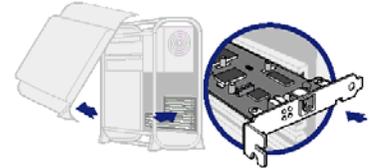
## Connecting Cables

The Router provides ports for either a USB or an Ethernet connection to your primary computer. Select the interface you will use to connect the Router, and follow the step-by-step instructions below for your chosen installation method.

### Ethernet Installation Method

To connect the SpeedStream 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

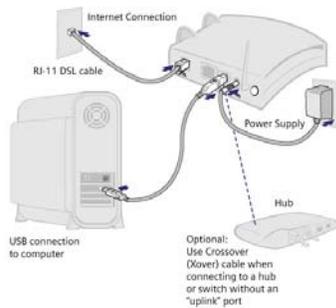
- 1) Connect the power adapter to the rear of the Router.
- 2) Plug the power adapter into the electrical wall outlet.
- 3) Flip the power switch to power on the SpeedStream Router.
- 4) Power on all connected computers.

#### 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.

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 [Chapter 3, Operating System Configuration](#).

## USB Installation Method (Microsoft Windows)



### 1. Connect the USB Cable

- 1) With your computer off, connect the provided USB cable to the USB port on the Router.
- 2) Connect the other end of the USB cable to an open USB port on your computer.
- 3) If desired, use standard 10/100 CAT5 Ethernet cables to connect additional computers to the 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. Install USB Driver Software

- 1) Insert the USB driver CD-ROM into the CD-ROM drive of your computer.
- 2) When prompted, follow the on-screen instructions to complete the driver installation.

### 5. Check the LEDs

- 1) The DSL, USB, and Power LEDs should be lit.

You can now configure the TCP/IP settings as detailed in [Chapter 3, Operating System Configuration](#).

## USB Driver Installation (Macintosh Systems)

When using the USB installation method on a Macintosh, follow these steps to install the USB drivers:

1. Insert the SpeedStream Installation CD into your CD-Rom drive.
2. Open the SpeedStream icon from the desktop.
3. Click Readme.txt to open it.
4. Follow the directions in the Readme.txt file.

You can now configure the TCP/IP settings as detailed in [Chapter 3, Operating System Configuration](#).

---

## Chapter 3

# Operating System Configuration

*This chapter explains how to configure your computer to work with the Router.*

To access the Internet through the SpeedStream Router, the TCP/IP protocol must be installed on your computer. If TCP/IP is not already installed on your computer, refer to your system documentation or online help for instructions. Once installed, you should [check the TCP/IP protocol settings](#) to make sure they are correct for use with the Router.

Once TCP/IP is installed and configured properly, the next step is to [configure your computer to use the Router for Internet access](#) by configuring the Web browser to access the Internet via the LAN rather than by a dial-up connection.

### 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 SpeedStream Router are:

IP Address:	192.168.254.254
Subnet Mask:	255.255.255.0

If using the default Router settings and the default Windows TCP/IP settings, you do not need to make any changes.

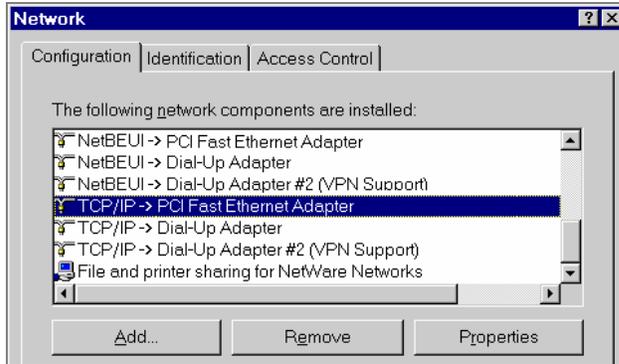
By default, the Router will act as a DHCP server, automatically providing a suitable IP address and related information to each computer when the computer boots up. For all non-server versions of Windows, the TCP/IP setting defaults to act as a DHCP client.

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

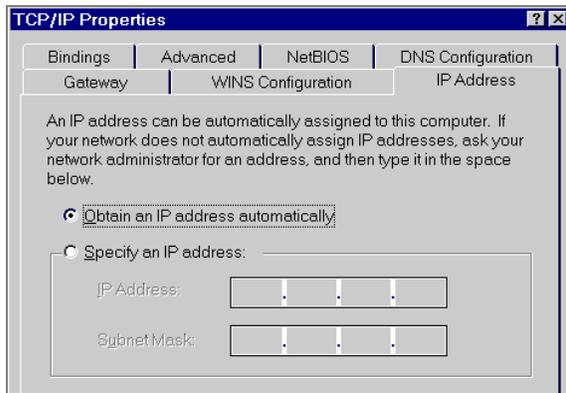
- [Windows 9x/ME](#)
- [Windows 2000](#)
- [Windows XP](#)
- [MAC OS 8.6 through 9.x](#)
- [MAC OSX](#)

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

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



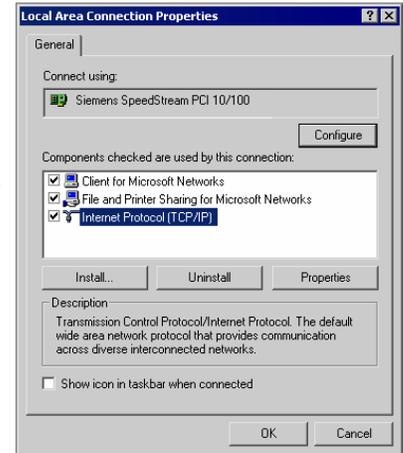
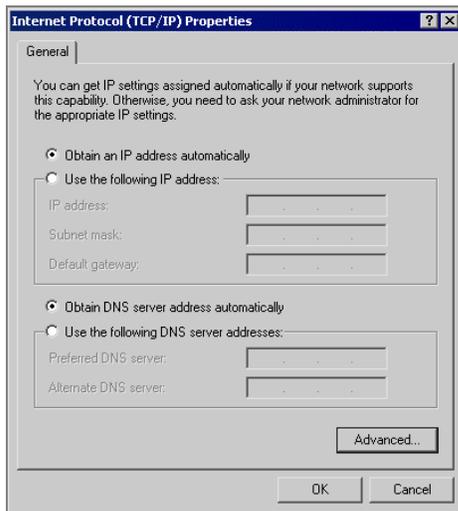
2. Select the TCP/IP protocol for your network card.
3. Click **Properties**. This displays the “TCP/IP Properties” window.



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)

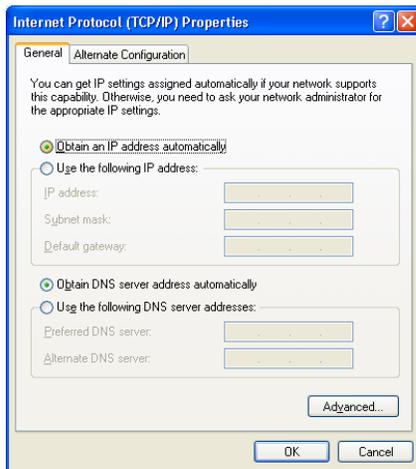
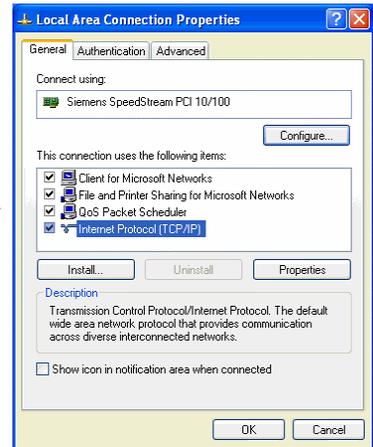
1. On the Windows taskbar click **Start>Settings>Control Panel**. This displays the "Control Panel" window.
2. Double-click **Network and Dial-up Connections**. This displays the "Network and Dial-up Connections" window.
3. Right-click **Local Area Connection** and select Properties. This displays the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

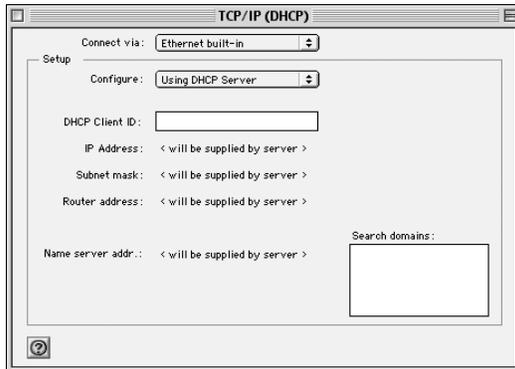
1. On the Windows taskbar click **Start>Control Panel**. This displays the "Control Panel" window.
2. Double-click the **Network Connection** icon. This displays the "Network Connections" window.
3. Right-click **Local Area Connection**, then click **Properties**. This displays the "Local Area Connection 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.



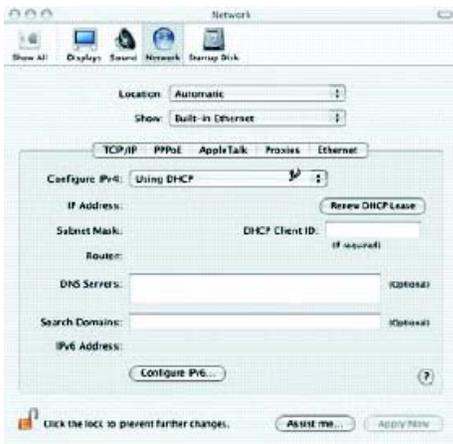
2. Select one of the following from the **Connect via** drop-down menu.
  - **Ethernet** or **Ethernet built-in** if connecting via Ethernet.
  - **Ethernet Adaptor [en0,en1,...]** if connecting via USB.
3. Select **Using DHCP Server** from the **Configure** drop-down menu.
4. Close the “TCP/IP window” 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 one of the following from the **Show** drop-down menu:
  - **Built-in Ethernet** if connecting via Ethernet.
  - **Ethernet Adaptor [en0,en1,...]** if connecting via USB.
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 provides details for the Router setup processes.*

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

To do this:	Refer to:
Configure users on the Router.	<a href="#">Chapter 5, "Configuring User Profiles"</a>
Configure ISP configuration parameters. This should only be done when instructed by your ISP.	<a href="#">Chapter 6, "Configuring ISP Connection Settings"</a>
Configure network related information.	<a href="#">Chapter 7, "Configuring Network Settings"</a>
Add security to your network.	<a href="#">Chapter 8, "Configuring Security Features"</a>
Monitor the health of the Router.	<a href="#">Chapter 9, "Monitoring Router Health"</a>

## 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 either the USB or Ethernet port on the Router.
- The SpeedStream 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.

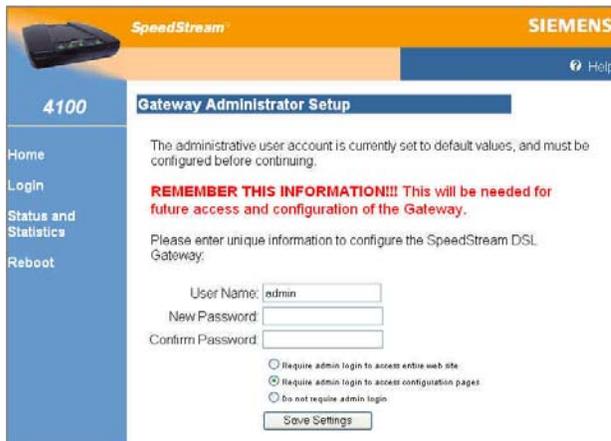
From this point on, you will perform all configuration of the SpeedStream Router from your computer using the Web browser-based setup program.

## Connecting to the Router

The SpeedStream Router contains an HTTP server that allows you to connect to the Router 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 Router:

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, enter the default router IP address: **http://speedstream** and press **Enter**. This displays the "Gateway Administrator Setup" window.



The first time you connect to the Router via the Web browser, you must set up an administrator account on the "Gateway Administrator Setup" window before you can proceed.

4. Specify a user name for the administrator. You may accept the default user name, **admin**, or enter a new user name in **User Name**. The user name is case-sensitive.
5. Enter a password in **New Password**; then enter the same password in **Confirm New Password**. The password field is case-sensitive.
6. Select a login security level from one of the following:
  - **Require admin login to access entire Web site**  
Before you can access any screen in the Web interface, you must log in with your network user name and password. (Security level = High)
  - **Require admin login to access configuration pages**  
Before you can access any screen in the Web interface that allows you to make configuration changes, you must log in with your network user name and password. (Security level = Medium)
  - **Do not require admin login:**  
After you log in for the first time, you will not be required to log in again at any screen. (Security level = Low)
7. Click **Save Settings**. Depending on your connection(s), one of the following screens will display:
  - If you have no Point-to-Point (PPP) connections configured, the **System Summary** screen is displayed.
  - If you have one Point-to-Point (PPP) connection configured, the PPP **Login** screen for that connection is displayed. Refer to [PPP Login](#) for more details.

- If you have multiple Point-to-Point (PPP) connections configured, the **PPP Login [choose connection]** screen displays the available connections. Refer to [Selecting PPP Connection](#) for more details.

Point-to-Point offers the Connect on Demand feature whereby the router will attempt to log on to a disconnected PPP session if there is requested traffic from the LAN side, and if there is a saved user name and password. This is especially useful with the Idle Timeout feature. Connect on Demand is non-configurable, but is always enabled.

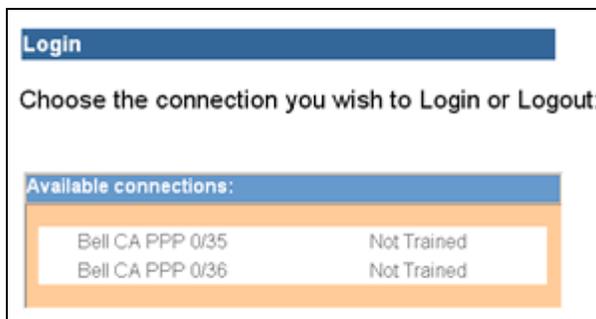
8. If you selected either option that requires admin login, you will be required to log in again before you are permitted to perform any activity. When you select any menu option the following login window is displayed.



9. Enter the user name and password you assigned to the administrator to perform the remaining configuration activities.
10. Click **OK**. This displays the screen for the menu option you selected.
11. Refer to the following chapters for details on configuring and managing the SpeedStream Router.

## Selecting PPP Connection

If you have configured multiple PPP (Point-to-Point) sessions on your computer, the “Login” window showing the available PPP connections is displayed after you log on using the “Administrative User Setup” window.



Click the connection you wish use.

## PPP Login

If you have configured only one PPP (Point-to-Point) session on your computer, the "Login" window for that PPP connection is displayed after you log on using the "Administrative User Setup" window.

1. Front the PPP **Login** window, enter the **Username** and **Password**.
2. To save the settings so you won't be asked for the user name and password in the future, click **Save Settings on Connect**.
3. To configure additional PPP options, click **Show Options**. This expands the window to show configurable options for the PPP connection.

4. Specify any desired PPP options from the following:
  - **Access Concentrator**  
Enter the name of the access concentrator as provided by your ISP.
  - **Service Name**  
Enter the service name provided by your ISP.
  - **Auto-Connect on Disconnect**  
If selected, the Router will attempt to login every time the DSL trains if you selected **Save Settings on Connect**.
  - **Idle Timeout (with time value)**  
Select to disconnect the PPP session if the router has had no traffic for a specified amount of time. Enter the time in minutes. (This option cannot be used with Autoconnect.)

## Home Window

After initial startup, the “Home” window is displayed on startup.

The screenshot shows the SpeedStream 4100/4200 router's Home window. The top bar includes the SpeedStream logo and SIEMENS branding. A left sidebar contains navigation options: Home, Login, Setup, Status and Statistics, Diagnostics, and Tools. The main content area displays system information and a table of RFC2684 connections.

System Summary		
<b>System Type:</b>	SpeedStream 4100/4200-Series	
<b>Config Part #:</b>	003-0045-INT	
<b>Firmware Part #:</b>	004-D240-INT	
<b>MAC Address:</b>	00:0B:23:8F:E9:10	
RFC2684 Connection Summary:		
B	2684(0) 0/32	DOWN
B	2684(1) 0/33	DOWN
B	2684(2) 0/34	DOWN
B	2684(3) 0/35	172.16.102.132
B	2684(4) 0/36	DOWN
B	2684(5) 0/37	DOWN
B	2684(6) 0/38	DOWN
B	2684(7) 0/39	DOWN

In the left navigation pane of the “Home” window, there are configuration, diagnostic, status and statistic options for the Router. The list of options displayed differs depending on how a user is logged into the system. An administrator has full configuration rights (shown above) so will see a complete set of options, while a user has limited configuration rights and will see the subset specified for that user profile.

Refer to the following chapters for information on how to use each of these options.

- Refer to [Chapter 5, “Configuring User Profiles”](#), for details on adding, modifying, or deleting user profiles.
- Refer to [Chapter 6, “Configuring ISP Connection Settings”](#), for details on setting ISP configuration parameters. This should only be done when instructed by your ISP.
- Refer to [Chapter 7, “Configuring Network Settings”](#), for details on configuring network related information.
- Refer to [Chapter 8, “Configuring Security Features”](#), for details on adding security to your network.
- Refer to [Chapter 9, “Monitoring Router Health”](#), for details on viewing network statistics and connection status.

---

# Chapter 5

## Configuring User Profiles



*This chapter contains details for configuring users on the SpeedStream Router.*

User profiles are used as a means for controlling Router and network access by individual users. Access to the configuration and management of the Router should be restricted to authorized users only. This chapter describes how to:

- [Add user profiles](#)
- [Edit user profiles](#)
- [Delete User Profiles](#)

### Add User Profiles

To add a new user profile:

1. Select **Setup>User Profiles** from the left navigation pane of the Web interface. This displays the “Current Profiles” window. User profiles are added using a Wizard accessed from this window.



2. Optionally select the **Force all users to be identified before surfing** option.
3. Click **New Profile**. This displays the “Profile User Information” window.



4. Enter a **Username** for the user.
5. Optionally enter a **Password** for the user and **Confirm** it.

6. Click **Next**. This displays the “Profile Content Filtering” window. Content filtering restricts access to undesirable Web sites and Web content.



7. 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.

8. 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 and click **Add Entry**. The system responds by adding the word or Web address to the Website word/name table. This can be done multiple times to add different entries to the table.
9. **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.
10. 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.



11. Optionally do one of the following:

- Click one or more of the available features permitting the user to access that feature. This places a checkmark in the corresponding box. (Click again if you want to remove the checkmark and deny access).
- Click **All Items** to select all features in the list.
- Click **Reset** to clear all selected items and deny the user access to those feature.

12. Click **Next**. This displays the “Profile Security Access” window.



13. Click one of the following:

- **Require admin login to access configuration pages**  
User must login as admin to change the Router configuration. This is the recommended setting.
- **Do not require admin login**  
User will be able to change the Router configuration without a password.

14. Click **Next**. This displays the “Constant Profile IP Address” window.



15. Optionally enter an **IP Address** to always be associated with this profile.

16. Click **Next**.

17. This completes the User Profile Wizard. Click **Finish** to close the Wizard and return to the “Current Profiles” window.

## Editing User Profiles

This section describes how to edit a user.

To edit a user:

1. Select **Setup>User Profiles** from the left navigation pane of the Web interface. This displays the “Current Profiles” window.



2. Click the name of the user you want to change. This displays the “Profile User Information” window. Make any desired changes.
3. Click **Next** to get to the next window you want to change. Make any desired changes.
4. Click **Finish** at any time when you are done making changes.

## Deleting User Profiles

This section describes how to delete a user.

To delete a user:

1. Select **Setup>User Profiles** from the left navigation pane of the Web interface. This displays the “Current Profiles” window.



2. Click the **Delete** button next to the name of the user you want to delete.

## Chapter 6

# 6

# Configuring ISP Connection Settings

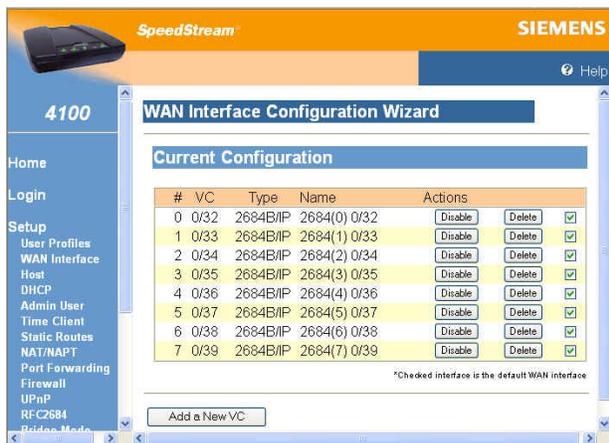
This chapter describes how to set advanced ISP configuration settings. The options in this section should only be configured with the help and guidance of your ISP. Incorrect changes to any of these options could result in the failure of your Internet connection.

The ISP connection options are listed below.

- [WAN Interface](#) Wizard for configuring the WAN Interface. The information requested by the Wizard should be supplied by the service provider.
- [Host](#) Configure the basic networking attributes of the Router (the host).
- [DHCP](#) Configure and control Dynamic Host Configuration Protocol (DHCP) and DNS functionality.
- [Static Routes](#) Add and monitor static IP routes assigned by your ISP. The routing functionality of the Router supports both Dynamic Routing and Static Routing. Static routing pertains to those routes between network-connected hosts that do not change over time.
- [RFC2684](#) Configure WAN-side DHCP functionality for RFC2684 based connections.

## WAN Interface

Connectivity to the Wide Area Network (WAN) is achieved by means of one or more Virtual Circuits (VC). Virtual Circuits are configured using the WAN Interface Configuration Wizard. The information requested by the Wizard should be supplied by the service provider.

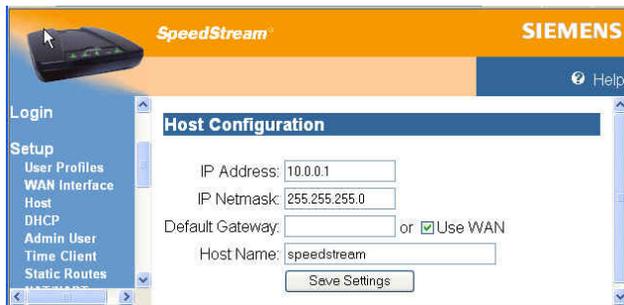


## Host

Host configuration attributes identify the Router on the network and, optionally, specify a default "gateway" to the Wide Area Network (WAN). Default values for many host IP address, netmask, default router and host name are automatically generated for the SpeedStream Router and should not be changed unless directed by your ISP. The ISP may ask you to change this information if, for example, you are assigned a static IP address.

To specify host configuration settings:

1. Select **Setup>Host** from the left navigation pane of the Web interface. This displays the "Host Configuration" window.



2. Change settings as specified by your ISP.
3. Click **Save Settings**. This displays a confirmation screen displays notification that the new setting will not take affect until you reboot the router. You may do so at this point or later.

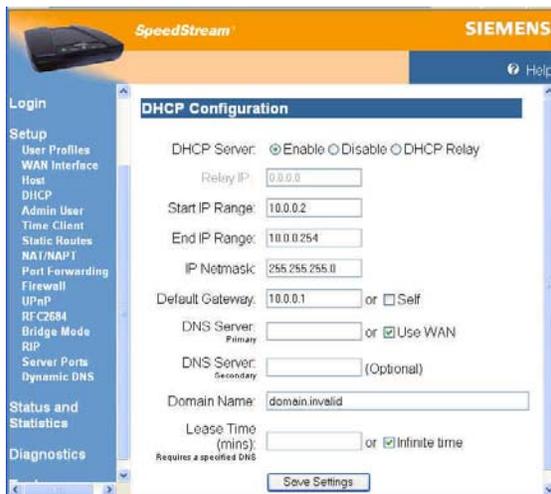
## DHCP

DHCP, the Dynamic Host Configuration Protocol, describes the means by which a system can connect to a network and obtain the necessary information for communication upon that network. Do not change the default DHCP Configuration settings unless directed by your ISP.

**Note:** All addresses must be entered as an IPv4 subnet mask in dotted-decimal notation (for example, 255.255.255.0).

To configure the DHCP feature:

1. Select **Setup>DHCP** from the left navigation pane of the Web interface. This displays the “DHCP Configuration” window.



2. Select one of the following:

- **Enable**

The Router will operate as a DHCP server to handle DHCP requests received from connected LAN-side hosts (DHCP clients). The DHCP server does not serve WAN-side DHCP clients.

The DHCP operating mode defaults to **Enable**, and the system auto-generates the current IP address range, IP netmask, and default router. Do not change these default settings unless directed by your ISP.

- **Disable**

Disables DHCP. If you are using a static IP address, you may need to disable DHCP and enter different addresses in the text boxes.

- **DHCP Relay**

Instead of getting an IP address from the Router, the IP address is gotten from the computer as defined in **Relay IP**. Used when DHCP information is received from a DHCP server on the WAN side. DHCP requests are forwarded to the WAN side to **Relay IP**, and DHCP responses are forwarded back to the LAN side.

3. In **Start IP Range**, enter the beginning IP address of the range of addresses from which the DHCP server will lease to requesting DHCP clients.

4. In **End IP Range**, enter the ending IP address of the range of addresses from which the DHCP server will lease to requesting DHCP clients.

This range definition should consider the following address restrictions:

- The range of IP addresses may extend over only one IP subnet.
- The maximum size of the address pool that may be managed by the DHCP server is 64. Therefore, the range of addresses must not exceed 64.
- The range of IP addresses should not include any IP address maintained internally by your SpeedStream device for other purposes. This includes the device's LAN-side static IP address, as well as the Default Router IP address, Primary or Secondary DNS IP addresses, and Primary or Secondary Relay IP addresses.

- Commonly used non-Internet routed IP address ranges include:

10.0.0.0	- 10.255.255.255
172.16.0.0	- 172.31.255.255
192.168.0.0	- 192.168.255.255

5. In **IP Netmask**, enter the IP subnet mask that corresponds to the range of IP addresses defined above.
6. In **Default Gateway**, do one of the following:
  - Enter the IP address of a default gateway, or router, to be provided to DHCP clients.
  - Click **Self** to specify that the SpeedStream Router is to be used as the default gateway.
7. In **DNS Server (primary)**, do one of the following:
  - Enter IP address of the primary Domain Name System (DNS) server to be provided to DHCP clients. A DNS server may be used by clients to resolve domain names to IP addresses.
  - Click **Use WAN** to specify that the address of the DNS server provided by your ISP is provided to DHCP clients on the LAN.
8. In **Domain Name**, optionally enter the DNS domain name for the DHCP server resident on your SpeedStream device. This value must be entered as an alpha-numeric string.
9. In **Lease Time**, do one of the following:
  - Enter the period of time an IP addresses leased from the DHCP server is valid. At the end of the lease period, the DHCP client will transmit a request to the server to extend the lease, at which time the server will extend the lease period of the IP address assigned to the client. If the lease period expires without the server receiving a request from the client to extend the lease, the server will assume the client's connection no longer exists. The server will release the IP address assigned to the client and return the address back to the pool of available addresses. (If you select this option, you must specify a DNS Server.)
  - Click **Infinite Time**:  
Leaves the lease time open-ended, preventing the server from releasing the IP address.
10. Click **Save Settings**.

## Static Routes

The SpeedStream DSL Router directs data traffic by “learning” source and destination information, then building a routing table. In some cases, network mappings cannot be learned because of incompatible addressing schemes. Sometimes a different source and destination path may be desired over the learned paths for example when your ISP assigns you a static route. In these situations, Static Routes can be configured to map a desired pathway.

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 a static route:

1. Select **Setup>Static Routes** from the left navigation pane of the Web interface. This displays the “Static Route Configuration” window.



2. Under **Add Route**, type the IP address of the destination device in the **Destination** box.
3. Type the net mask of the destination device in the **Net Mask** box.
4. Optionally, type the IP address where the data packets will be forwarded in the **Next Hop** box.
5. Select a connection type from the **Interface** drop-down menu. This is the interface that will forward the packets.
6. Click **Apply**. The system responds by adding your new route to the routing table.
7. You can repeat this procedure for each static route you wish to add.

**Note:** To edit a static route, click the **Edit** column for the static route you want to edit.

**Note:** To delete a static route, click the **Delete** column for the static route you want to delete.

## RFC2684

The SpeedStream Router supports two basic types of connections: Point-to-Point (PPP) and RFC2684.

By default, RFC2684 connections rely on a server located on the Wide Area Network (WAN) to supply the Router a dynamic IP address and other IP-based configuration parameters for the Router's WAN-side interface. To accomplish this, the Router executes a Dynamic Host Configuration Protocol (DHCP) client associated with the WAN-side connection. This client, in turn, communicates with the DHCP server located on the WAN.

Under some circumstances, this automated procedure may not be desirable or even possible. In such situations, you will need to disable the DHCP client on the router and manually define the required IP configuration parameters, as supplied by your service provider.

To configure RFC2684 functionality:

1. Select **Setup>RFC2684** from the left navigation pane of the Web interface. This displays the "RFC2684 Configuration" window.



2. Select the connection you want to configure from the **Connection** drop-down menu.
3. Select one of the following from **DHCP**:
  - **Enabled**  
Enables the Dynamic Host Configuration Protocol for the selected connection.
  - **Disable**  
Disables the Dynamic Host Configuration Protocol for the selected connection.
4. In **IP Address**, enter the IP address to be used for the WAN-side of the Router, normally obtained from a DHCP server located on the WAN.
5. In **IP Netmask**, enter the netmask corresponding to **IP Address**.
6. In **Default Gateway**, optionally enter the IP address of a router located on the WAN to be used as the "gateway" to the WAN.
7. In **DNS Server**, optionally enter the IP address of a DNS server located on the WAN to be used to resolve domain name/IP addresses.
8. Click **Save**.

---

## Chapter 7



# Configuring Network Settings

This section contains details for configuring network-related information. The network settings options are listed below.

- [RIP](#)                      Activate and control RIP functionality. 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.
- [Port Forwarding](#)        Control WAN-side access to LAN-side servers through private IP addressing.
- [UPnP](#)                      Configure and control UPnP interoperability and security.
- [Bridge Mode](#)             Configure the Router as a true WAN/LAN bridge.
- [Server Ports](#)            Specify server ports used by common applications such as HTTP (Web site traffic), FTP, and Telnet.
- [Dynamic DNS](#)            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.

## RIP (Routing Information Protocol)

By default, the SpeedStream Router does not support routing protocols. However, support for the Routing Information Protocol (RIP), versions 1, 2 or 1 and 2, can be activated. This support may be configured for any WAN connection currently configured or for the LAN in general.

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 is based on distance algorithms to calculate the shortest path using information in the routing table. The shortest path is based on the number of hops between two points.

To use the RIP option:

1. Select **Setup>RIP** from the left navigation pane of the Web interface. This displays the “RIP Configuration” window.



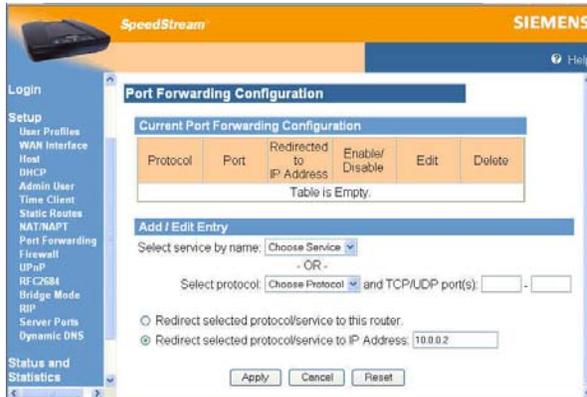
2. Select one of the following options from under the **RIP Version** heading next to the connection of your choice:
  - **1**: Provides essential RIP packet formatting for routing information packets.
  - **2**: Provides enhanced packet formatting for routing information packets by providing the following: 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.

## Port Forwarding

Port forwarding allows selected servers running on the LAN side of the router to be accessed from the WAN side. Requests from the WAN to a configured TCP or UDP port will be forwarded to the selected IP address on the LAN. NAT functionality ensures that the LAN-side server is known to the WAN only through the public IP address. The server's actual private IP address remains unknown to any WAN-side hosts.

To configure port forwarding:

1. Select **Setup>Port Forwarding** from the left navigation pane of the Web interface. This displays the "Port Forwarding Configuration" window.



2. Under **Add/Edit Entry**, do one of the following:
  - Select the service you want to configure from the **Select service by name** drop-down menu.
  - Select the protocol you want to configure from the **Select protocol** drop down menu. This can be TCP, UDP, ICMP, or GRE. If you select TCP or UDP you must also specify either a single port or range of ports that apply.
3. Select one of the following:
  - Redirect selected protocol/service to this router  
Select this option if you want inbound traffic forwarded to the SpeedStream.
  - Redirect selected protocol/service to IP address  
Select this option if you want inbound traffic forwarded to a host located on the LAN. In this case, you must specify the IP address of the host on which the server resides.
4. Click **Apply**.

## UPnP (Universal Plug and Play)

Microsoft UPnP allows the Router 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, where applicable. This communication between the operating system and Router 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, you must ensure that the UPnP component is installed on your computer and enabled.

To enable UPnP functionality:

1. Select **Setup>UPnP** from the left navigation pane of the Web interface. This displays the “UPnP Configuration” window.



2. Select one of the following control options.
  - **Disable UPnP**  
Prevents the Router 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 Router 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.
3. Select one of the following options:
  - **Enable access logging**  
Generates a system log message whenever an UPnP client accesses the router.
  - **Read-only mode**  
Restricts the kind of access an UPnP client can have into the router. Only requests in the UPnP protocol that query the status of the router are allowed. Any requests that could potentially modify the router's behavior are blocked.
4. Click **Apply** to accept the settings. This displays the “UPnP Finish” window.

## Bridge Mode

The Router supports two fundamental modes of operation with respect to connectivity between the Local Area Network (LAN) and the Wide Area Network (WAN): bridge/routing mode and bridge mode.

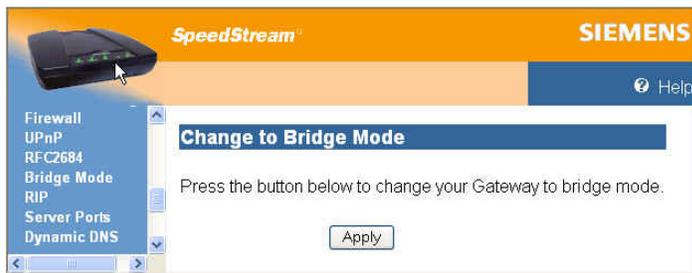
The default mode of operation is bridge/routing mode. With bridge/routing mode, the Router provides typical routing functionality between the WAN side and the LAN side. However, all LAN-side interfaces are "bridged."

The second mode of operation provides only "bridging" functionality. This applies to both WAN-to-LAN connectivity as well as to all LAN-side interfaces. Point-to-Point (PPP) connections are not available under the bridge mode of operation.

**Important!** If you switch to Bridge mode, you will lose access to the Web management interface and can only return to Router mode by resetting the Router to factory defaults.

To change to bridge mode:

1. Select **Setup>Bridge Mode** from the left navigation pane of the Web interface. This displays the "Change to Bridge Mode" window.



2. Click **Apply**.

## 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. Select **Setup>Server Ports** from the left navigation pane of the Web interface. This displays the “SpeedStream Gateway Server Ports” window.



2. Optionally, type a port number in the **HTTP** box. The default port for this field is 80.
3. Optionally, type a port number in the **FTP** box. The default port for this field is 21.
4. Optionally, type a port number in the **Telnet** box. 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.

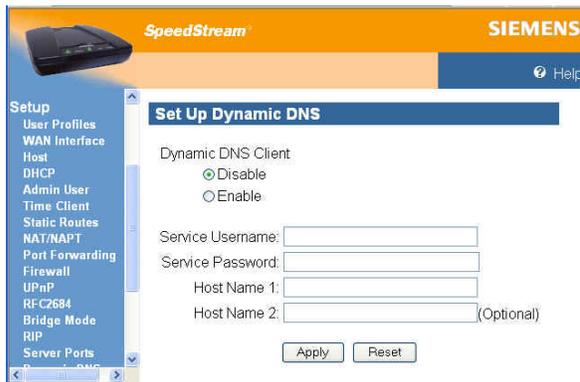
## Dynamic DNS

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](http://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. Select **Setup>Dynamic DNS** from the left navigation pane of the Web interface. This displays the "Set Up Dynamic DNS" window.



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

---

## Chapter 8



# Configuring Security Features

The Router provides broad security measures against unwanted users. Security also allows for the configuration of the firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration. The security options are listed below.

- [Admin User](#) Manage administrator login name and password.
- [Time Client](#) Configure network-based date and time functionality. An accurate date and time is of use when logging system and firewall events, and is a requirement for some firewall functionality (e.g., ICSA-compliant firewall operation).
- [NAT/NAPT](#) Configure and control IP addressing on the Local Area Network through either NAT or NAPT.
- [Firewall](#) Configure and control the internal firewall. Many of these features require a thorough understanding of networking principles and firewall operations. The firewall options are listed below.

## Admin User

The Administrator profile controls the requirements for logging into the Web interface and accessing configuration pages, as well as defining the administrator login name and password.

To configure administrator settings:

1. Select **Setup>Admin User** from the left navigation pane of the Web interface. This displays the "Gateway Administrator Setup" window.



2. Specify a user name for the administrator. You may accept the default user name, admin, or enter a new user name in **User Name**. The user name is case-sensitive.
3. Enter a password in **New Password**; then enter the same password in **Confirm New Password**. The password field is case-sensitive.
4. Select a login security level from one of the following:
  - **Require admin login to access entire Web site**  
Before you can access any screen in the Web interface, you must log in with your network user name and password. (Security level = High)
  - **Require admin login to access configuration pages**  
Before you can access any screen in the Web interface that allows you to make configuration changes, you must log in with your network user name and password. (Security level = Medium)
  - **Do not require admin login**  
After you log in for the first time, you will not be required to log in again at any screen. (Security level = Low)
5. Click **Save Settings**.

## Time Client

An accurate log timestamp is one of the requirements of the ICSA Labs firewall criteria (ver 3.0a). In order to maintain accurate timestamps in each log message, the firewall implements a Simple Network Time Protocol (SNTP) client. This allows the system to automatically synchronize its date and time with Coordinated Universal, the international time standard. The system date and time are set and corrected automatically via the designated server(s).

To configure the time client:

1. Select **Setup>Time Client** from the left navigation pane of the Web interface. This displays the “Time Client Configuration” window.



2. Select **Enable** from **Enable Time Client**.
3. In **Primary Server IP Address**, enter the IP address of the primary server to use as the time server (a “well-known” Network Time Protocol Server).
4. In **Secondary Server IP Address** enter the IP address of the secondary server to use as the time server if the router does not receive a response from the primary server.
5. In **Select Time Zone**, enter the time zone in minutes from UTC.
6. Click **Apply**.

## NAT/NAPT Server

Hosts located on a Local Area Network (LAN) are often required to use private IP addresses as opposed to public IP addresses. Private IP addresses, however, are not known on the public Wide Area Network (WAN). In order to expose LAN-side hosts assigned private IP addresses to the public WAN, the Router can be configured to use one of two methodologies: Network Address Translation (NAT) or Network Address Port Translation (NAPT). NAT can expose a single LAN-side host to the WAN; NAPT can expose multiple LAN-side hosts. NAT/NAPT functionality can be individually configured for each WAN connection.

To configure NAT/NAPT functionality:

1. Select **Setup>NAT/NAPT** from the left navigation pane of the Web interface. This displays the "NAT/NAPT Configuration" window showing the WAN Interface connections.



2. Select one of the following for the desired connection:
  - **NAT & NAPT Disabled**  
Disable both NAT and NAPT in order to, for example, to set up static routes assigned by your ISP.
  - **NAT Only Enabled**  
Enable NAT and specify the destination IP address for incoming packets. Depending on your configuration, NAT is sometimes enabled by default.
  - **NAPT Only Enabled**  
Use NAPT only to handle multiple addresses based on port forwarding rules.
  - **NAT&NAPT Enabled**  
Some service providers support a concurrent NAT/NAPT. Under this configuration, a single WAN interface may support multiple NAT connections with each NAT connection again exposing a single LAN-side host through a single WAN-side public IP address. Through either NAT or NAPT, the Router ensures that the LAN-side host is known to the WAN side only through the public IP address of the Router's WAN-side connection. The host's actual private IP address remains unknown to any WAN-side hosts or servers.
3. Click **Apply** when you have finished configuring all desired connections.

## Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall is designed to protect hosts located on the *Local Area Network* (LAN) from attacks initiated on the *Wide Area Network* (WAN). Protection is not provided for attacks initiated from the LAN. Due to the nature of firewall operations and the system resources required to service these operations, firewall operations may degrade the performance of the Router – especially under heavy network traffic loads.

The firewall menu item accessible from the left navigation pane of the Web interface expands to provide a list of options to be enabled or disabled as well as links to configure the more complex details of each security feature.

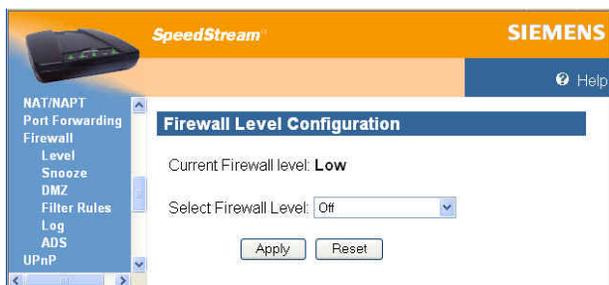
<a href="#">Level</a>	Set the firewall security level.
<a href="#">Snooze</a>	Temporarily disable the firewall. It is important to note that when the firewall is snoozing all protection provided by the firewall is disabled.
<a href="#">DMZ</a>	Configure firewall DMZ for controlling a virtual DMZ on the Local Area Network. The purpose of the DMZ is to redirect suspicious network traffic received from a public WAN to a secured LAN-side host dedicated to this purpose.
<a href="#">Filter Rules</a>	Add and delete custom inbound and outbound firewall rules.
<a href="#">Log</a>	View log listing of firewall activity including records of denial of access, reason codes, and descriptions.
<a href="#">ADS</a>	Configure what events the internal Attack Detection System (ADS) will protect against and log from a list of well-known attacks initiated on the Wide Area Network.

## Level

The firewall contained within the Router may be configured to operate in one of several modes, referred to as levels. For ease of use, three generic levels are preconfigured – Low, Medium and High. A separate level, ICSA 3.0a Compliant, is provided for those users who require compliance with the criteria set forth by ICSA Labs for firewall behavior. (Please refer to Appendix D, “Firewall Security Levels,” in the User Guide on CD-ROM for a detailed description of these preconfigured levels.)

In addition to the preconfigured levels, a Custom level is provided for advanced users who require the capability to define a unique custom set of firewall rules. To specify the firewall security level:

1. Select **Setup>Firewall>Level** from the left navigation pane of the Web interface. This displays the “Firewall Level Configuration” window.



2. Select one of the following from the **Select Firewall Level** drop-down menu.

- **Off**  
No restrictions are applied to either inbound or outbound traffic. In addition, Network Address Port Translation (NAPT) functionality is disabled. Because there is no address/port translation when the firewall is placed in this mode, all LAN-side connected hosts must be assigned a valid public IP address.
- **Low**  
Minimal restrictions with respect to outbound traffic. Outbound traffic is allowed for all supported IP-based applications and Application Level Routers (ALGs). The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host.
- **Medium**  
Moderate restrictions with respect to outbound traffic. Outbound traffic is allowed for most supported IP-based applications and Application Level Routers (ALGs). The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host.
- **High**  
High restrictions with respect to outbound traffic. Outbound traffic is allowed only for a very restricted set of supported IP-based applications and ALGs. The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host and permitted by this firewall mode.
- **ICSA 3.0a-compliant**  
Supports the ICSA Labs criteria for firewall behavior. (For more information, visit the ICSA site at <http://www.icsalabs.com>).
- **Custom**  
Allows advanced users to add, modify, and delete their own firewall rules. If you select this option, you must set customized rules for both inbound and outbound traffic using the IP Filtering option.

3. Click **Apply**.

## Snooze

The snooze feature allows you to temporarily disable 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. **Note: Important!** 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 **Setup>Firewall>Snooze** from the left navigation pane of the Web interface. This displays the "Firewall Snooze Control" window.



2. Select one of the following:
  - **Disable Snooze**  
Disables all snooze control. In this mode, the firewall is not disabled.
  - **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.
3. Click **Apply**.

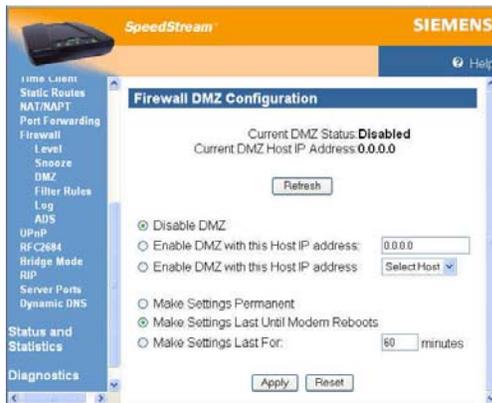
## DMZ

The firewall supports virtual DMZ in single (LAN) port router models. Virtual DMZ redirects traffic to a specified IP address rather than a physical port. Because this redirection is a logical application rather than physical, it is called “virtual DMZ.”

Using virtual DMZ, a single node on the LAN can be made “visible” to the WAN IP network. Any incoming network traffic not handled by port forwarding rules is automatically forwarded to an enabled DMZ node. Outbound traffic from the virtual DMZ node circumvents all firewall rules. 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. Under this mode of operation all network traffic received from the WAN that is not destined for a host specifically exposed through NAT or for a server exposed through Port Forwarding will be redirected to the designated DMZ host. 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 **Setup>Firewall>DMZ** from the left navigation pane of the Web interface. This displays the “Firewall DMZ Configuration” window.



2. 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 menu.
3. 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.
4. Click **Apply**.

## Filter Rules

If the firewall security level is set to Custom, this feature allows you to specify a unique set of firewall rules for handling inbound and outbound traffic customized to the user's specific requirements. In this mode of operation the firewall provides an extensive amount of configurability. As such, only advanced users should employ this feature.

Rules can be filter-based on any of the following:

- Source and destination router interfaces
- IP protocols
- Direction of traffic flow
- Source and destination network/host IP address
- Protocol-specific attributes such as ICMP message types
- Source and destination port ranges (for protocols that support them), and support for port comparison operators such as less than, greater than, and equal to.

Rules can specifically allow or deny packets to flow through the router. Default actions taken when no specific rule applies can also be configured.

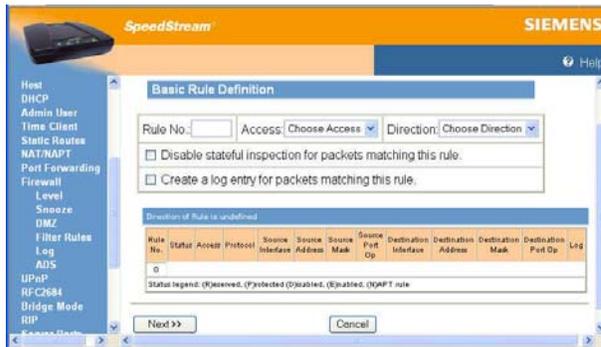
To define inbound and outbound IP filter rules:

1. Select **Setup>Firewall>Filter Rules** from the left navigation pane of the Web interface. This displays the "Firewall IP Filter Configuration Wizard" window.



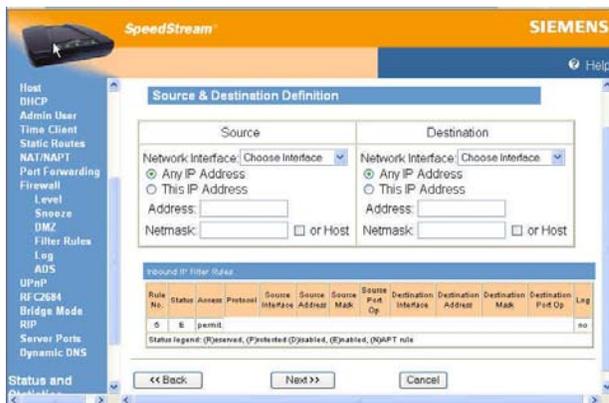
2. Do one of the following:
  - To add new IP filter rules as you define them, click **Add New IP Filter Rule**. This displays the "[Basic Rule Definition](#)" window.
  - To clone IP filter rules already defined, click **Clone IP Filter Level**. This displays the "[Clone Rule Definition](#)" window. Once cloned, you can modify the existing rules.

## Creating Custom IP Filter Rules



To add a new rule:

1. Type up to a five digit numeric value in the **Rule No** box 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 the **Disable stateful inspection for packets matching this rule** to prevent the firewall from creating a stateful inspection session for packets matched on this rule.
5. Optionally, select the **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 & 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.
  - Or, 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.
  - Or, 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

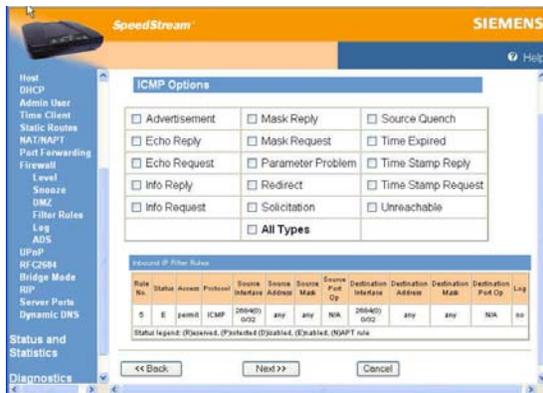
The "TCP/UDP Options" window is displayed if you select TCP or UDP protocol from the "[Protocol Definition](#)" window. If you selected either of these protocol types, you must identify the source and destination ports.



- 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.
- Optionally, select the **Check TCP syn packets** checkbox if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
- Click **Next**.
- 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 the **All Types** checkbox 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. Click **Clone IP Filter Level** from the “Firewall IP Filter Configuration Wizard” window. This displays the “Clone Rule Definition” window.

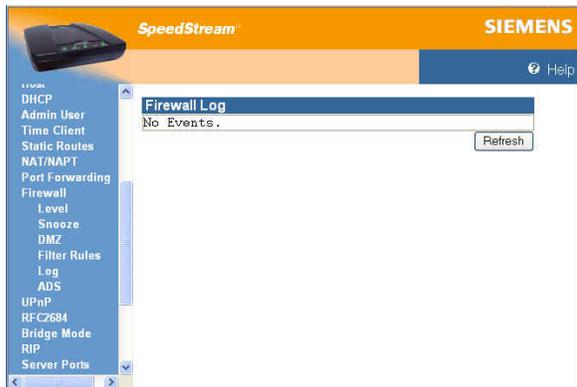


2. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
  - **Low**  
Clones low-level IP filter rules.
  - **Medium**  
Clones medium-level IP filter rules.
  - **High**  
Clones high-level IP filter rules.
3. Click **Apply**. This displays the “Firewall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

## Log

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

To view the firewall log, select **Setup>Firewall>Log** from the left navigation pane of the Web interface. This displays the "Firewall Log" window.



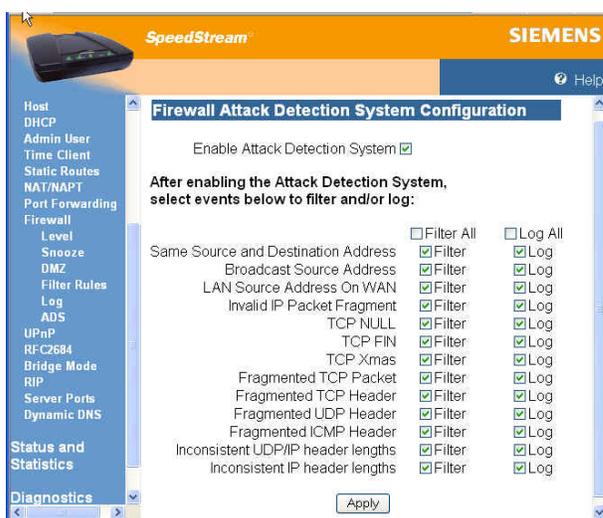
## ADS

The firewall provides an advanced Attack Detection System (ADS) that may be used to detect and identify various types of attacks initiated on the Wide Area Network (WAN). The system has the capability to detect such attacks the moment they start and to protect the Local Area Network (LAN) from such attacks.

If the Attack Detection System is enabled, the SpeedStream 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 **Setup>Firewall>ADS** from the left navigation pane of the Web interface. This displays the "Firewall Attack Detection System" window.



2. Select **Enable Attack Detection**.
3. Select the **Filter** checkbox for each event in the list you want to filter or, if you want to filter all events, select the **Filter All** checkbox. This provides maximum protection against malicious intrusion from outside your network.
4. Select the **Log** checkbox for each event in the list you want to log or, if you want to log all events, select the **Log All** checkbox. When logging is selected for a particular offending packet, the ADS will write an entry to the firewall log once a minute for as long as the attack persists. This shows that a long-term attack is taking place without completely filling up the firewall log with entries for every single packet.
5. 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.

---

## Chapter 9

# 9

# Monitoring Router Health

*This chapter describes how to monitor the health of the Router.*

The Router health options listed below are used to gauge the Router's health.

<a href="#">Status and Statistics</a>	View Internet, home networking, security statistics, system and firewall log files.
<a href="#">Diagnostics</a>	Run a diagnostic program against a selected connection on your Router.
<a href="#">Tools</a>	Reset, reboot, or update firmware.

## Status and Statistics

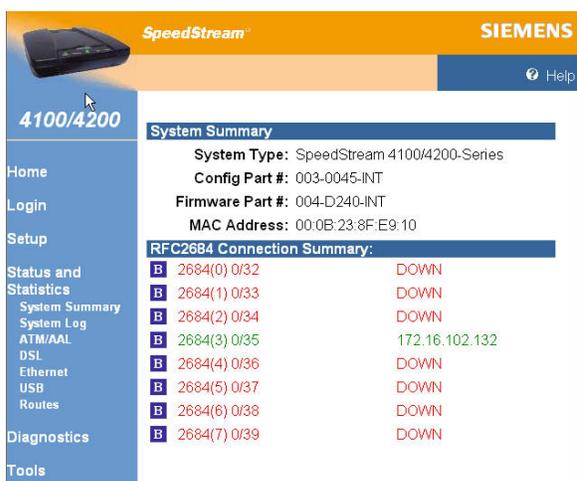
You can display statistics for the Internet, Home Networking, Security, and Logging.

<a href="#">System Summary</a>	Basic descriptive information that identifies the router.
<a href="#">System Log</a>	Displays a record of all system activity, including what actions were performed, what packets were dropped and what packets were forwarded.
<a href="#">ATM/AAL</a>	Displays status information about the ATM connection.
<a href="#">DSL</a>	Displays status information about the DSL connection.
<a href="#">Ethernet</a>	Displays status information about the Ethernet connection.
<a href="#">USB</a>	Displays status information about the USB connection.
<a href="#">Routes</a>	Displays status information about the current routing table.

## System Summary

The “System Summary” window provides basic descriptive information that identifies the router, system type, current software and firmware versions, the MAC address (unique device identifier), and the status of currently configured connections.

Connection information includes the identification and current status of configured point-to-point (PPP) and static connections. Select **Status and Statistics>System Summary** from the left navigation pane of the Web interface to view this information.



**System Summary**

System Type: SpeedStream 4100/4200-Series  
 Config Part #: 003-0045-INT  
 Firmware Part #: 004-D240-INT  
 MAC Address: 00:0B:23:8F:E9:10

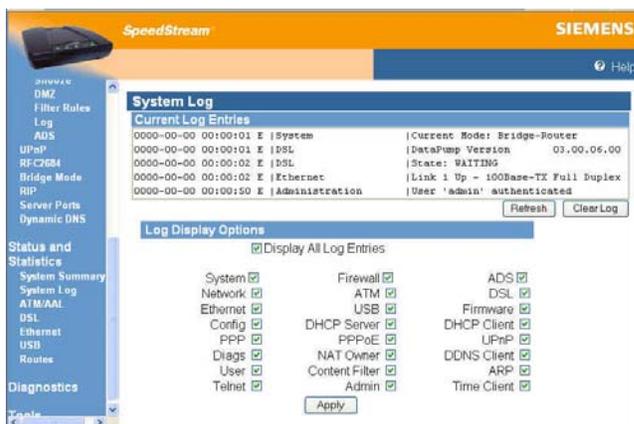
**RFC2684 Connection Summary:**

ID	Name	Status
2684(0)	0/32	DOWN
2684(1)	0/33	DOWN
2684(2)	0/34	DOWN
2684(3)	0/35	172.16.102.132
2684(4)	0/36	DOWN
2684(5)	0/37	DOWN
2684(6)	0/38	DOWN
2684(7)	0/39	DOWN

## System Log

The “System Log” window displays a record of all system activity, including what actions were performed, what packets were dropped and what packets were forwarded. This information allows you to make informed decisions about the need to add new filter rules.

The System Log contains a maximum of 200 entries; each entry may contain a maximum of 200 characters. Select **Status and Statistics>System Log** from the left navigation pane of the Web interface to view the “System Log” window.



**System Log**

Current Log Entries

0000-00-00 00:00:01 E  System	Current Mode: Bridge-Router
0000-00-00 00:00:01 E  DSL	DataPump Version: 03.00.06.00
0000-00-00 00:00:02 E  DSL	State: WAITING
0000-00-00 00:00:02 E  Ethernet	Link 1 Up - 100Base-TX Full Duplex
0000-00-00 00:00:50 E  Administration	User 'admin' authenticated

Log Display Options

Display All Log Entries

System <input checked="" type="checkbox"/>	Firewall <input checked="" type="checkbox"/>	ADS <input checked="" type="checkbox"/>
Network <input checked="" type="checkbox"/>	ATM <input checked="" type="checkbox"/>	DSL <input checked="" type="checkbox"/>
Ethernet <input checked="" type="checkbox"/>	USB <input checked="" type="checkbox"/>	Firmware <input checked="" type="checkbox"/>
Config <input checked="" type="checkbox"/>	DHCP Server <input checked="" type="checkbox"/>	DHCP Client <input checked="" type="checkbox"/>
PPP <input checked="" type="checkbox"/>	PPPoE <input checked="" type="checkbox"/>	UPnP <input checked="" type="checkbox"/>
Diags <input checked="" type="checkbox"/>	NAT Owner <input checked="" type="checkbox"/>	DDNS Client <input checked="" type="checkbox"/>
User <input checked="" type="checkbox"/>	Content Filter <input checked="" type="checkbox"/>	ARP <input checked="" type="checkbox"/>
Telnet <input checked="" type="checkbox"/>	Admin <input checked="" type="checkbox"/>	Time Client <input checked="" type="checkbox"/>

Buttons: Refresh, Clear Log, Apply

- To update the display, click **Refresh**.
- To clear the log, click **Clear Log**.
- To change the events displayed in the log, modify the **Log Display Options**, then click **Apply**.

### 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).

Select **Status and Statistics>ATM/AAL** from the left navigation pane of the Web interface to view ATM/AAL statistics. This window displays ATM connection status, uptime, and transmit/receive data, VPI/VCI and related data for each circuit

**ATM/AAL Status/Statistics**

**ATM Status**

Status	Uptime (hh:mm:ss)	Max Theoretical Speed (bits/sec)
UP	00:07:07	8096000

**ATM Statistics**

	Octets	Cells	PDU Counters						
			Unicast	Non-Unicast	Total	Dropped	Errors	Invalid	Queued
Tx	52861	1101	149	0	149	0	0	N/A	0
Rx	19503	406	284	0	284	0	0	0	N/A

**ATM/AAL Status/Statistics**

VPI/VCI	Protocol	Admin Status	Oper Status	Tx-Rate (kbps)	Rx-Rate (kbps)	Tx-PDUs	Rx-PDUs	Tx-Errs	Rx-Errs
0/32	B1483	UP	UP	1024	8096	16	0	0	0
0/33	B1483	UP	UP	1024	8096	16	0	0	0
0/34	B1483	UP	UP	1024	8096	16	0	0	0
0/35	B1483	UP	UP	1024	8096	5	234	0	0
0/36	B1483	UP	UP	1024	8096	16	42	0	0
0/37	B1483	UP	UP	1024	8096	16	8	0	0

### 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.

Select **Status and Statistics>DSL** from the left navigation pane of the Web interface to view DSL statistics. This displays information about the DSL connection.

**DSL Status/Statistics**

**DSL Status**

Status	ATU-C Current Tx Rate (bits/sec)	ATU-R Current Tx Rate (bits/sec)
UP	8096000	1024000

**DSL Statistics (accumulated at 15 minute intervals)**

System Time	Tx CRC	Tx FEC	Rx CRC	Rx FEC	LOS	SEF	LOS (sec)	SEF (sec)	Err (sec)	Rx (blocks)	Tx (blocks)	SNR	Atten.
00:07:58	1	9	0	0	0	0	0	0	1	15180	15180	7.5	42.0
Totals	1	9	0	0	0	0	0	0	1	15180	15180	N/A	N/A

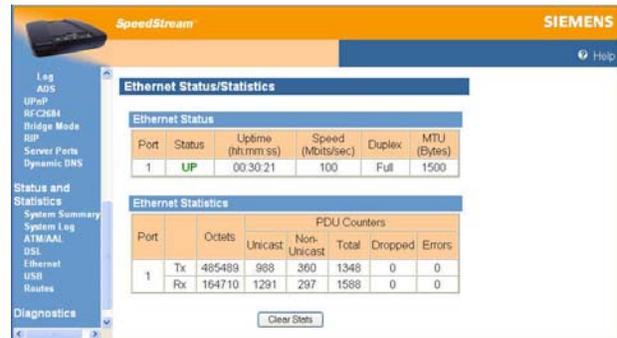
Clear Stats

### Ethernet Statistics

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.

Select **Status and Statistics>Ethernet** from the left navigation pane of the Web interface to view Ethernet statistics.

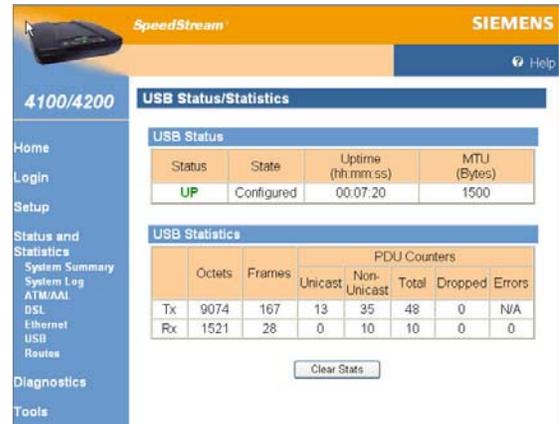


### USB Statistics

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

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

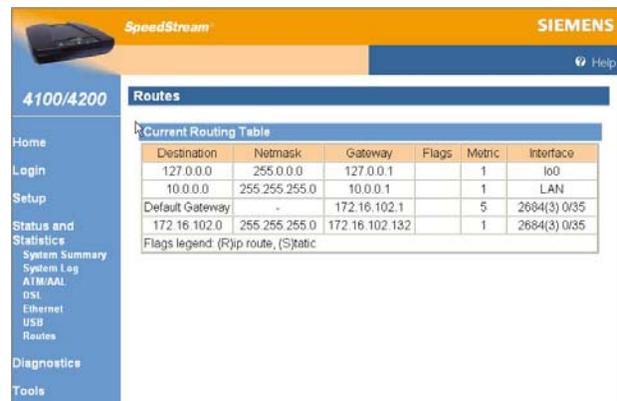
Select **Status and Statistics>USB** from the left navigation pane of the Web interface to view USP statistics.



### Routes

View all IP routes currently known by the Router. Both static and dynamic routes are shown along with their respective netmask, Router, and the corresponding interface.

Select **Status and Statistics>Routes** from the left navigation pane of the Web interface to view the current routing table, which contains the data pertaining to all currently known static and dynamic IP routes



## Diagnostics

The Router provides a considerable amount of diagnostic functionality for testing connectivity on both the Local Area Network (LAN) and the Wide Area Network (WAN). This includes LAN-side connections within the home and WAN-side connections to the carrier, service provider and Internet. WAN-side testing may be performed for each of the WAN-side connections currently configured. This data is commonly requested by technical support to assist in troubleshooting.

**Note:** This option may not be available on your Router configuration.

To run diagnostics:

1. Select **Diagnostics** from the left navigation pane of the Web interface. This displays "Diagnostics" window.

SpeedStream<sup>®</sup> SIEMENS

4100/4200

Home  
Login  
Setup  
Status and Statistics  
System Summary  
System Log  
ATM/AAL  
DSL  
Ethernet  
USB  
Routes  
Diagnostics  
Tools

**Diagnostics**

Your Gateway is capable of testing your DSL service, and the individual tests are listed below. If a test displays a **FAIL** status, click on the "Run Diagnostics" button at the bottom of this page to make sure the failure is consistent. If the test continues to fail, check all connections and passwords, or contact your ISP for help.

Connections in the Home		
Test	Description	Result
LAN	Test the Ethernet/USB Connection	PASS
ADSL	Test ADSL synchronization	PASS

Connections at the Carrier		
Test	Description	Result
Eth to ATM	Test Ethernet connection to ATM	PASS
OAM Segment	Test ATM OAM segment ping	N/A
OAM end-to-end	Test ATM OAM end-to-end ping	N/A

Internet Service Provider		
Test	Description	Result
PPPoE	Test PPPoE Server connection	N/A
PPPoE Session	Test PPPoE session	N/A

2. Select the connection you want to test from the **Connection to Test** drop-down menu.
3. Click **Run Diagnostics**. The test results display under the **Results** column.  
If one of the following failed, contact your Service Provider.
  - **Connections at the Carrier**
  - **Independent Service Provider**
  - **Internet Connectivity**
4. If a test displays a **FAIL** status for any other reason than listed above, click **Run Diagnostics** again to confirm the failure.
5. If the test still displays a **FAIL** status, check all connections and passwords; then click **Run Diagnostics** again.
6. If the test still displays a **FAIL** status, contact your Service Provider for further assistance.

## Tools

This section describes how to use the tools listed below.

### [Interface Map](#)

View a graphical representation of the current LAN and WAN configurations.

### [Reboot](#)

Reboot the Router.

### [Update](#)

Update Router firmware.

## Interface Map

Some Router configurations provide a graphical representation of the current LAN and WAN configurations. This is particularly useful for Technical Support in verifying that correct protocol encapsulations are assigned and Virtual Circuits (VCs) are mapped to the correct network interfaces.

**Note:** This option may not be available on your Router configuration.

To display the interface map, select **Tools>Interface Map** from the left navigation pane of the Web interface. This displays the "Interface Map" window.

The screenshot shows the Siemens SpeedStream 4100/4200 router web interface. The main content area displays the "Interface Map" tool. On the left, there is a diagram showing the router's internal structure with "Ethernet 1" and "USB" connected to a "Bridge/Router MUX", which is connected to the "Router".

The main area contains a table of Virtual Circuits (VCs) with the following data:

2684(0) 0/32	2684 Bridged	0132
2684(1) 0/33	2684 Bridged	0133
2684(2) 0/34	2684 Bridged	0134
2684(3) 0/35	2684 Bridged	0135
2684(4) 0/36	2684 Bridged	0136
2684(5) 0/37	2684 Bridged	0137
2684(6) 0/38	2684 Bridged	0138
2684(7) 0/39	2684 Bridged	0139

Below the table is a "Scan for active VCs" button. At the bottom, there is a legend:

**Legend**

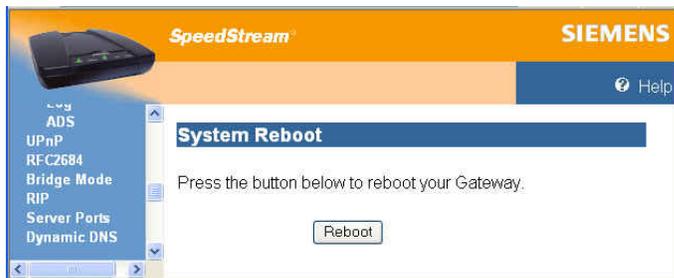
- UP - Interface is up at the Gateway and at the remote end
- DOWN - Interface is down at the Gateway
- ? - Interface is up at the Gateway, but could not be verified at the remote end

## 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 without losing your current configuration settings.

**Note:** This option may not be available on your Router configuration.

To reboot the Router, select **Tools>Reboot** from the left navigation pane of the Web interface. This displays “System Reboot” window.



The “System Reboot” window displays a countdown while processing. When the Router has finished rebooting, the “System Summary” window is displayed.

### Reset to system defaults:

Reset the Router to system defaults should be done 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. **Important:** This option resets all custom settings, users, and passwords on your Router.

**Note:** This option may not be available on your Router configuration.

To reset the Router:

1. Using the tip of a ballpoint pen or unfolded paperclip, press and hold the **Reset** button located on the bottom of the router. The **pwr** LED will blink red once, indicating that the reset has begun.
2. Continue depressing the **Reset** button for four seconds or until the **pwr** LED begins to blink alternating red-to-green.
3. Release the **Reset** button.

### To cancel the reset:

Continue depressing the **Reset** button for longer than 10 seconds. The **pwr** LED will return to green, and the action will be cancelled.

## Update

This feature updates the firmware of your Router through the Internet or from a device connected to your Router.

**Note:** This option may not be available on your Router configuration.

To update the firmware:

1. Select **Tools>Update** from the left navigation pane of the Web interface. This displays "System Update" window.



2. Select one of the following:

- **Remote**  
Checks the Internet for the appropriate upgrade file. This is the recommended method.
- **Local**  
Download the firmware update file from a location on your network. 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!

---

## Appendix A



# Troubleshooting

Connection problems usually occur when the router's software configuration contains incomplete or incorrect information. The router's diagnostic tools can help you identify and solve many of these problems.

## Basic Troubleshooting Steps

Before contacting Technical Support, you should attempt to resolve the issue by following these steps:

1. Check the LEDs on the front panel to diagnose the possible problem.
2. Check specific issues addressed in this chapter, and follow the instructions for resolving the problem.
3. Reboot the router. Any settings you have configured will be saved.
4. Reset the router only as a last resort. You will lose any settings you have configured.

## Interpreting the LED Display

The LED indicators on the front of the router give you a visual clue to the router activity. When the router is configured and working correctly, all LED indicator lights briefly turn a solid green. The following table shows the possible states indicated by the LEDs. If the LEDs indicate a problem, refer to "Resolving Specific Issues" later in this chapter.

LED	pwr	dsl	USB	enet*
<b>Off</b>	No power to router	- No power to router - DSL signal not detected	- No power to router - No USB device connected - USB driver not installed or installed incorrectly	- No power to router - No Ethernet device connected - Wrong Ethernet cable used (cross-over instead of straight-through)
<b>Green</b>	Normal system operation	Connected and ready for data traffic	Normal USB operation, link okay, no user traffic	Normal Ethernet operation, link okay, no user traffic
<b>Blinking Green</b>	N/A	- Steady blinking: DSL attempting to connect - Sporadic blinking: DSL connected and user traffic flowing	USB user traffic flowing in either direction	Ethernet user traffic flowing in either direction
<b>Blinking Red/Green</b>	Flash Write in progress	N/A	N/A	N/A
<b>Red</b>	- POST tests in progress (first 30 sec. after powering on or rebooting) - POST error occurred	N/A	N/A	N/A

## Resolving Specific Issues

### *pwr* LED Not Lit

If the **pwr** (power) LED is not lit, it is not connecting to the power source. Verify that the power cord is firmly plugged into the back panel of the router and that the other end is plugged into an active AC wall or power-strip outlet.

### *dsl* LED Not Lit

If the DSL LED is not lit, it is not detecting a valid signal from the Central Office (CO). Verify that the DSL cable is plugged into the correct router port and the router power cord is plugged into the electrical outlet. If the cables are secure, you should contact your Service Provider.

### *enet* LED Not Lit

This indicates that there is no Ethernet link detected. If you are using the Ethernet connection method, check the Ethernet cable connection from the computer to the router. If you have used the wrong cable, the LED on the Ethernet (NIC) card in your computer will not be lit either.

### USB LED Not Lit

This indicates that there is no USB link detected. If you are using the USB installation method, check the USB cable connection from the computer to the router.

### Login Password Error

If after being prompted for the login password, you receive the error message: `Login Password is invalid:`

- Retype the password, and then click **Save Settings**.
- If you forget your password, you must reset the router.

**Note:** The password is case-sensitive. Be sure that you have not accidentally activated the Caps key.

### **POST Failure (red *pwr* LED)**

POST is the router's "power-on self-test." When you power on or reboot the router, the **pwr** LED goes to a solid red until one of two things occurs: it either fails its initial POST tests, or it comes fully up and is ready to run.

- If POST passes, the router continues through the rest of its initialization, and the **pwr** LED changes to solid green.
- If the initial POST diagnostic tests fail, the **pwr** LED will remain red, indicating a POST failure, and will lock the router. You will need to contact Efficient Networks Technical Support to resolve this issue.

## Contacting Technical Support

If you still cannot resolve the issue after following the recommended troubleshooting procedures, contact Efficient Networks Technical Support.

**Telephone:** (972) 852-1000

**Fax:** (972) 852-1001

**Email:** [usa.800siemens@icn.siemens.com](mailto:usa.800siemens@icn.siemens.com)

**Internet:** <http://www.icn.siemens.com/subscriber>

## Appendix B



# Firewall Security Levels

The following table shows the security of each mode of the firewall for specific applications and protocols.

**Note:** All applications and protocols are conditionally allowed IN if the outbound session was initiated locally and allowed OUT.

Application/ Protocol	Security									
	High		Medium		Low		NAPT Off		ICSA-Compliant	
	In	Out	In	Out	In	Out	In	Out	In	Out
Abuse.Net				√		√		√		
Age of Empires				√		√		√		
AOL		√		√		√		√		
AOL IM						√		√		
Asheron's Call				√		√		√		
Baldur's Gate II				√		√		√		
BattleNet				√		√		√		
Buddy Telephone				√		√		√		
Bungie.Net				√		√		√		
Calista IP Telephone				√		√		√		
Counterstrike				√		√		√		
CUSEeMe						√		√		
Delta Force				√		√		√		
Descent II/III				√		√		√		
Diablo				√		√		√		
Diablo 2				√		√		√		
Dialpad				√		√		√		
DirectPlay				√		√		√		
DNS		√		√		√		√		√
Doom				√		√		√		
Dune 2000				√		√		√		
EverQuest				√		√		√		√
FTP				√		√		√		
GNUtella						√		√		

Application/ Protocol	Security									
	High		Medium		Low		NAPT Off		ICSA-Compliant	
	In	Out	In	Out	In	Out	In	Out	In	Out
H.323						√		√		
Half Life				√		√		√		
Heretic II				√		√		√		
Hexen II				√		√		√		
HTTP		√		√		√		√		√
HTTPS		√		√		√		√		√
ICMP		√		√		√		√		
ICQ 2000						√		√		
ICU II						√		√		
IGMP				√		√		√		
IPSec multi-session				√		√		√		
IPSec single-session				√		√		√		
IRC						√		√		
Kali				√		√		√		
L2TP				√		√		√		
MechWarrior 4				√		√		√		
Mplayer				√		√		√		
MS Netmeeting						√		√		
MSN Gaming Zone				√		√		√		
MSN Messenger						√		√		
Myth				√		√		√		
Napster						√		√		
Need for Speed				√		√		√		
Net2telephone				√		√		√		
Netshow Client						√		√		
NNTP						√		√		
NTP				√		√		√		√
PCAnywhere						√		√		
Ping		√		√		√		√		
POP3				√		√		√		

Application/ Protocol	Security									
	High		Medium		Low		NAPT Off		ICSA-Compliant	
	In	Out	In	Out	In	Out	In	Out	In	Out
PPPoE				√		√		√		
PPTP multi-session				√		√		√		
PPTP single-session				√		√		√		
Quake Arena				√		√		√		
Quake II				√		√		√		
Quicktime 4		√		√		√		√		
Rainbow Six				√		√		√		
Real Audio		√		√		√		√		
Real Video		√		√		√		√		
Red Alert II				√		√		√		
Rogue Spear				√		√		√		
RTSP		√		√		√		√		
SIP						√		√		√
SMTP				√		√		√		
Soldier of Fortune				√		√		√		
SSH				√		√		√		
Starcraft				√		√		√		
T.120						√		√		
Telnet				√		√		√		√
Tiberian Sun				√		√		√		
Traceroute		√		√		√		√		
Ultima Online				√		√		√		
Unreal Tournament				√		√		√		
VNC						√		√		
Warcraft				√		√		√		
Windows Media Player		√		√		√		√		
XDM						√		√		
Yahoo Messenger						√		√		

**Siemens Subscriber Networks**

4849 Alpha Road  
Dallas, TX 75244 USA  
(972) 852-1000 Tel  
(972) 852-1001 Fax

[usa.800siemens@icn.siemens.com](mailto:usa.800siemens@icn.siemens.com)  
<http://www.icn.siemens.com/subscriber>