SpeedStream®

Router User Guide

Series: 5100, 5200, 5400, 5500

Efficient NETWORKS™

Part No. 007-0820-001

Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Efficient Networks, Inc. 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.

Efficient Networks, Inc. – End User Software License and Limited Warranty

INSTALLATION OF THE HARDWARE AND SOFTWARE PROVIDED BY EFFICIENT NETWORKS, INC. ("EFFICIENT") 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 EFFICIENT DSL customer premises equipment ("Hardware") and the limited warranty that EFFICIENT 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, EFFICIENT 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 EFFICIENT, whether delivered via tangible media (CD ROM or floppy disk), down loaded from EFFICIENT 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 EFFICIENT.

7. **Termination**. Without limiting EFFICIENT's other rights, EFFICIENT 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 EFFICIENT 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**. EFFICIENT 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**. EFFICIENT 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, EFFICIENT 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 EFFICIENT's exclusive obligation for breach of this limited warranty is, in EFFICIENT's sole option, either (a) a refund of the purchase price paid for the Hardware/Software or (b) repair or replacement of the Hardware/Software with new or remanufactured products. Any replacement Hardware or Software will be warranted for the remainder of the original warranty period or thirty (30) days, which ever is longer.

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

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

B. After receiving an RMA, the end user shall ship the product, including power supplies and cable, where applicable, freight or postage prepaid and insured, to EFFICIENT at 4849 Alpha Road, Dallas Texas 75244, U.S.A. Within five (5) days notice from EFFICIENT, the end user shall provide EFFICIENT with any missing items or, at EFFICIENT's sole option, EFFICIENT 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 EFFICIENT. Products that pass all functional tests will be returned to the end user.

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

E. Upon request from EFFICIENT, 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 EFFICIENT, including acts of nature and damage caused by shipping.

EFFICIENT 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 EFFICIENT authorized service provider.

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

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

EFFICIENT 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 EFFICIENT 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 EFFICIENT 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 EFFICIENT HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. EFFICIENT'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 EFFICIENT 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 EFFICIENT must be mailed by certified mail to the following address:

Efficient Networks, Inc.
4849 Alpha Road
Dallas, TX 75244
U.S.A.
Attn: Customer Service

Contents

List of Illustrations

Note Illustrations in this document were taken from the Microsoft® Internet Explorer™ browser. If you are using a different browser, your actual screens may differ somewhat from those shown.

Introduction

Congratulations on your purchase of the SpeedStream® Router with SecureRoute™. Efficient Networks is proud to provide you with a powerful yet simple communication device for connecting your computer or *local area network (LAN)* to the Internet.

This manual covers the SpeedStream model series 5100, 5200, 5400 and 5500.

SpeedStream 5100 Series
(1 Ethernet port, no USB port)

SpeedStream 5200 series
(1 Ethernet port, 1 USB port)

SpeedStream 5400 Series
(4 Ethernet ports, no USB port)

SpeedStream 5500 series
(4 Ethernet ports, 1 USB port)

Hardware Description

The LED display panel on the front of your SpeedStream router displays system power and port indicators that simplify installation and network troubleshooting. The rear panel provides port connections for Ethernet, DSL, USB (5200, 5500 series), and the power connection. The recessed **Reset** button is located on the bottom of the router.

About the SpeedStream Router

Your SpeedStream 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 SpeedStream router can also be used to connect the corporate local area network (LAN) to the Internet over the wide area network (WAN).

Features and Benefits

- Effortless installation via configurable *Universal Plug and Play* (UPnP) integration with an intuitive graphical user interface (GUI) on UPnP-supported operating systems (Windows ME and XP).

- Intuitive Web-based *management interface* to simplify operation and support.

- 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 connectivity (5200, 5500 series) providing added flexibility of connecting your computer via the Ethernet or USB port.

- Support for G.lite and full-rate DSL ensures compatibility with most DSL networks.

- Multiple computers can share a single DSL connection through the integrated switch ports, each providing full- or half-duplex data transmission (5400, 5500 series).

- *Firewall Security* with four conveniently pre-set standard levels of firewall security (Off, Low, Medium, High), an ICSA-compliant mode, and a custom setting for advanced users.

- *Stateful Inspection Firewall* that provides many security features such as blocking common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- *Network Address Port Translation* (NAPT) and a secure firewall to protect your data while your computer is connected to the Internet.

- *Port Forwarding* to provide more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

- *Virtual Private Network* that 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.

Firewall Security

The firewall in the SpeedStream router is a stateful packet inspection filter that works at the IP level. The firewall consists of an IP packet filtering mechanism, a Network Address Port Translator (NAPT), and a Network Address Translator (NAT). When the NAPT/NAT feature is enabled, the local (unreachable) IP addressing used in the LAN automatically protects it from access. Even when NAPT/NAT is disabled and the LAN is accessible from the WAN, you can configure the firewall to protect the LAN from external attacks by creating custom filters to fine-tune access control.

Note *Firewall* and *NAPT/NAT* are not the same thing; but a NAPT/NAT system works like a firewall and is often considered to be one. In the specific context of SpeedStream routers and their associated Web management interfaces, the term “firewall” refers to IP packet filtering (stateful inspection, etc.). However, in the generic sense of firewall functionality, SpeedStream products also include NAT and NAPT.

The firewall includes the following high-level, industry-standard features:

- Port forwarding through NAPT/NAT.
- Numerous Application Level Gateways (ALGs) for proper NAPT/NAT functioning.
- Stateful IP filtering with sophisticated rules database.
- Automatic and protocol-specific session tracking.
- Preconfigured and custom firewall levels.
- Virtual DMZ.
- Firewall logging with Network Time Protocol and SysLog support.
- Attack Detection System (ADS).

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 SpeedStream firewall allows traffic on such secondary sessions without manual configuration.

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

Installing the Router

Minimum System Requirements

At a minimum, your computer must be equipped with the following.

Ethernet Port Connectivity (5100, 5200, 5400, 5500 series)

- 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 Port Connectivity (5200, 5500 series)

If connecting to the router via USB, your computer must meet manufacturer's minimum requirements and be equipped with the following:

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

Important! Your specific configuration may vary slightly from the instructions and illustrations in this chapter. Refer to your Service Provider's documentation or contact them for questions regarding your 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. You should, however, comply with the safety guidelines specified in the General Safety Guidelines.

Basic Installation Procedure

1. Install line filters if necessary.
2. Connect the cables.
3. Plug the router into the electrical outlet; then verify port status.
4. Install USB drivers if necessary (5200, 5500 series).
5. Configure network settings on your computer.
6. Configure the router via the Web-based management interface.
7. Reboot the computer if prompted.

Recording System Settings

Another important step is to record the current router configuration in the worksheets provided in Appendix A, “Configuration Data Sheets.” Although the router is already configured for your particular network, it is important to record this configuration in case it must be restored for any reason, or if you make changes to the default settings and need to restore them at any point.

Installing Line Filters

Note This section may not apply to you. Consult your provider if you are unsure.

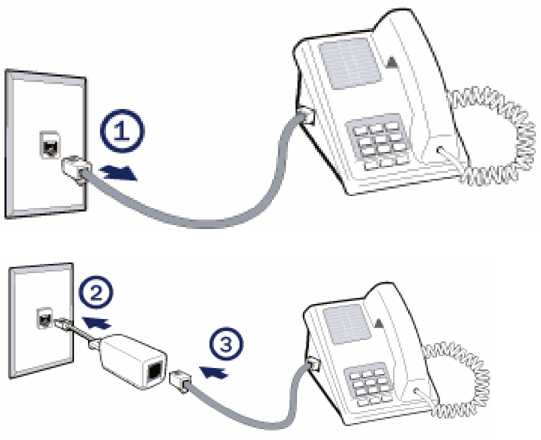
Because DSL shares your telephone line, you may need to separate the two signals so they do not interfere with each other. A line filter (may be included with some models) prevents DSL traffic from disrupting the voice signal on the telephone line, and vice versa. Follow the procedures below to install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

You will need one of these type 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.

You may also need a *two-to-one adapter* if you want to connect more than one device to the telephone wall plate.

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



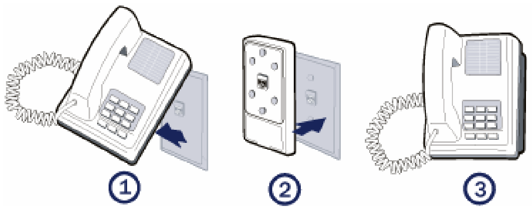
In-Line Filter

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.

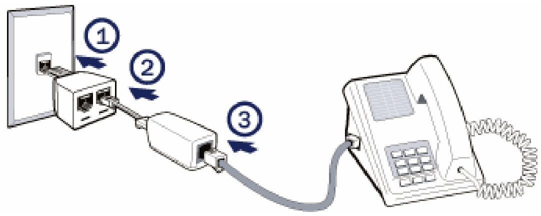
3. Plug the telephone cord (or other device cord) into the filter.



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.



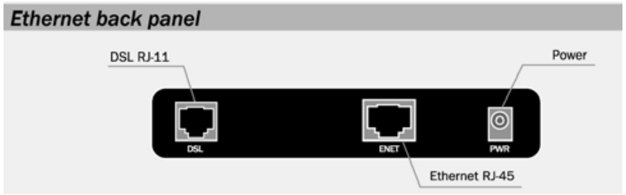
Two-to-One Adapter

If your DSL router and another device will share the same telephone jack, install a two-to-one adapter:

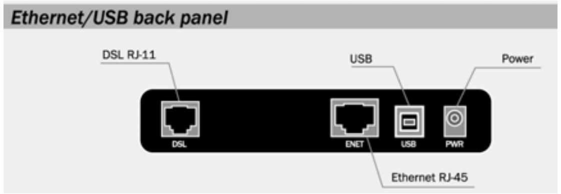
1. Plug a two-to-one adapter into the telephone jack.
2. Plug a line filter into one of the sockets of the two-to-one adapter. The other socket will be used to connect the DSL cable.
3. Plug the device cord into the line filter.

Connecting the Cables

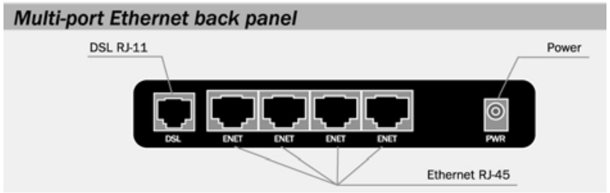
You can connect your SpeedStream router to an existing Ethernet port on your computer. Some models provide the added flexibility of connecting to your computer’s Ethernet port, USB port, or both. Determine the cable to use for your physical connection, and then follow the instructions below for the appropriate installation method.



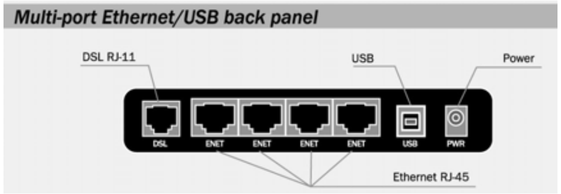
SpeedStream 5100 series



SpeedStream 5200 series



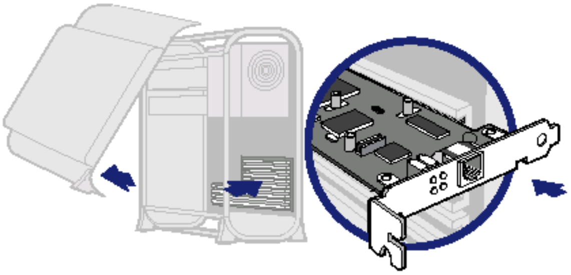
SpeedStream 5400 series

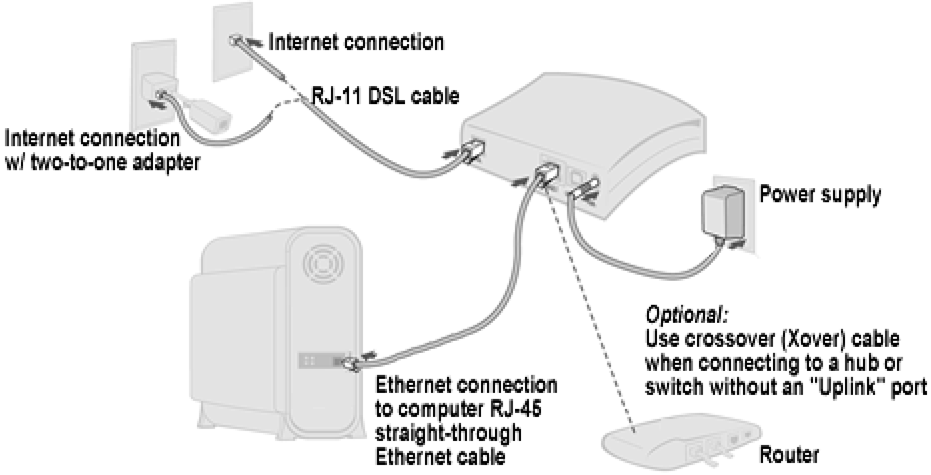


SpeedStream 5500 series

Ethernet Installation Method

To connect the SpeedStream router via the Ethernet interface, your computer must have an Ethernet adapter (network interface card, or “NIC”) installed. If your computer does not have this adapter, you will need to install it before proceeding further. Refer to the Ethernet adapter documentation for complete installation instructions.




Internet connection
RJ-11 DSL cable
Internet connection w/ two-to-one adapter
Power supply
Optional: Use crossover (Xover) cable when connecting to a hub or switch without an "Uplink" port
Ethernet connection to computer RJ-45 straight-through Ethernet cable
Router

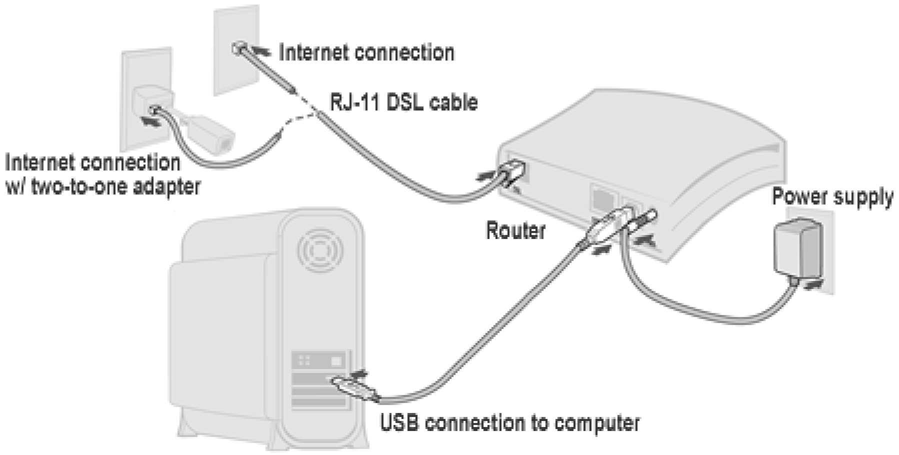
1. Make sure the router is not plugged in to the electrical outlet.
2. Connect the Ethernet straight-through cable to the Ethernet port on the router.
3. Connect the other end of the Ethernet cable to the Ethernet port on your computer.
4. Plug the telephone cable into the DSL port on the router.
5. Plug the other end of the telephone cable into the telephone jack.

   Note If using a two-to-one adapter, plug the cable into the open socket.
6. Plug the power adapter into the router and the electrical outlet.

When using the Ethernet installation method, you do not have to install any software. Refer to your Internet Service Provider’s instructions for installing their software and/or connecting to the Internet.

You can now configure the TCP/IP settings as detailed in the next chapter.

USB Installation Method


Internet connection
RJ-11 DSL cable
Internet connection w/ two-to-one adapter
Power supply
Router
USB connection to computer

1. Ensure that your computer meets the minimum requirements for USB installation.
2. Make sure the router is not plugged in to the electrical outlet.
3. Connect the USB cable to the USB port at the rear of the router.
4. Connect the other end of the USB cable to the USB port on your computer.
5. Plug the telephone cable into the DSL port on the router.
6. Plug the other end of the telephone cable into the telephone jack.

   Note If using the two-to-one adapter, plug the cable into the open socket.
7. Plug the router power adapter into the router and then into the electrical outlet.

Note The Plug and Play process for installing the USB drivers begins as soon as you turn on your computer and it discovers the router. To install the USB drivers, insert the SpeedStream CD-ROM and follow the on-screen instructions.

You can now configure the TCP/IP settings as detailed in the next chapter.

Configuring Computer Network Settings

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.

The default network settings for the SpeedStream router are:

IP Address:	192.168.254.254
Subnet Mask:	255.255.255.0

Windows 95/98/ME

1. On the Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.

   The Windows **Control Panel** displays.

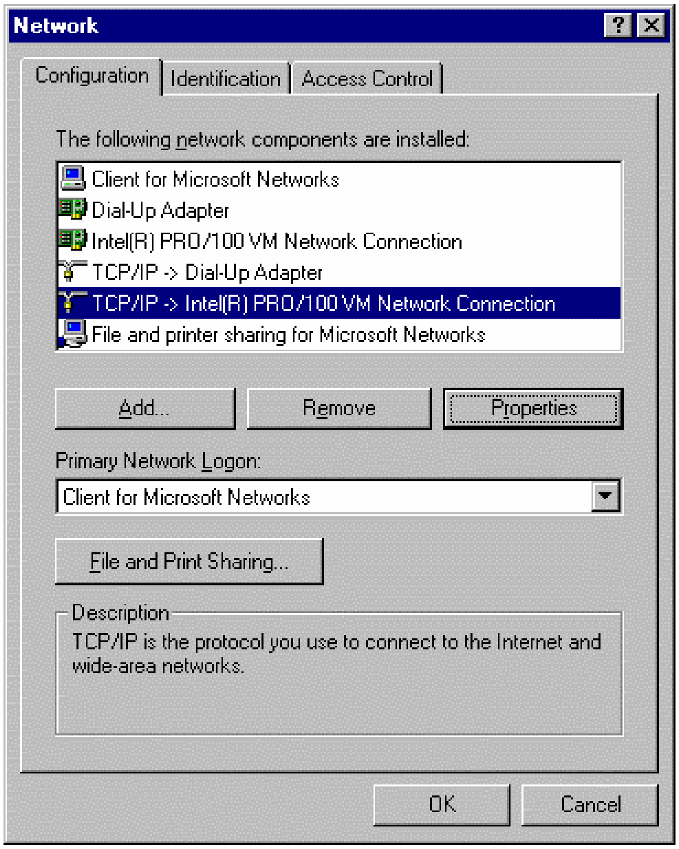
2. In **Control Panel**, double-click **Network**.

   The **Network** dialog box displays.

3. On the **Configuration** tab of the **Network** dialog box, select the TCP/IP entry for your Ethernet adapter; then click **Properties**.

   The **TCP/IP Properties** dialog box displays.

   Note The components list for your computer may differ from this screenshot.



The following network components are installed:

- Client for Microsoft Networks
- Dial-Up Adapter
- Intel(R) PRO/100 VM Network Connection
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> Intel(R) PRO/100 VM Network Connection
- File and printer sharing for Microsoft Networks

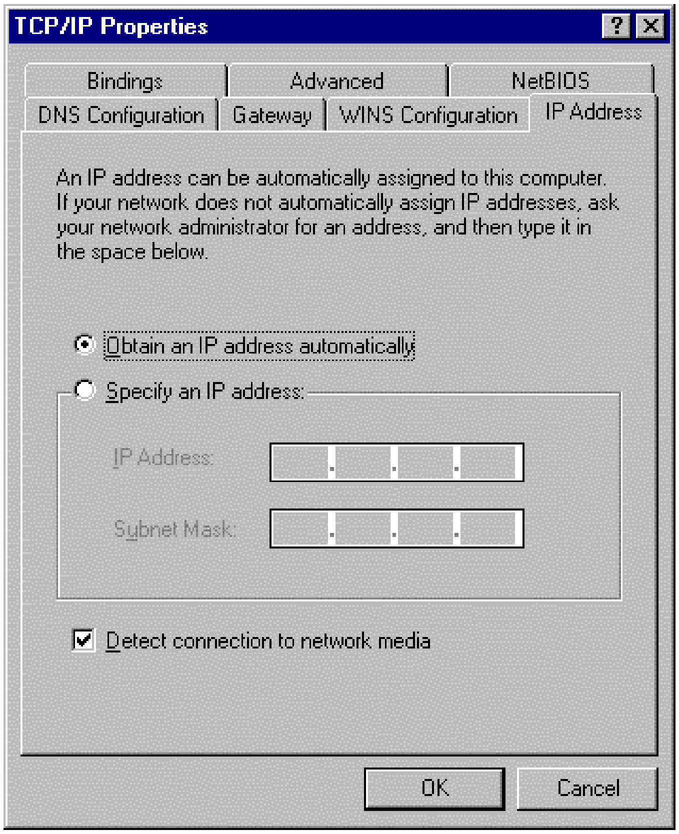
Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.

5. On the **IP Address** tab, make sure that **Obtain IP address automatically** and **Detect connection to network media** are selected.

6. Click the **DNS Configuration** tab.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

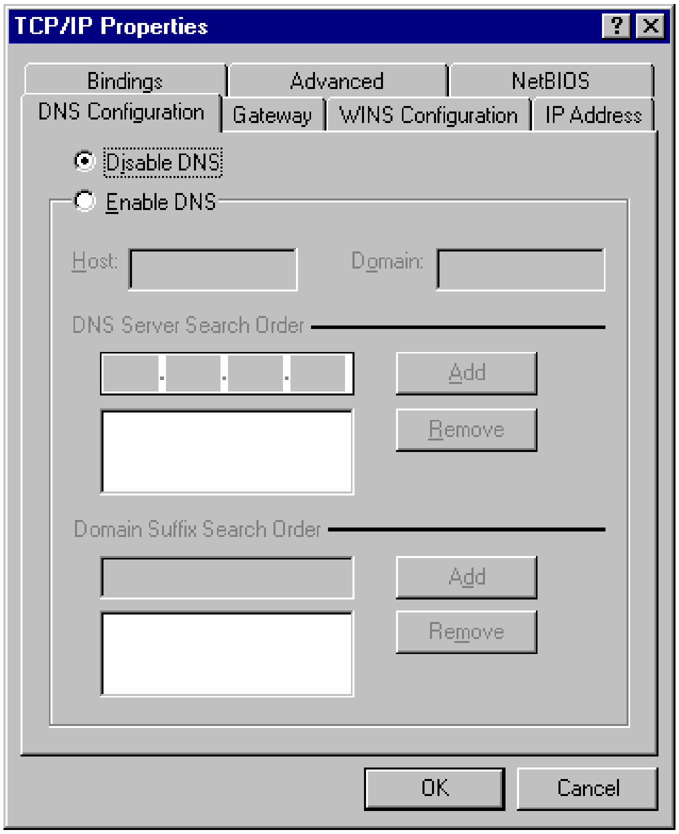
○ Specify an IP address:

☑ Detect connection to network media

7. On the **DNS Configuration** tab, make sure that **Disable DNS** is selected.

8. Click **OK** twice to save your settings.

9. Reboot your computer if prompted.



● Disable DNS

○ Enable DNS

Windows NT 4.0

1. On the Windows taskbar, click **Start**, then point to **Settings**, and then click **Control Panel**.

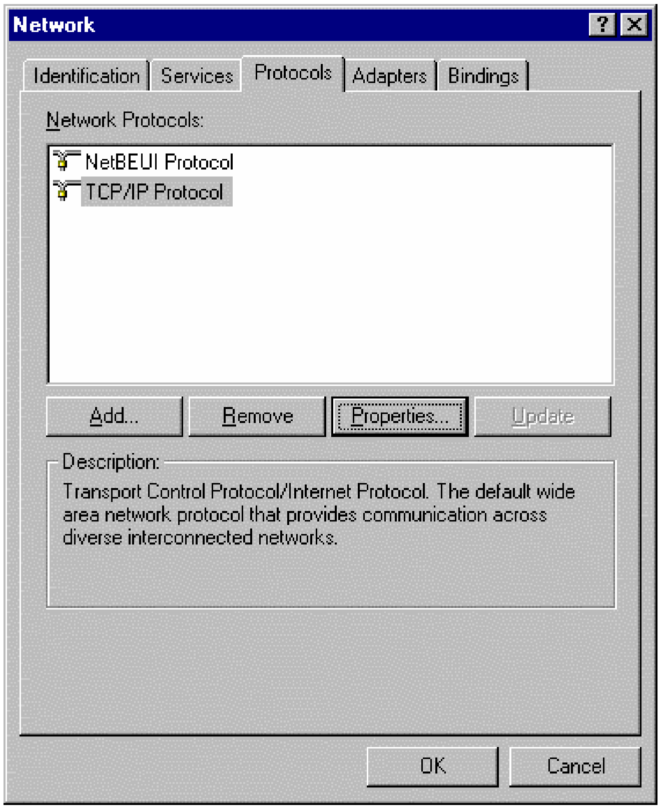
   The Windows Control Panel displays.

2. In Control Panel, double-click **Network**.

   The **Network** dialog box displays.

3. On the **Protocols** tab, select **TCP/IP Protocol**, and then click **Properties**.

   The **Microsoft TCP/IP Properties** dialog box displays.



Network

Network Protocols:

NetBEUI Protocol

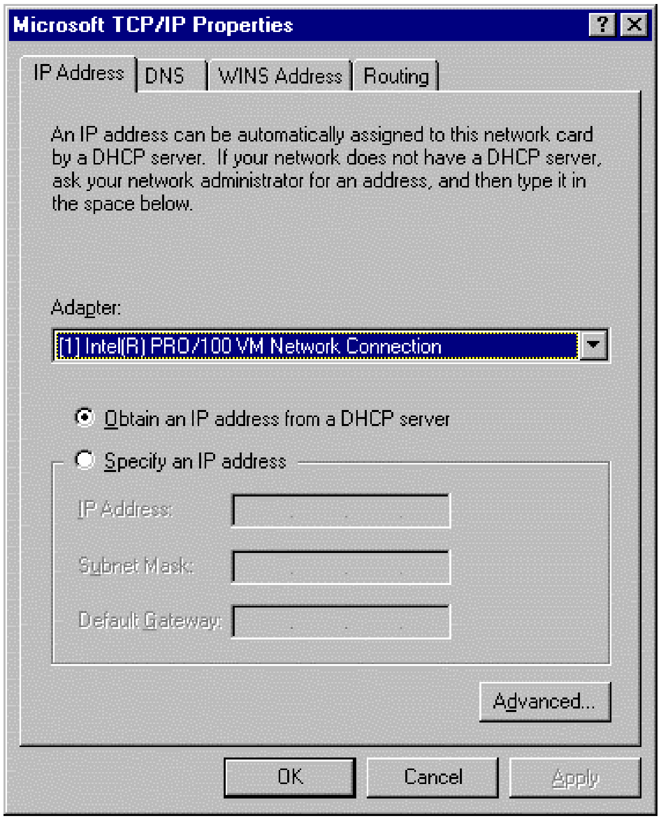
TCP/IP Protocol

Description:

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

4. In the **Microsoft TCP/IP Properties** dialog box, make sure that the correct network adapter is selected in the **Adapter** menu and that **Obtain an IP address from a DHCP server** is selected; then click **OK**.

   Note Your network adapter may differ from this illustration.



Microsoft TCP/IP Properties

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter:

[1] Intel(R) PRO/100 VM Network Connection

● Obtain an IP address from a DHCP server

○ Specify an IP address

IP Address:

Subnet Mask:

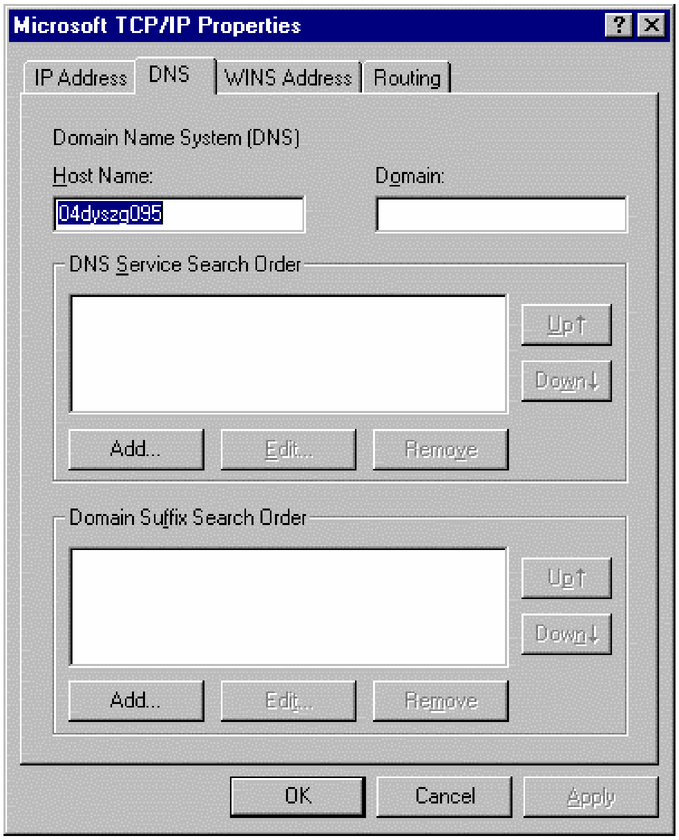
Default Gateway:

5. In the **Microsoft TCP/IP Properties** dialog box, click the **DNS** tab.

6. On the **DNS** tab, delete any IP addresses listed in the **DNS Service Search Order** box.

7. Click **OK** twice to save your settings.

8. Reboot your computer if prompted.



Host Name: 04dyszg095

Domain:

Windows 2000

1. On the Windows taskbar, click **Start**, then point to **Settings**, and then click **Control Panel**.

   The Windows Control Panel displays.

2. Double-click **Network and Dial-up Connections**.

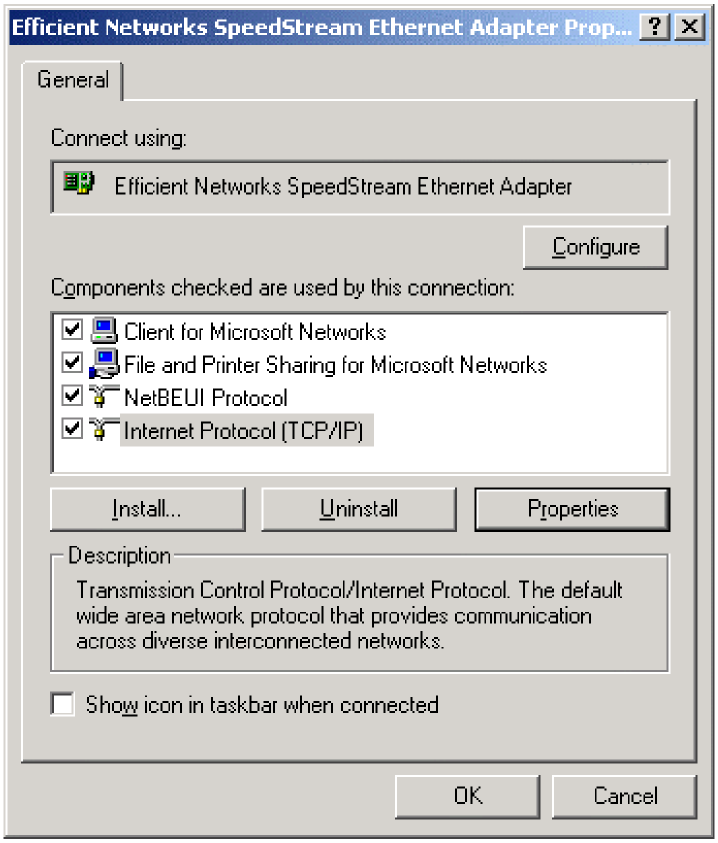
   If the Ethernet card in your computer is installed correctly, the **Local Area Connection** icon will be present.

3. Right-click on your Local Area Connection (LAN), and then click **Properties**.

   The **Local Area Connection Properties** dialog box displays.

4. Select **Internet Protocol (TCP/IP),** and then click **Properties**.

   The **Internet Protocol (TCP/IP) Properties** dialog box displays



Connect using:

Efficient Networks SpeedStream Ethernet Adapter

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ NetBEUI Protocol
☑ Internet Protocol (TCP/IP)

Description

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

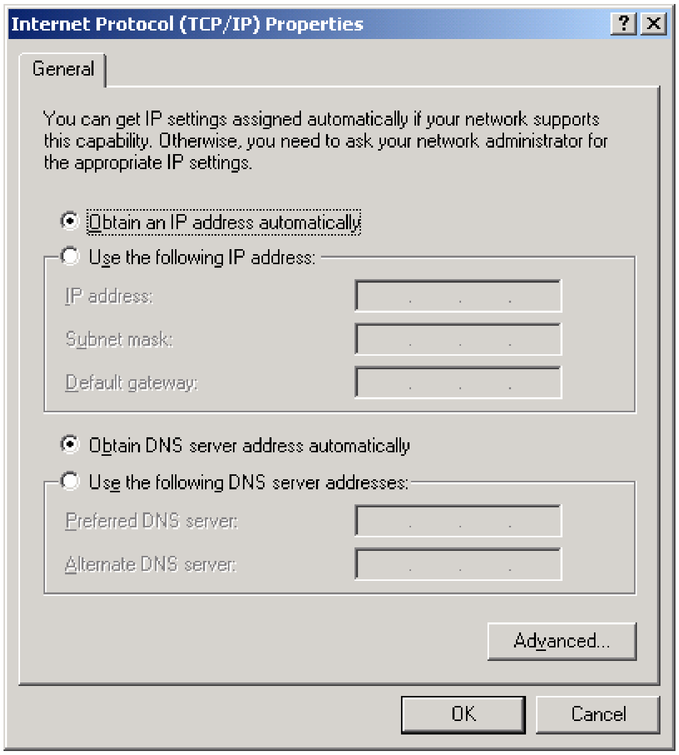
☐ Show icon in taskbar when connected

Note Your network adapter may differ from this illustration.

5. In the **Internet Protocol (TCP/IP) Properties** dialog box, make sure that **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

6. Click **OK** twice to save your settings.

7. Reboot your computer if prompted.



Internet Protocol (TCP/IP) Properties

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

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

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

Windows XP

1. On the Windows taskbar, click **Start**, then click **Control Panel**, and then click **Network and Internet Connections**.

2. Click **Network Connections**, then click **Local Area Connection**, and then select **Properties**.

   The **Local Area Connection Properties** dialog box displays.

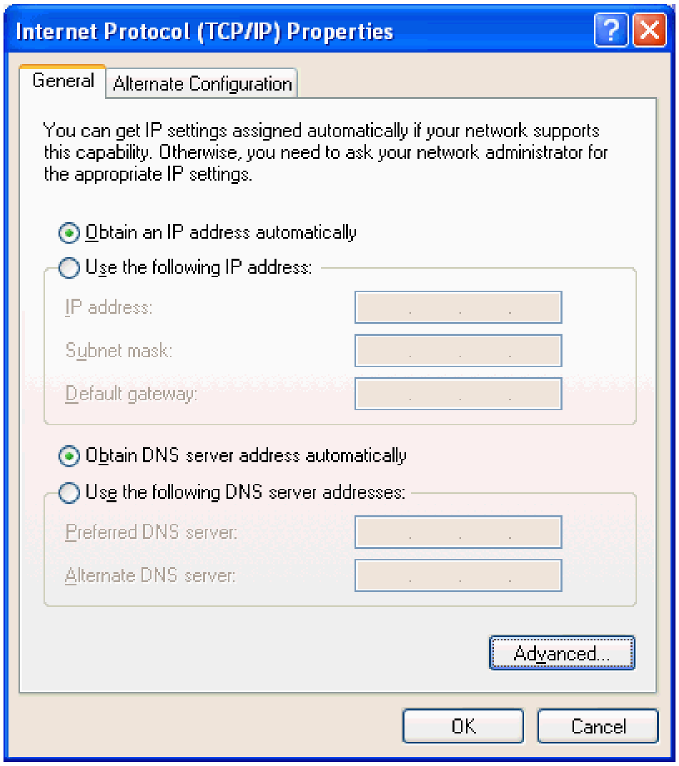
3. Select the **Internet Protocol (TCP/IP)** check box, and then click **Properties**.

   The **Internet Protocol (TCP/IP) Properties** dialog box displays.

4. In the **Internet Protocol (TCP/IP) Properties** dialog box, ensure that **Obtain IP address automatically** and **Obtain DNS server address automatically** are selected.

5. Click **OK** twice to save your settings.

6. Reboot your computer if prompted



Internet Protocol (TCP/IP) Properties

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

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

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

You can now configure the SpeedStream router as detailed in "Configuring the Router."

Getting Started

By this point, you should have completed the following:

- Connected the router.
- Verified that the TCP/IP protocol is installed on all computers in your network. (If you need to install TCP/IP, refer to your system documentation or Windows Help.)
- Configured the network settings on those computers.

You can now easily configure the SpeedStream router from the convenient Web-based management interface. From your Web browser (Microsoft Internet Explorer or Netscape Navigator, versions 4.0 or above), you will log in to the interface to define system parameters, change password settings, view status screens to monitor network conditions, and control the router and its ports.

Navigating the Web Interface

Note Depending on which model you are configuring, the Web-based management interface may include these menu items:

Home At first login, displays the **Administrative User Setup** screen; after first login, displays the **System Summary** screen.

Login If PPP session(s) have been configured, allows you to enter or modify the Point-to-Point Protocol (PPP) user name and password. If not connected, displays disconnect status.

Advanced Setup Access advanced features to configure custom settings. Unless you have a specific need to change the settings, you should leave them as their defaults. To change some of these settings, you may need to acquire information from your ISP or network administrator.

- **Host** Enter host IP address and netmask, default router and host name.
- **DHCP** Enable or disable DHCP; specify DHCP parameters.
- **User** Change system user name and password.
- **Time Client** Configure Time Client parameters to automatically synchronize system internal date and time.
- **Static Routes** View or configure static routes.
- **NAT/NAPT** Enable or disable NAT mode, view NAT table, add or edit NAT table entries.
- **Port Forwarding** View, add, or edit NAPT table entries.
- **Firewall** Setup and control firewall settings.
  - **Level** Specify firewall level.
  - **Snooze** Configure firewall snooze control.

DMZ	View current DMZ status and host IP address, disable or enable Virtual DMZ, specify DMZ host IP address.
IP Filter Rules	View, add or change custom filter rules.
Log	View log listing of all firewall activity including record of any denial of access, reason code and description string.
ADS	Configure the Attack Detection System (ADS).
UPnP	Configure Universal Plug and Play options.
RFC2684	Configure settings for RFC2684 (multi-protocol encapsulation over AAL5).
Bridge Mode	Enable bridge mode.
RIP	Configure Router Information Protocol.
LAN Servers	Configure non-standard port values for LAN servers.
Status and Statistics	View system and connections summary data.
System Summary	View system and PPP connection data.
System Log	View system activity entries.
ATM/AAL	View ATM and AAL5 connection data.
DSL	View DSL connection data.
Ethernet	View Ethernet connection data.
USB	View USB connection data (5200, 5500 series).
Routes	View all static and dynamic IP routes known by router.
Diagnostics	Perform DSL diagnostics.
Tools	Access interface tools.
Interface Map	View current interface configuration.
Reboot	Reboot router.
Update	Install updated system firmware.

Screen Navigation Elements

The Web management interface provides several screens that allow you to change settings and view system status. Although the navigation elements on the screens vary according, the common elements may include:

- **Apply**
  Initializes setting changes you have entered.

- **Cancel**
  Deletes any changes you have entered and resets that data to its previous value.

- **Clear / Clear Stats**
  On a page where you can select an item from the table to edit, resets the form back to a *blank* state.

- **Reset**
  Invokes the standard "reset" functionality of HTML form, resetting the form contents back to the *initialized* values originally displayed.

- **Save Settings**
  Initializes the settings you have entered.

Logging On to the Web Interface

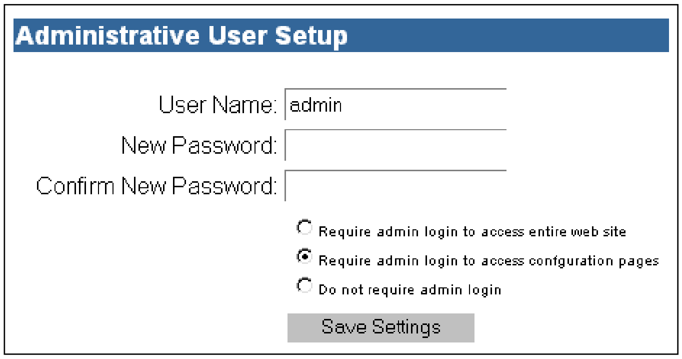
The first time you log on to the Web interface, you will be required to enter a system password in the **Administrative User Setup** screen. You will also have the option of changing the user name from the default setting of **admin**. After your initial log on, the **System Summary** or PPP **Login** [Choose Connection] screen will display, depending on your connection.

To log on to the Web interface for the first time:

1. In your Microsoft Internet Explorer **Address** bar or Netscape Navigator **Location** bar, enter the default router IP address: **http://192.168.254.254**

   The **Administrative User Setup** screen displays.

2. You may accept the default user name **admin**, or enter a new user name in the **User Name** box. The user name is case-sensitive.



Administrative User Setup

User Name: admin

New Password:

Confirm New Password:

○ Require admin login to access entire web site

● Require admin login to access configuration pages

○ Do not require admin login

3. Enter a password in the **New Password** box; then enter the same password in the **Confirm New Password** box.

   Note You *must* enter a password before proceeding. Both user name and password are case-sensitive. Be sure to record your user name and password. You will need to use them when you log on again.

   Important! Any keystroke or combination of keystrokes can be used as a password. For example, the Delete shortcut key combination, CTRL+X, would be accepted as a valid password character.

4. Select the login security level you prefer:

   - **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 **OK**. Depending on your connection(s), one of the following screens will display:
   - If you have *no PPP connections* configured, the **System Summary** screen displays.
   - If you have only *one PPP connection* configured, the PPP **Login** screen for that connection displays.
   - If you have *multiple PPP connections* configured, the PPP **Login** [choose connection] screen displays the available connections.

Entering the Network Password

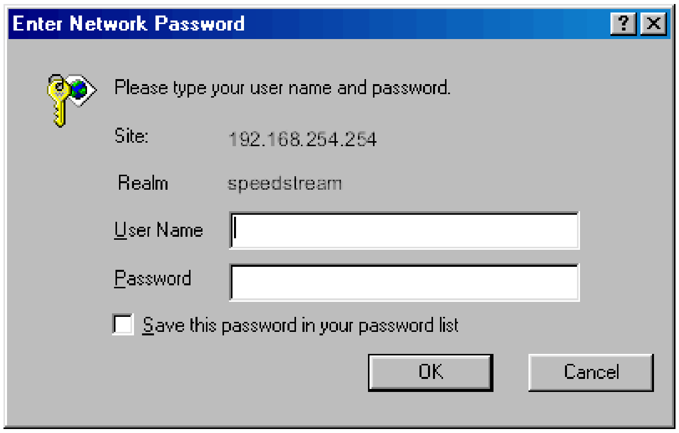
If you selected either of these options in the **Administrative User Setup** screen, you will be required to log on again:

- **Require admin login to access entire Web site**
- **Require admin login to access configuration pages**

1. After you have logged on to the Web interface under either of these two conditions, the **Enter Network Password** screen displays.

2. In the **Enter Network Password** dialog box, enter your user name and password.

3. If you Want to circumvent this screen in the future (which in effect cancels your previous settings), click **Save this password in your password list**.



Please type your user name and password.

Site: 192.168.254.254

Realm speedstream

User Name

Password

□ Save this password in your password list

4. Click **OK**.

   The **Enter Network Password** dialog box closes, and the screen you were trying to access displays.

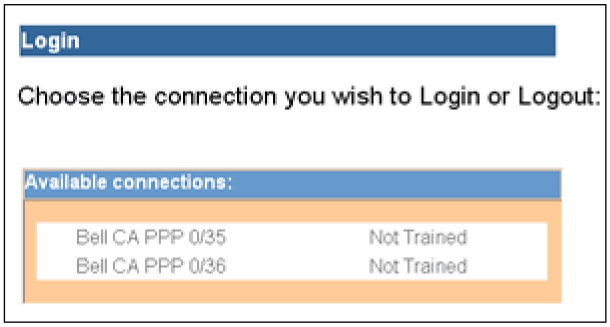
Logging On to a PPP Session

After you log on to the **Administrative User Setup** screen, one of two screens will display.

1. **If you have configured multiple PPP sessions**, the **Login** screen will display the available connections. Click the connection you wish to log on to.

   - or -

   If you have configured only one PPP session, the PPP **Login** screen displays.



Choose the connection you wish to Login or Logout:

Available connections:

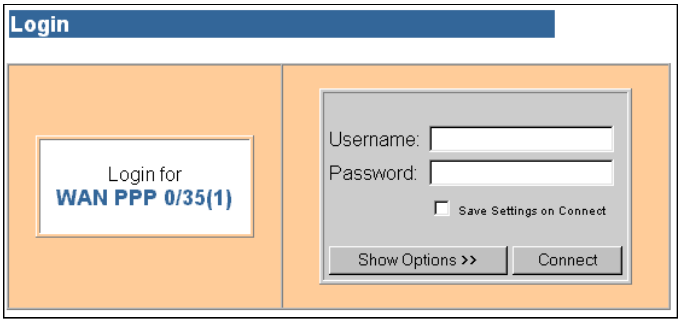
Bell CA PPP 0/35	Not Trained
Bell CA PPP 0/36	Not Trained

2. In the PPP **Login** screen, enter the user name and password.

3. To save the settings, select **Save Settings on Connect.**

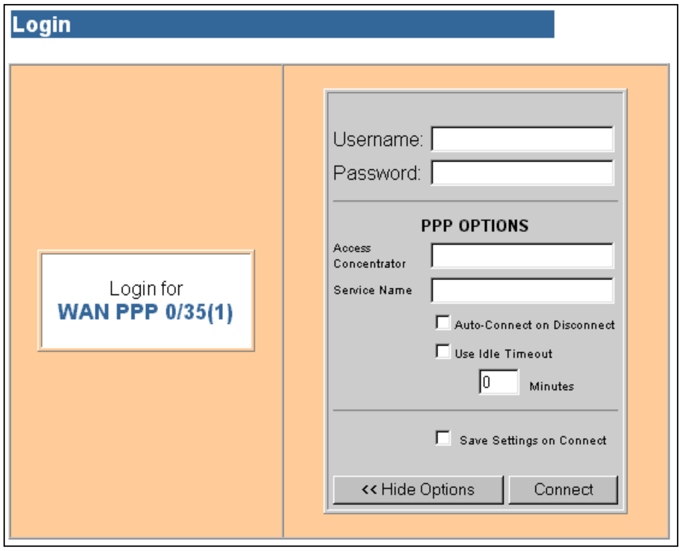
4. To configure additional PPP options, click **Show Options**.

   The input box expands to display the **PPP Options** section.



5. Enter the desired PPP options:

   - **Access Concentrator:** Enter the [optional] name of the access concentrator as provided by your ISP.
   - **Service Name:** Enter the [optional] service name provided by your ISP.
   - **Auto-Connect on Disconnect:** If selected, 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 the specified amount of time. Enter the time in minutes. This cannot be used with **Autoconnect.**



PPP 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.

Customizing Router Settings

This section provides you with the information and procedures to customize various settings on your SpeedStream router. Many of these procedures require a mid- to advanced-level understanding of networking principles. If unsure, contact your Service Provider for assistance.

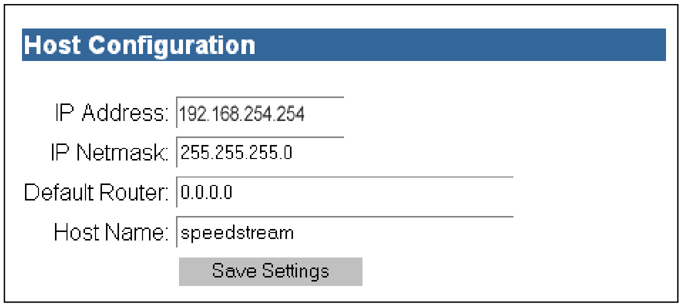
Host

The **Host Configuration** screen allows you to change the host IP address, netmask, default router and host name. The information in this section is auto-generated and should not be changed unless your ISP directs you to do so; for example, if you have been assigned a static IP address.

To specify the host configuration settings:

1. If your ISP has assigned a static IP address for this machine, enter that IP address and subnet mask.
2. Enter the default router address if other than that specified.
3. Enter the host name if other than **speedstream**.
4. Click **Save Settings**.

   A confirmation screen displays notification that the new setting will not take effect until you reboot the router. You may do so at this point or later.



Host Configuration

IP Address: 192.168.254.254

IP Netmask: 255.255.255.0

Default Router: 0.0.0.0

Host Name: speedstream

5. To reboot the router, click **Reboot** on the confirmation screen.

   The **System Reboot** screen displays with a countdown while the router is rebooting. When finished, the **System Summary** screen displays.

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. The information in this section is auto-generated and should not be changed unless your ISP directs you to do so; for example, if you have been assigned a static IP address.

IP Address Restrictions

Certain restrictions apply to the range of IP addresses specified by the parameters **Start IP Range**, **End IP Range**, and **IP Netmask** defined above. These restrictions are as follows:

- 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

DHCP Configuration Options

- **DHCP Server:**
  When *Enabled*, 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.
- **Start IP Range:**
  Specifies the beginning IP address of the range of addresses from which the DHCP server will lease to requesting DHCP clients. This value must be entered as an IPv4 address expressed in *dotted-decimal notation* (e.g., 192.168.254.1).
- **End IP Range:**
  Specifies the beginning IP address of the range of addresses from which the DHCP server will lease to requesting DHCP clients. This value must be entered as an IPv4 address expressed in *dotted-decimal notation* (e.g., 192.168.254.1).
- **IP Netmask:**
  Specifies the IP subnet mask that corresponds to the range of IP addresses defined above. This value must be entered as an IPv4 subnet mask in *dotted-decimal notation* (e.g., 255.255.255.0).
- **Default Router:**
  Specifies the IP address of a default *gateway*, or router, to be provided to DHCP clients. This value must be entered as an IPv4 address expressed in *dotted-decimal notation* (e.g., 192.168.254.254).

  or Self:
  Specifies that the SpeedStream router is to be used as the default gateway.
- **DNS IP Address:**
  Specifies the 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. This value must be entered as an IPv4 address expressed in *dotted-decimal notation* (e.g., 192.168.254.254).

or Use WAN:
Specifies that the DNS server address received from the WAN-side DHCP server is to be provided to DHCP clients on the LAN.

- **Domain Name:**
  Specifies the DNS *domain name* for the DHCP server resident on your SpeedStream device. This value must be entered as an alpha-numeric string. This parameter is optional.

- **Lease Time:**
  IP addresses are *leased* from the DHCP server and are valid for a specified period of time, the *lease time.* 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 that the client's connection no longer exists, and the server will release the IP address assigned to the client and return the address back to the pool of available addresses.

- **or Infinite Time:**
  Leaves the lease time open-ended, preventing the server from releasing the IP address.

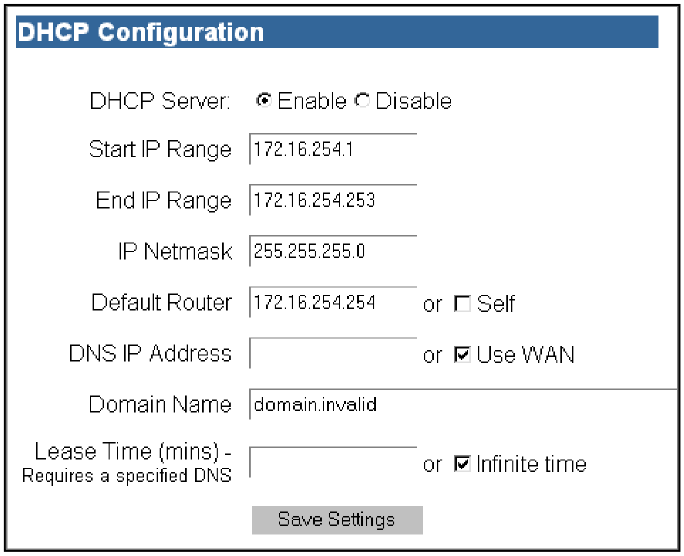
To specify the DHCP configuration settings:

The DHCP operating mode defaults to **Enable**, and the system auto-generates the current IP address range, IP netmask, and default router. If you are using a static IP address, you may need to disable DHCP and enter different addresses in the text boxes. Contact your ISP or network administrator for additional information.

1. Select the DHCP operating mode:

   If you select **Disable**, skip to step 3.

2. Enter the range of IP addresses (**Start IP Range** and **End IP Range**) and the corresponding subnet mask **(IP Netmask)** to be managed by the DHCP server. (You may need to contact your ISP for this information.)



DHCP Configuration

DHCP Server:	● Enable ○ Disable
Start IP Range	172.16.254.1
End IP Range	172.16.254.253
IP Netmask	255.255.255.0
Default Router	172.16.254.254 or □ Self
DNS IP Address	or ☑ Use WAN
Domain Name	domain.invalid
Lease Time (mins) - Requires a specified DNS	or ☑ Infinite time

3. To use your SpeedStream router as the default router, select **Self**. (This is the most common choice.)

   - or-

   Enter the IP address of the default router. (You may need to contact your ISP or network administrator for this information.)

4. To use the DNS server provided by your ISP, select **Use WAN**. (This is the most common choice.)

   - or -

   To specify a WAN-side DNS server to be used by the LAN, enter the **DNS IP Address**.

5. Enter the domain name. This information may be provided by your ISP.

6. Enter the lease time, in minutes, to specify the amount of time that a DHCP lease should be provided the host (requires that you specify a DNS IP address).

   - or –

   Select **Infinite time** to hold the lease until you go back in and change these settings.

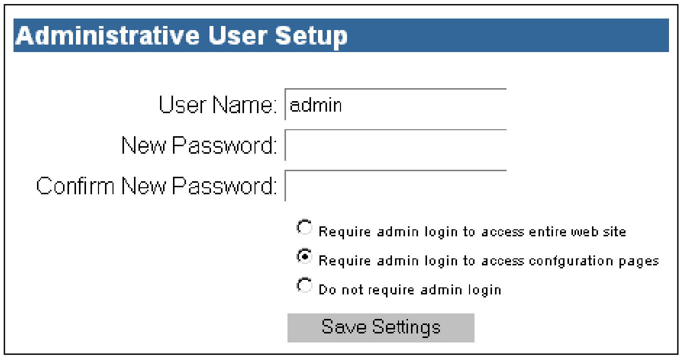
7. To apply the data you entered, click **Save Settings**.

   A confirmation screen displays.

User Setup (System Login)

After you have initially set your user name and password, the **System Status** screen will display the next time you log on to the Web interface. To change the system user name and/or password, you must open the **Administrative User Setup** screen from the main menu.

To change the user name or password:



Administrative User Setup

User Name: admin
New Password:
Confirm New Password:

○ Require admin login to access entire web site
● Require admin login to access confguration pages
○ Do not require admin login

1. From the main menu, click **User Setup**.

   The **Administrative User Setup** screen displays.

2. If you Want to change the user name, enter the new name in the **User Name** box.

3. Enter the new password in both the **New Password** and **Confirm New Password** boxes.

4. Select the login security level you prefer:

   - **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 **OK**.

   The **System Status** screen displays.

- (For more information, visit the ICSA site at http://www.icsalabs.com)

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 Time (UTC), the international time standard. The system date and time are set and corrected automatically via the designated server(s).

Time Client Configuration Options

- **Primary Server IP Address**:
  Specifies the primary IP address of a "well-known" Network Time Protocol Server (NTPS).

- **Secondary Server IP Address**:
  Specifies the secondary IP address of a "well-known" NTPS. If the router does not receive a response from the primary NTPS, it will switch to the secondary.

To configure the Time Client:

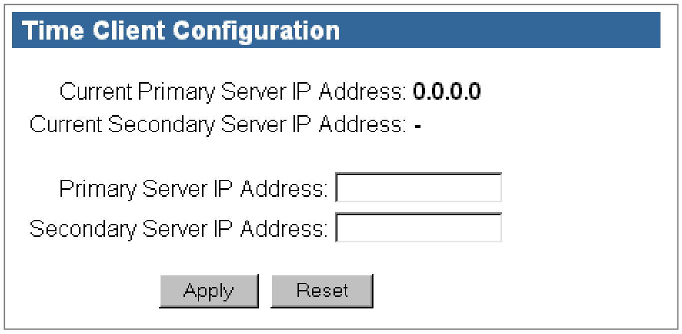
1. On the main menu, click **Advanced Setup**, and then click **Time Client.**

   The **Time Client Configuration** screen displays.

2. Enter the **Primary Server IP Address** for the time server.

3. If applicable, enter the **Secondary Server IP Address** for the time server.

4. To save the settings, click **Apply**.



Time Client Configuration

Current Primary Server IP Address: **0.0.0.0**
Current Secondary Server IP Address: **-**

Primary Server IP Address:
Secondary Server IP Address:

Static Routes

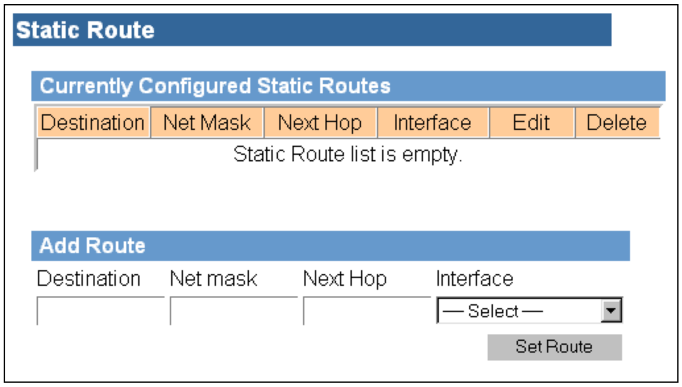
Your SpeedStream DSL router directs data traffic by "learning" source and destination information, then building a routing table. In some cases, network mappings cannot be learned because of incompatible addressing schemes; or learned paths other than the desired source and destination may be possible. In these situations, *Static Routes* can be configured to map these pathways, eliminating the need for the router to learn them.

To add a static route:

1. On the main menu, click **Advanced Setup**, and then click **Static Routes.**

   The **Static Routes** screen displays.

2. In the **Destination** box, enter the IP address of the destination server.



Static Route

Currently Configured Static Routes

Destination	Net Mask	Next Hop	Interface	Edit	Delete
Static Route list is empty.					

Add Route

Destination	Net mask	Next Hop	Interface
			— Select —

3. In the **Netmask** box, enter the IP netmask of the destination server.

4. In the **Next Hop** box, enter the IP address to which the data packets will be forwarded.

5. From the **Interface** list, select the interface that will forward the data packets.

6. To create the static route from your settings, click **Set Route**.

NAT/NAPT Server

The SpeedStream router provides you with several options for using Network Address Translation (NAT) and Network Address Port Translation (NAPT):

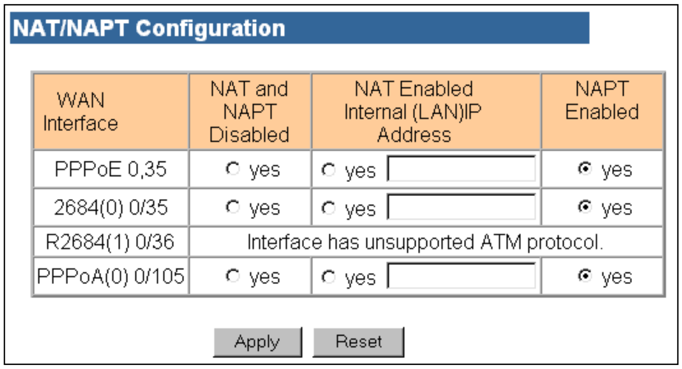
- Use NAT and specify the destination IP address for incoming packets on the selected WAN interface.
- Use NAPT only to handle multiple addresses based on port forwarding rules.
- Disable both NAT and NAPT and, for example, set up static routes.

Note Depending on your configuration, NAT is sometimes enabled by default. Disable NAT only in advanced situations where the ISP has assigned static IP addresses.

To access the NAT/NAPT Configuration screen:

1. On the main menu, click **Advanced Setup**, and then click **NAT/NAPT**.

   The **NAT/NAPT Configuration** screen displays your configured PPP connections in the **WAN Interface** column.



NAT/NAPT Configuration

WAN Interface	NAT and NAPT Disabled	NAT Enabled Internal (LAN)IP Address	NAPT Enabled
PPPoE 0,35	○ yes	○ yes	● yes
2684(0) 0/35	○ yes	○ yes	● yes
R2684(1) 0/36	Interface has unsupported ATM protocol.		
PPPoA(0) 0/105	○ yes	○ yes	● yes

2. Continue to define NAT and/or NAPT settings as described below.

To disable NAT and NAPT:

1. In the **NAT and NAPT Disabled** column, select **yes**.

2. To save your setting, click **Apply**.

   - or -

   Continue to define NAT and/or NAPT settings.

To enable NAT and specify a destination IP address:

1. In the **NAT Enabled Internal (LAN) IP Address** column, select **yes**.
2. Enter the IP address for incoming packets on the selected WAN interface.
3. To save your settings, click **Apply**.

   - or -

   Continue to define NAT and/or NAPT setting.

To enable NAPT:

1. In the **Specify External (WAN) IP Address** box, enter a WAN IP address.
2. To initialize your setting, click **Apply**.

   - or -

   Continue to define NAT and/or NAPT settings.

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 forwarded to the selected IP address on the LAN.

In order to provide such access, your SpeedStream router may be configured to forward certain inbound traffic from the WAN-side to a specified LAN-side server. WAN-side connections have knowledge of, and hence direct access to, only the known *public* IP address associated with the WAN-side interface of your SpeedStream device.

This methodology is commonly referred to as *port forwarding*, and is implemented by means of a *Network Address Port Translation* (NAPT) operation.

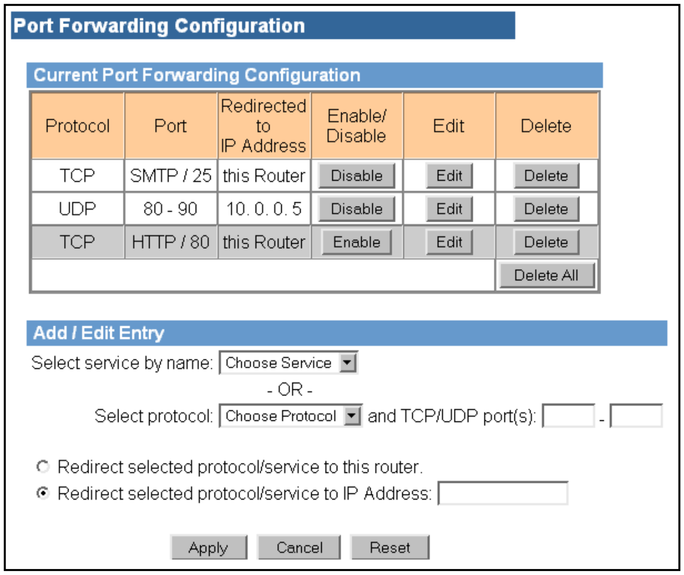
Port Forwarding Configuration Options

- **Select service by name:**
  You can select either a service name or protocol to which the port forwarding rule will be applied.

- **Select protocol:**
  To apply the port forwarding rule to a protocol, select **TCP**, **UDP**, **ICMP** or **GRE** from the **Protocol** list.

- **Enter port range for TCP/UDP protocol:**
  Required if you selected the TCP or UDP protocol, you must also define either a single port or range of ports.

- **Redirect selected protocol/service to this router/IP address:**
  Select this option if the server for the previously specified service or protocol resides on the router.



Port Forwarding Configuration

Current Port Forwarding Configuration

Protocol	Port	Redirected to IP Address	Enable/ Disable	Edit	Delete
TCP	SMTP / 25	this Router	Disable	Edit	Delete
UDP	80 - 90	10. 0. 0. 5	Disable	Edit	Delete
TCP	HTTP / 80	this Router	Enable	Edit	Delete
					Delete All

Add / Edit Entry

Select service by name: Choose Service ▾

- OR -

Select protocol: Choose Protocol ▾ and TCP/UDP port(s): ___ - ___

○ Redirect selected protocol/service to this router.

● Redirect selected protocol/service to IP Address: ___

- **Redirect selected protocol/service to IP address:**
  Select this option if the server for the previously specified service or protocol resides on a host located on the LAN. In this case, you must specify the IP address of the host on which the server resides. (This option is usually selected.)

To edit an existing port forwarding configuration:

1. On the main menu, click **Advanced Setup**, and then click **Port Forwarding**.

   The **Port Forwarding Configuration** screen displays.

2. In the **Current Port Forwarding Configuration** table, click **Edit** in the row that you wish to reconfigure.

   The **Add/Edit Entry** data refreshes and displays the current configuration for the selected protocol.

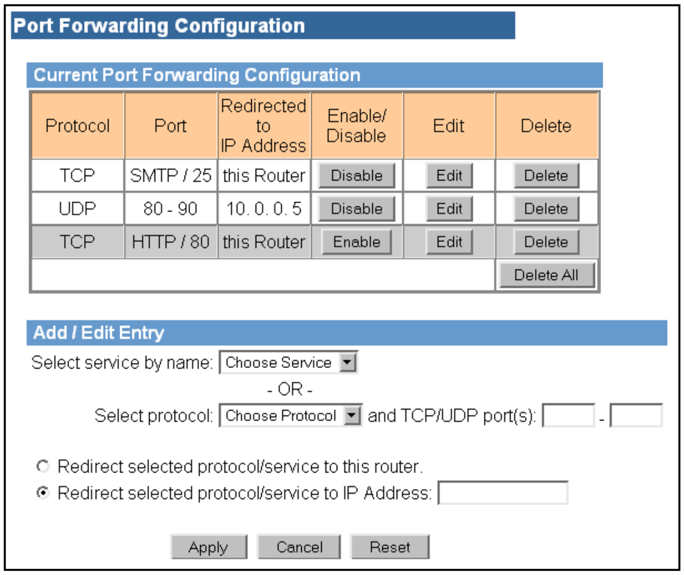
3. Enter your changes (see **Port Forwarding Configuration Options**).

4. To save your settings, click **Apply.**

To delete an existing entry:

- In the **Current Port Forwarding Configuration** table, click **Delete** in the row that you wish to remove.

  The entry is deleted, and the table refreshes.



Port Forwarding Configuration

Current Port Forwarding Configuration

Protocol	Port	Redirected to IP Address	Enable/ Disable	Edit	Delete
TCP	SMTP / 25	this Router	Disable	Edit	Delete
UDP	80 - 90	10. 0. 0. 5	Disable	Edit	Delete
TCP	HTTP / 80	this Router	Enable	Edit	Delete
					Delete All

Add / Edit Entry

Select service by name: Choose Service ▾

- OR -

Select protocol: Choose Protocol ▾ and TCP/UDP port(s): ____ - ____

○ Redirect selected protocol/service to this router.

● Redirect selected protocol/service to IP Address: ____

Apply Cancel Reset

To delete all entries in the table:

- In the last row of the table, click **Delete All**.

  All port forwarding rules listed in the **Configured Ports** table are deleted and the table refreshes.

To add a port forwarding entry:

1. From the **Choose Protocol** list, select **TCP**, **UDP**, **ICMP**, or **GRE**.

2. If you select **TCP** or **UDP**, select a service from the **Choose Service** list.

   - or -

   Enter a port number in the **Port Number** box.

3. If you want inbound traffic forwarded to the SpeedStream router, select **Redirect selected protocol/service to this router**.

   - or -

   To enter a specific IP address, select **Redirect selected protocol/service to IP Address** and enter the address in the text box.

4. To save your settings, click **Apply.**

Firewall

Your SpeedStream router includes a user-configurable firewall that provides various levels of security against outside attacks. This firewall provides only WAN-side protection. The firewall does not provide any LAN-side protection.

The firewall also includes an advanced *Attack Detection System (ADS)* containing various algorithms to detect and identify WAN attacks the moment they start and protect the LAN from such attacks. Though WAN access may be temporarily hindered, the LAN is protected from such harmful traffic load.

Firewall Security Levels

The SpeedStream router is shipped with a set of preconfigured firewall database rules grouped into levels, allowing you to easily configure the firewall. The default set of levels include:

- **Off:**
  No restrictions are applied to either inbound or outbound traffic. In addition, all *Network Address Port Translation* (NAPT) functionality is disabled - there is no address/port translation. Since 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 Gateways* (ALGs). The only inbound traffic that is allowed is that which is received within the context of an outbound session initiated on the local host and permitted by this firewall mode.

- **Medium:**
  Moderate restrictions with respect to outbound traffic. Outbound traffic is allowed for most supported IP-based applications and *Application Level Gateways* (ALGs). The only inbound traffic that is allowed is that which is received within the context of an outbound session initiated on the local host and permitted by this firewall mode.

- **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 that is allowed is that which is 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.

Note For specific application and protocol security modes, refer to Appendix D, “Firewall Security Levels.”

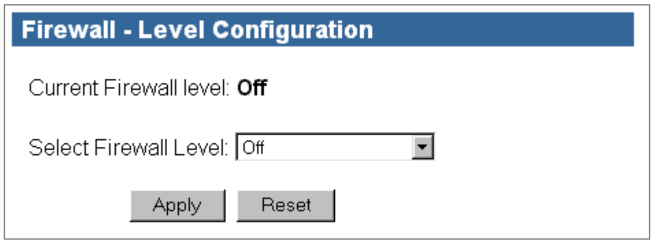
To select the firewall security level:

1. On the main menu, click **Advanced Setup**, then click **Firewall**, and then click **Simple Setup**.

   The **Firewall – Simple Setup & Control** screen displays.

2. Select the level from the **Select Firewall Level** list.

3. To accept your selection, click **Apply**.



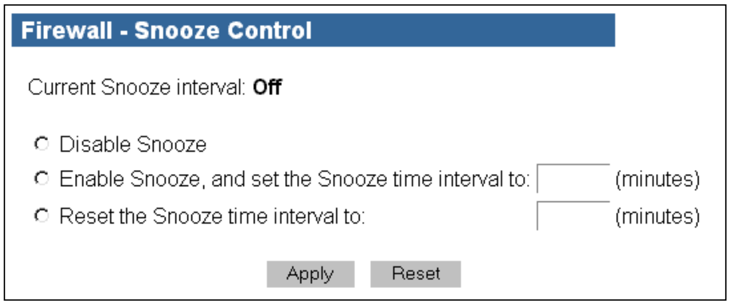
Firewall - Level Configuration

Current Firewall level: **Off**

Select Firewall Level: Off

Firewall Snooze Control

The firewall supports a Snooze feature by which , the firewall can be made to temporarily "sleep," or go into an *Off* state, for a specified period of time. The firewall will restore itself to its previous state after the specified time period elapses.



Firewall - Snooze Control

Current Snooze interval: **Off**

○ Disable Snooze

○ Enable Snooze, and set the Snooze time interval to: (minutes)

○ Reset the Snooze time interval to: (minutes)

To disable Snooze and allow the firewall to become active:

1. Select **Disable Snooze**.
2. Click **Apply**.

To enable Snooze, temporarily disabling the firewall:

1. Select the **Enable Snooze** option.
2. Enter the number of minutes you Want the firewall disabled.
3. Click **Apply** to accept the settings.

To reset the Snooze time interval:

1. During the active Snooze time interval, select **Reset the Snooze time interval to:**
2. Enter the number of minutes you Want the firewall further disabled.
3. Click **Apply** to accept the settings.

DMZ Settings

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.

DMZ Configuration Options

- **Host Name Setting:**

This feature was added to the DMZ configuration to assist with the dynamic nature of DHCP. Typically, the DMZ host is selected by entering the host's IP address on the configuration screen. However, if the host does not have a static IP address and uses DHCP, you will not immediately know what the new IP address is after a reboot or reset. In *host name mode*, the router will "remember" the MAC address of the selected host. When the DHCP server gives out an IP address to that MAC address, it will also update the DMZ module with the new IP address.

In order for this feature to work effectively, you need to set the host name of each of the hosts running DHCP. In Windows, this is called "Computer Name" and is set in a variety of places, depending on the operating system you are running. (Please refer to your Windows documentation or Windows online Help for specific instructions on designating the computer name.)

- **Temporary DMZ Settings:**
  The SpeedStream router allows you to temporarily override the "persistent" DMZ status, which normally remains the same, either on or off, even after rebooting. This feature was designed to accommodate certain games and applications that do not work well behind a NAPT router. Usually, the simplest way to make them work is by directing the router's DMZ at the computer running the game. However, you may not Want to always have the game machine set as the DMZ host, since it might affect security issues. In this case, you would select it as a *temporary* host. Once the specified time expires or the router is rebooted, the DMZ will return to the persistent host or disable itself if no persistent host was selected.

  The persistent/temporary setting options are:

  – **Make settings permanent:**
  Host settings will be persistent.

  – **Make settings last until modem reboots:**
  Host settings will return to persistent mode after router reboots.

  – **Make settings last for XX minutes:**
  Host settings will be in effect for specified number of minutes, then will disable or return to persistent mode.

To enable DMZ and specify an accessible computer:

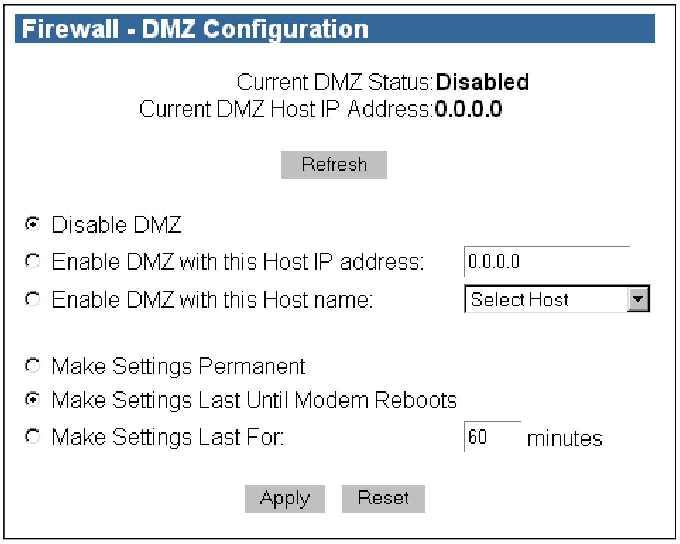
1. On the main menu, click **Advanced Setup**, then click **Firewall**, and then click **DMZ**.

   The **Firewall – DMZ Configuration** screen displays.

2. Select **Enable DMZ, and set the DMZ Host IP address to**.

3. Enter the IP address of the machine to be accessible to inbound traffic.

4. To accept the settings, click **Apply**.



Firewall - DMZ Configuration

Current DMZ Status: **Disabled**
Current DMZ Host IP Address: **0.0.0.0**

● Disable DMZ
○ Enable DMZ with this Host IP address: 0.0.0.0
○ Enable DMZ with this Host name: Select Host

○ Make Settings Permanent
● Make Settings Last Until Modem Reboots
○ Make Settings Last For: 60 minutes

To disable DMZ:

1. On the **Firewall – DMZ Configuration** screen, click **Disable DMZ**.
2. To accept the settings, click **Apply**.

Custom IP Filter Rules

You can configure the SpeedStream Router firewall to perform IP filtering and stateful inspection of packets. The firewall supports a rules database to allow sophisticated access tailoring. A network conversation is first authorized by verifying the packet against the current rules database configured within the firewall. If the first packet of a conversation is allowed, then a dynamic state engine takes over and tracks that conversation. All protocols are tracked whether they are stream-based or not; i.e., ICMP, UDP, TCP, GRE.

The filtering rules database gives you control over the configurable firewall rules. 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.

Note You must have previously selected **Custom Level** in the **Firewall - Simple Setup & Control** screen.

Cloning a Rule Definition

You can create a new set of custom IP filter rules from one of the existing preconfigured firewall levels. (See screenshot on next page.)

To clone an IP filter rule:

1. In the **Clone Rules Definitions** box, select the firewall level to copy.
2. Click **Clone Rule Set**. The Rules table refreshes to display the new rules for that level.
3. If you Want to change any of a rule’s criteria, click **Edit** in the row of that rule, and then complete steps 1 through 5 as relevant (refer to the following section for detailed instructions.)

Creating Custom IP Filter Rules

You can create a new filter rule based on criteria you enter.

Note You must have selected the **Custom** firewall level from the **Firewall – Simple Setup** screen.

The following instructions reference the step numbers on the **Firewall – Custom IP Filter Configuration** screen.

Step 1: Fill in the following information:

1. In the **Rule No.** text box, enter an unused rule number. If you enter a number that is already in the rules database, an error message will display.

2. In the **Access** drop-down list box, select the access value, **Permit** or **Deny**.

3. In the **Direction** drop-down list box, select whether the rule applies to **Inbound** or **Outbound** packet traffic.

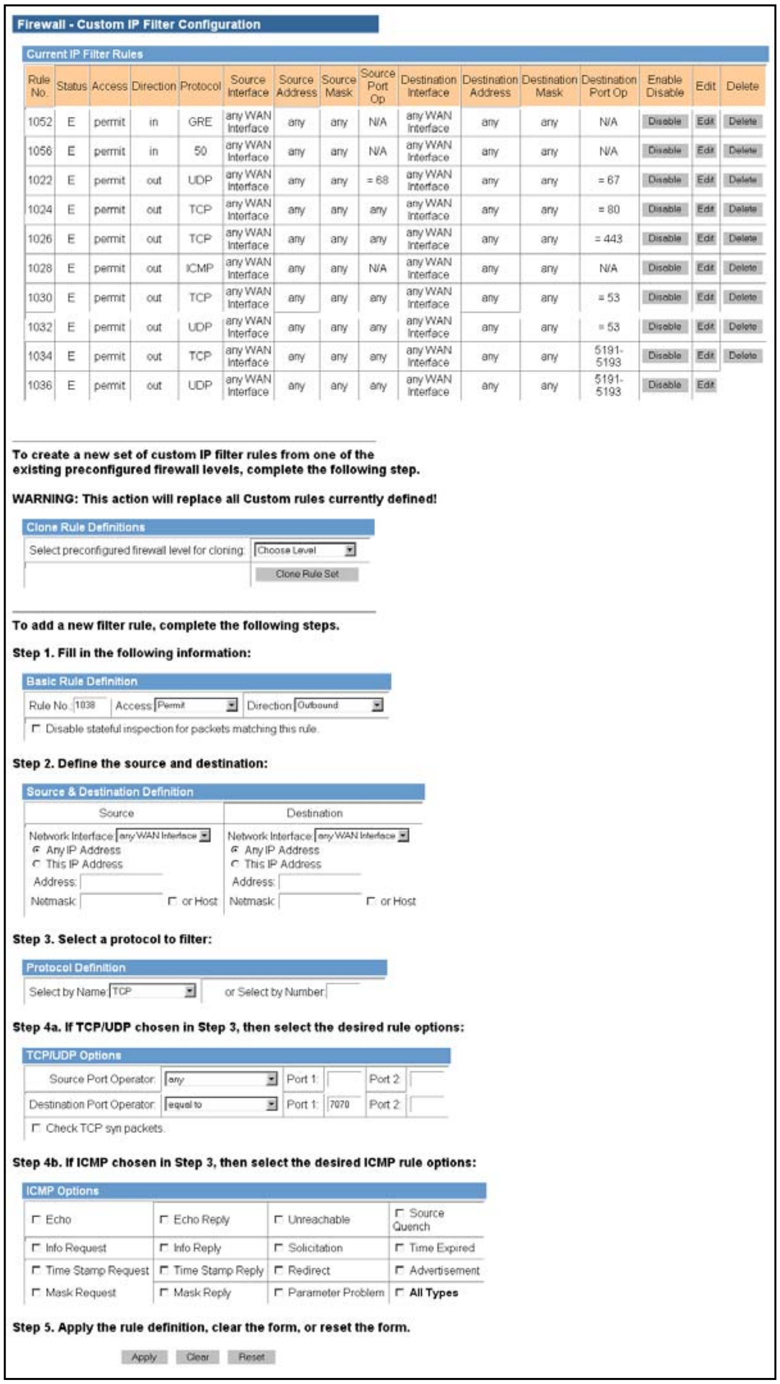
4. To prevent the firewall from creating a stateful inspection session for packets matched on this rule, select the **Keep stateless** check box.

Step 2: Define the source and destination:

1. In the **Network Interface** list under the **Source** heading, select the **Network Interface**.

2. Designate whether the source is any IP address or a specific address; if the latter, enter the IP address and netmask.

3. Repeat the previous steps to specify the **Destination** criteria.



Firewall - Custom IP Filter Configuration

Current IP Filter Rules

Rule No.	Status	Access	Direction	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Enable Disable	Edit	Delete
1052	E	permit	in	GRE	any WAN Interface	any	any	N/A	any WAN Interface	any	any	N/A	Disable	Edit	Delete
1056	E	permit	in	50	any WAN Interface	any	any	N/A	any WAN Interface	any	any	N/A	Disable	Edit	Delete
1022	E	permit	out	UDP	any WAN Interface	any	any	= 68	any WAN Interface	any	any	= 67	Disable	Edit	Delete
1024	E	permit	out	TCP	any WAN Interface	any	any	any	any WAN Interface	any	any	= 80	Disable	Edit	Delete
1026	E	permit	out	TCP	any WAN Interface	any	any	any	any WAN Interface	any	any	= 443	Disable	Edit	Delete
1028	E	permit	out	ICMP	any WAN Interface	any	any	N/A	any WAN Interface	any	any	N/A	Disable	Edit	Delete
1030	E	permit	out	TCP	any WAN Interface	any	any	any	any WAN Interface	any	any	= 53	Disable	Edit	Delete
1032	E	permit	out	UDP	any WAN Interface	any	any	any	any WAN Interface	any	any	= 53	Disable	Edit	Delete
1034	E	permit	out	TCP	any WAN Interface	any	any	any	any WAN Interface	any	any	5191-5193	Disable	Edit	Delete
1036	E	permit	out	UDP	any WAN Interface	any	any	any	any WAN Interface	any	any	5191-5193	Disable	Edit	

To create a new set of custom IP filter rules from one of the existing preconfigured firewall levels, complete the following step.

WARNING: This action will replace all Custom rules currently defined!

Clone Rule Definitions

Select preconfigured firewall level for cloning: Choose Level
Clone Rule Set

To add a new filter rule, complete the following steps.

Step 1. Fill in the following information:

Basic Rule Definition

Rule No.: 1038 Access: Permit Direction: Outbound
□ Disable stateful inspection for packets matching this rule.

Step 2. Define the source and destination:

Source & Destination Definition

Source	Destination
Network Interface: any WAN Interface	Network Interface: any WAN Interface
● Any IP Address	● Any IP Address
○ This IP Address	○ This IP Address
Address:	Address:
Netmask: □ or Host	Netmask: □ or Host

Step 3. Select a protocol to filter:

Protocol Definition

Select by Name: TCP or Select by Number:

Step 4a. If TCP/UDP chosen in Step 3, then select the desired rule options:

TCP/UDP Options

Source Port Operator:	any	Port 1:		Port 2:	
Destination Port Operator:	equal to	Port 1:	7070	Port 2:	

□ Check TCP syn packets.

Step 4b. If ICMP chosen in Step 3, then select the desired ICMP rule options:

ICMP Options

□ Echo	□ Echo Reply	□ Unreachable	□ Source Quench
□ Info Request	□ Info Reply	□ Solicitation	□ Time Expired
□ Time Stamp Request	□ Time Stamp Reply	□ Redirect	□ Advertisement
□ Mask Request	□ Mask Reply	□ Parameter Problem	□ **All Types**

Step 5. Apply the rule definition, clear the form, or reset the form.

Step 3: Select a protocol to filter:

- In the **Select by Name** list box, select the protocol name.

  - or -

  In the **Select by Number** text box, enter
  the protocol number.

Depending on the protocol you selected in Step 3, select the applicable rule options:

- If you selected TCP/UDP in Step 3, go to **Step 4a**.
- If you selected ICMP in Step 3, go to **Step 4b**.
- If you selected any other protocol in Step 3, go to **Step 5**.

Step 4a: If TCP/UDP chosen in Step 3, select the desired rule options:

1. Specify **Source Port Operator** options:
   - Select the source port operator.
   - Enter the first port number.
   - If applicable, enter the second port number.

2. Specify **Destination Port Operator** options:
   - Select the destination port operator.
   - Enter the first port number.
   - If applicable, enter the second port number.

- If applicable, select Apply rule only to TCP connections that are already established.
- If applicable, select Check syn packets for TCP connectors.

Step 4b. If ICMP chosen in Step 3, select the desired ICMP rule options.

- From the table, select one or multiple options; or click **All Types** to automatically select all options.

Step 5. Apply the rule definition, clear the form, or reset the form.

- To accept the settings, click **Apply**.

ADS (Attack Detection System)

The firewall Advanced Attack Detection System (ADS) contains various algorithms to detect and identify WAN attacks the moment they start and protect the LAN from such attacks. Though WAN access may be temporarily hindered, the LAN is protected from harmful traffic.

ADS typically looks for two types of packets: *malformed* packets and *spoofed source address* packets.

- Malformed packets have been purposefully constructed with errors in them. These are used to crash systems that don't properly handle the errors. This type of attack usually happens against large sites rather than home users.

- Packets with spoofed source addresses are commonly sent to smaller hosts, not with the intent of bringing down a particular computer, but rather to take down a large host through a mechanism called *Distributed Denial of Service (DDoS).* In this situation, when a huge number of computers are used to request services, those services are rendered unavailable because of the traffic load.

The ADS generates a log entry for a particular type of attack once per minute. Consequently, there will be multiple entries for long-term attacks. This lets the user know the period of time that the attack persisted.

Background

TCP/IP (Transmission Control Protocol/Internet Protocol) is the "language" computers that make up the Internet (called *hosts*) use to talk to each other. Basically, *TCP* and *IP* dictate the meaning of two sets of tags (or headers) that are added to user data before being sent. An *IP header* contains a *destination address* and a *source address* that tell all of the hosts delivering the data where it is supposed to go, much like an envelope for an inter-office memo. A *TCP header* is similar to a subject line on the memo: it contains information that allows the recipient to quickly figure out what the data is and where it goes once the IP "envelope" has been removed. The combination of a block of data and its associated TCP and IP headers is often referred to as a *packet*.

The part of a host that writes and reads the TCP and IP headers is called a *network stack*. Almost all network stacks have flaws in them (some more than others!) due to intolerance to improper or invalid headers. This can result in a variety of problems from computer crashes to security breaches. While newer protocols attempt to address these issues (e.g., IPSec), the current version of IP, called *IPv4*, will be here to stay for some time, flaws and all. This is where the SpeedStream Attack Detection System (ADS) comes in.

Types of Attack

The two most common attack types are *unauthorized access* and *Denial of Service (DoS)*. Someone guessing your login password is one example of unauthorized access; unfortunately, an external device like the SpeedStream router is unable to do much to prevent that except perhaps have a firewall rule that limits which hosts may log in. The SpeedStream ADS, however, can block attempts by external (WAN) hosts to "impersonate" a LAN host in order to gain access to weakly protected data services on other LAN connected computers.

DoS attacks take several forms, but the basic intended effect is the same: to prevent a host from accessing other hosts, or preventing other hosts from accessing it. In effect, this kicks the host off the Internet. One type of DoS attack sends more data to a host than its connection can handle. Little can be done about this attack without having the Internet Service Provider block it upstream.

Another type of DoS attack attempts to crash the host by sending bad data to its network stack. The SpeedStream ADS as described below can filter several popular incarnations of this attack. One way in which the bad data is created is by *spoofing*, or modifying, the source address in the IP header. Normally, when a host sends a packet to another host, it puts its address in the IP header so the other host knows where it came from.

While most small users will never be on the receiving end of a direct DoS attack, a new twist to the DoS does quite often take advantage of broadband-connected Internet hosts. Instead of attempting to generate enough data to flood a large Internet host's connection, a would-be attacker instead "convinces" hundreds or thousands of other hosts to do it for him. This is called a *Distributed Denial of Service (DDoS)*. Several viruses can turn a host into a remote-controlled "zombie," although some attacks can simply use a host's network stack to do the job if it is too trusting. The SpeedStream ADS monitors this behavior.

ADS Configuration Options

The SpeedStream Attack Detection System filters (i.e., discards) and/or logs the following attack attempts from the WAN:

- **Same Source and Destination Address (a.k.a. *Land Attack*):**
  This packet has a spoofed source IP address set to be the same as the destination host and can result in the DoS or crash of the local host. 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 (a.k.a. *Smurf or Fraggle Attack*):**
  This packet has a spoofed source IP address set to the "broadcast" address. Most hosts only accept packets destined for their own IP address, but there are a couple of special IP address called broadcast addresses that hosts will also accept in addition to their own. The broadcast address is invalid as a packet's source address, however, because a packet has to come from a host. If a network stack does respond to a packet with a broadcast source address, the response will be sent to the broadcast address on which all of the hosts on the subnet are listening. All of the hosts that received the broadcast would then respond back to the host flooding it with data, possibly making inaccessible to other users.

- **LAN Source Address On WAN:**
  This packet has a spoofed source address set to be a typical trusted LAN address. One method of separating a LAN from a WAN is through the use of NAPT. This allows the LAN to use IP addresses that are normally not accessible by WAN hosts and, therefore, helps shield the LAN from WAN attacks. A packet with a LAN source address coming from the WAN is attempting to masquerade as a LAN packet so that it might be trusted by a LAN host and received.

- **Invalid IP Packet Fragment (a.k.a. *Ping of Death*):**
  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. If each stage of reassembly is not carefully checked by the receiving host's network stack, a specially crafted invalid fragment can cause the host to crash.

- **TCP NULL Flags:**
  The TCP header contains a set of "flags" that indicate information about the packet which is used by receiving host to process it. At least one TCP flag must be set, but for a TCP NULL flags packet, none were. This packet can cause some hosts to crash.

- **TCP FIN Flag:**
  The TCP FIN flag should never appear in a packet by itself. This packet can cause some hosts to crash.

- **TCP Xmas Flags:**
  The TCP Xmas flag configuration is an invalid combination of the FIN, URG and PUSH flags. This packet can cause some hosts to crash.

- **Fragmented TCP Packet:**
  As discussed in the Invalid IP Packet Fragment description, packets may be fragmented in transit. While it is entirely valid to fragment a TCP packet, this is rarely done because of a process called "MTU discovery" that occurs when two hosts begin communicating. The rarity of TCP packet fragmentation makes its occurrence suspicious and could indicate a flawed network stack exploit attempt.

- **Fragmented TCP Header:**
  This indicates that the TCP header in the packet was split into multiple IP fragments. This never normally occurs and is most likely a flawed network stack exploit attempt.

- **Fragmented UDP Header:**
  This indicates that the IP header in the packet was split into multiple IP fragments. This never normally occurs and is most likely a flawed network stack exploit attempt.

- **Fragmented ICMP Header:**
  This indicates that the ICMP header in the packet was split into multiple IP fragments. This never normally occurs and is most likely a flawed network stack exploit attempt.

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 allows one to tell that a long-term attack is taking place without completely filling up the firewall log with entries for every single packet.

To enable ADS:

- On the main menu, click **Advanced Setup**, then click **Firewall**, and then click **ADS**.

  The **Attack Detection System Configuration** screen displays.

To globally enable ADS without losing any of the individual packet types:

- Select **Enable Attack Detection**.

To filter, or drop, a packet type:

- Select **Filter** to the right of the desired option.

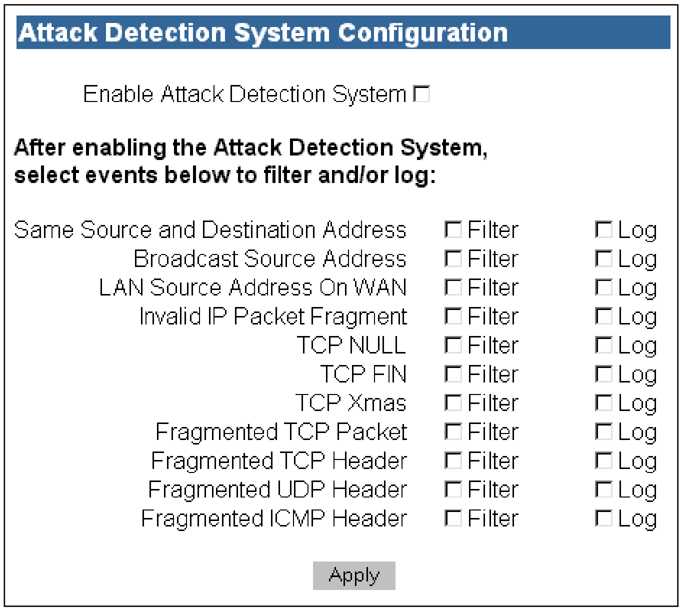
To log a packet type to the Firewall Event Log:

- Select **Log** to the right of the desired function.

Note Filtering and logging are independent operations. You can select either, neither or both.

To save the new settings:

- Click **Apply**.



Attack Detection System Configuration

Enable Attack Detection System □

After enabling the Attack Detection System, select events below to filter and/or log:

Same Source and Destination Address	□ Filter	□ Log
Broadcast Source Address	□ Filter	□ Log
LAN Source Address On WAN	□ Filter	□ Log
Invalid IP Packet Fragment	□ Filter	□ Log
TCP NULL	□ Filter	□ Log
TCP FIN	□ Filter	□ Log
TCP Xmas	□ Filter	□ Log
Fragmented TCP Packet	□ Filter	□ Log
Fragmented TCP Header	□ Filter	□ Log
Fragmented UDP Header	□ Filter	□ Log
Fragmented ICMP Header	□ Filter	□ Log

A confirmation screen displays.

RFC2684

Note This option may not be available on your router configuration.

The SpeedStream router supports two basic types of connections, *Point-to-Point (PPP)* and *RFC2684*. Typically, RFC2684 connections rely on a server located on the *Wide Area Network (*WAN) to supply the modem 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 certain 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.

RFC2684 Configuration Options

- **Connection:**
  The connection for which you Want to enable RFC2684.

- **DHCP:**
  Enable/Disable the Dynamic Host Configuration Protocol for this connection.

- **IP Address:**
  The IP address to be used for the WAN-side of the modem, normally obtained from a DHCP server located on the WAN somewhere.

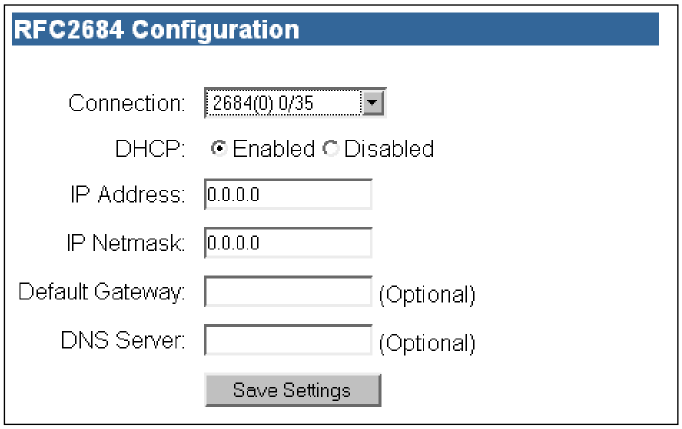
- **IP Netmask:**
  The netmask corresponding to the above IP address.

- **Default Gateway:**
  The IP address of a router located on the WAN to be used as the "gateway" to the WAN.

- **DNS Server:**
  The IP address of a DNS server located on the WAN to be used to resolve domain name/IP addresses.

To configure RFC2684 settings:

1. Select the connection for which you Want to enable RFC2684.



RFC2684 Configuration

Connection: 2684(0) 0/35

DHCP: ● Enabled ○ Disabled

IP Address: 0.0.0.0

IP Netmask: 0.0.0.0

Default Gateway: (Optional)

DNS Server: (Optional)

Contact your Service Provider for the following information.

2. To disable DHCP, select **Disabled**.

3. Enter the **IP Address**.
4. Enter the **IP Netmask**.
5. Enter the **Default Gateway** (optional).
6. Enter the **DNS Server** (optional).

UPnP (Universal Plug and Play)

UPnP is an industry standard networking protocol that enables devices to discover and control each other over a residential network. The SpeedStream router implements the UPnP networking forum specified Internet Gateway Device (IGD) protocol version 1.0. Through UPnP, other devices on the LAN can obtain access to the broadband Internet connection provided by the router.

UPnP Configuration Options

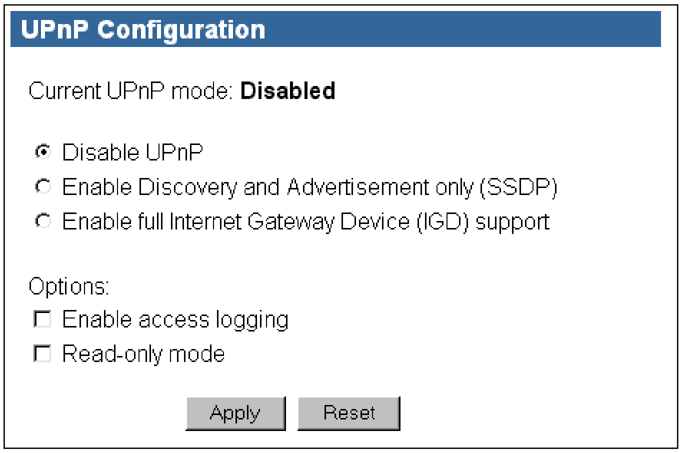
- **Disable UPnP:**
  Shuts down UPnP support within the router.

- **Enable Discovery and Advertisement only (SSDP):**
  Puts the UPnP module in a mode that makes it possible for UPnP clients to discover the router and bring up the router's GUI within a browser, but does not allow the UPnP client to control the router through the UPnP directly.

- **Enable full Internet Gateway Device (IGD) support:**
  Exposes the UPnP module features to all clients, including discovery and control.

- **Enable access logging:**
  Generates a system log message whenever a UPnP client accesses the router.

- **Read-only mode:**
  Restricts the kind of access a 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.



UPnP Configuration

Current UPnP mode: **Disabled**

● Disable UPnP
○ Enable Discovery and Advertisement only (SSDP)
○ Enable full Internet Gateway Device (IGD) support

Options:
□ Enable access logging
□ Read-only mode

To configure UPnP settings:

1. Select the UPnP mode.
2. Enable any options.
3. Click **Apply**.

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). Under the normal mode of operation, referred to as "bridge/routing" mode, the router provides typical routing functionality between the WAN side and the LAN side. However, all LAN-side interfaces are "bridged."

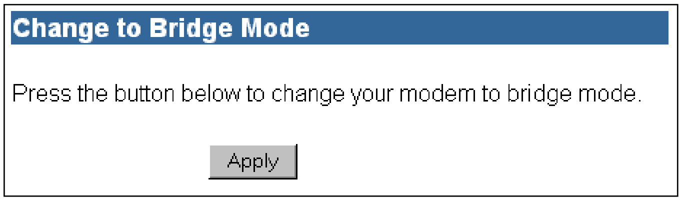
In the second mode of operation, the router provides only "bridging" functionality. This applies to WAN-to-LAN connectivity as well as to all LAN-side interfaces. Point-to-Point (PPP) connections are not available under the bridge mode of operation.

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 modem to factory defaults.

To enable bridge mode:

1. From the main menu, click **Advanced Setup**, and then click **Bridge Mode**.

   The Change to Bridge Mode screen displays.



Change to Bridge Mode

Press the button below to change your modem to bridge mode.

2. Click **Apply**.

   A confirmation screen displays notification that the new setting will not take effect until you reboot the router. You may do so at this point or later.

RIP (Routing Information Protocol)

Under normal circumstances the SpeedStream router does not support routing protocols. However, support for the *Routing Information Protocol* (RIP), versions 1, 2 or 1 and 2, may be activated through the **RIP** page. This support may be configured for any WAN connection currently configured or for the LAN in general.

Routers user RIP to automatically “learn” new routes to other places without human intervention. The router uses a *route* to make decisions on how to forward Internet traffic. It will then use the *routing table* to decide which interface will carry the outbound IP packet. If all routes in the routing table fail, the router will forward the IP packet to its *default route*. When the router boots up, it will *broadcast* its routing table on configured interfaces; i.e., it shares its routing table with other routers that support RIP. This broadcast occurs about every 30 seconds. A router can also “ask” another RIP router for its routing table. If the SpeedStream router receives a valid request, it will respond with the SpeedStream router routing table.

RIP Configuration Options

- **Interface:**
  The system-generated list of LAN or WAN interfaces available for RIP enabling.

- **RIP Version 1:**
  Allows RIP version 1 to be transmitted/received on the selected interface. Currently, RIPv1 is seldom used, but supported on the SpeedStream router.

- **Version 2:**
  Allows RIP version 2 to be transmitted/received on the selected interface. This would be the most common choice.

- **Versions 1 and 2:**
  Simultaneously supports RIP versions 1 and 2 on the selected interface.

- **Active Mode:**
  If enabled, the router will receive routing updates on the selected interface and will broadcast regular routing updates to other routers. If not enabled (default), the router will receive routing updates on this interface, but will not broadcast routing tables.

To configure RIP settings:

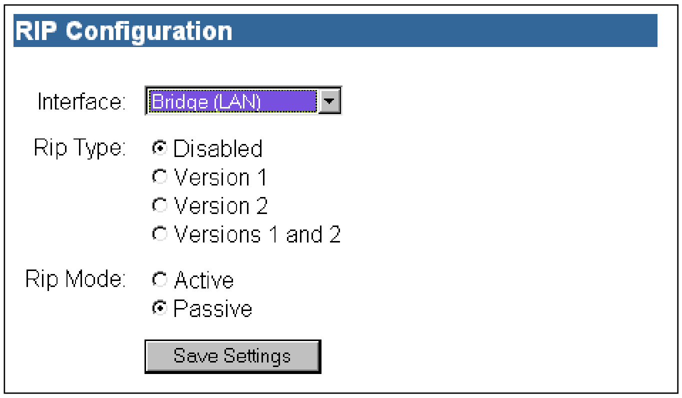
The RIP settings default to all interfaces disabled.

1. In the row of the interface for which you Want to enable RIP, select the RIP version.

2. If you want to enable routing update broadcasts, click the checkbox under **Active Mode**.

3. Click **Apply**.

   A confirmation screen displays notification that the new setting will not take effect until you reboot the router. You may do so at this point or later.


RIP Configuration

Interface: Bridge (LAN)

Rip Type: ● Disabled ○ Version 1 ○ Version 2 ○ Versions 1 and 2

Rip Mode: ○ Active ● Passive

LAN Servers

Servers such as HTTP, FTP and Telnet located on a LAN typically use their “well-known” port values for communication (HTTP/80, FTP/21, Telnet/23). Under some circumstances, it may be necessary or desirable for these servers to use a port value other than the standard one. In such situations, the router must be configured manually with the non-standard port value for each affected server.

Note There is a restriction on the new port values that may be specified for these LAN servers. The new port value must be in the range 1024-59999. Port values below 1024 are reserved for well-known port values, and values above 60000 are used for port forwarding.

System Log

The System Log records 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.

System Log Configuration Options

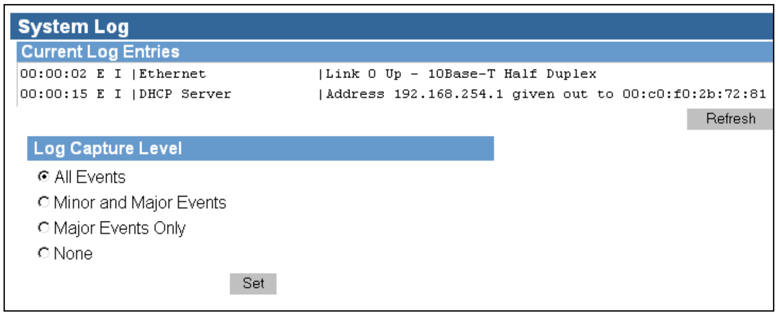
- **All Events**:
  Logs all events.
- **Informative Events**:
  Logs general information about non-critical changes in system status.
- **Minor Events**:
  Logs events that might indicate a condition requiring user intervention, and generates a warning about this change in the system status.
- **Major Events**:
  Logs events that require immediate user attention, and generates a warning about critical conditions or changes in the system status.
- **None**:
  Logs no events.

To configure the System Log:

1. From the main menu, click **Status and Statistics**, and then click **System Log**.

   The **System Log** screen displays.

2. Select the log capture level, and then click **Set**.



```
00:00:02 E I |Ethernet             |Link 0 Up - 10Base-T Half Duplex
00:00:15 E I |DHCP Server          |Address 192.168.254.1 given out to 00:c0:f0:2b:72:81
```

● All Events
○ Minor and Major Events
○ Major Events Only
○ None

Reboot

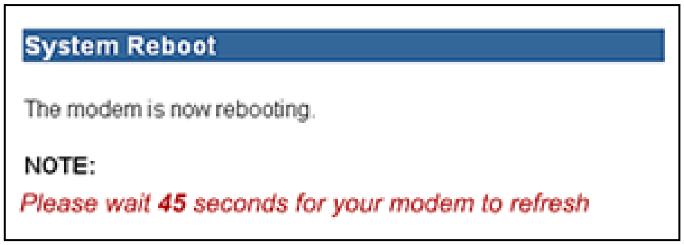
You can shut down and then restart router without losing your current configuration settings.

1. From the main menu, click **Reboot**.

   The **System Reboot** screen displays.

2. Click **Reboot**.

   The **System Reboot** screen displays a countdown while processing. When the router has finished rebooting, the **System Summary** screen displays.



The modem is now rebooting.

NOTE:
Please wait 45 seconds for your modem to refresh

You can also reboot the router by pressing and quickly releasing the **Reset** button located on the bottom of the modem. The **pwr** LED will blink once.

Reset

Note This option may not be available on your router configuration.

If rebooting the router does not resolve the problem, you can reset it to the factory default settings or to the last firmware update.

Important!

- When you reset the router, you will lose any settings you have entered manually.
- Do not disconnect any cables or the power cord while the router is resetting.

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.

Firmware Update

Note This option may not be available on your router configuration.

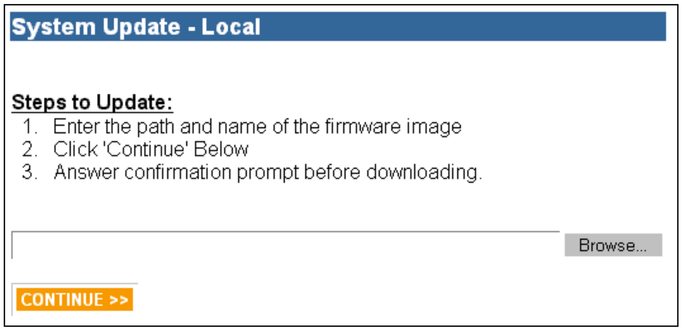
Efficient Networks will occasionally provide *firmware* updates to your ISP, which will notify you when updates are available.

To update the router firmware:

1. Download the update file (*.img) to your hard drive. Note where you save the file.

2. Open the **Tools** menu, and then click **Update**.

   The **System Update – Local** screen displays.



System Update - Local

Steps to Update:

1. Enter the path and name of the firmware image
2. Click 'Continue' Below
3. Answer confirmation prompt before downloading.

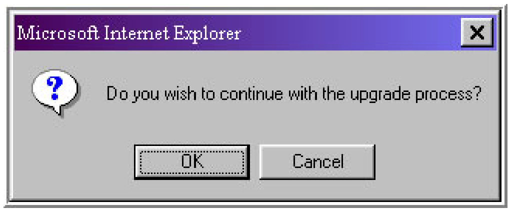
3. Click **Browse** and navigate to the folder that contains the updated firmware (*.img).

4. Select the file, and then click **OK**.

   The file name displays in the **Browse** text box.

5. Click **Continue**.

   A confirmation dialog box displays. (Your browser may display a dialog box that differs from this illustration.)

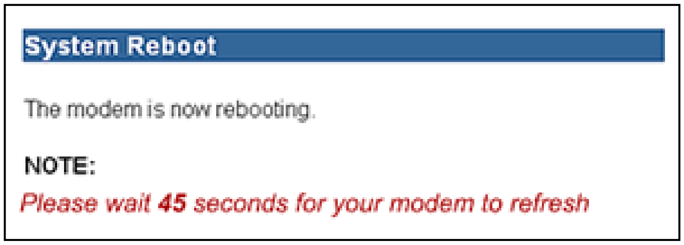


Microsoft Internet Explorer

Do you wish to continue with the upgrade process?

6. Click **OK** to proceed.

   The file is sent to the router. If a valid update file, the router writes the update to its internal flash memory. The **System Reboot** screen displays a countdown during the Flash Write process. When the update is completed, the **Login** screen displays.



System Reboot

The modem is now rebooting.

NOTE:

*Please wait **45** seconds for your modem to refresh*

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.

Diagnostics

Note This option may not be available on your router configuration.

The **Diagnostics** screen allows you to test your DSL service.

1. From the main menu, click **Diagnostics**.

   The **Diagnostics** screen displays.

2. Click **Run Diagnostics** at the bottom of the screen.

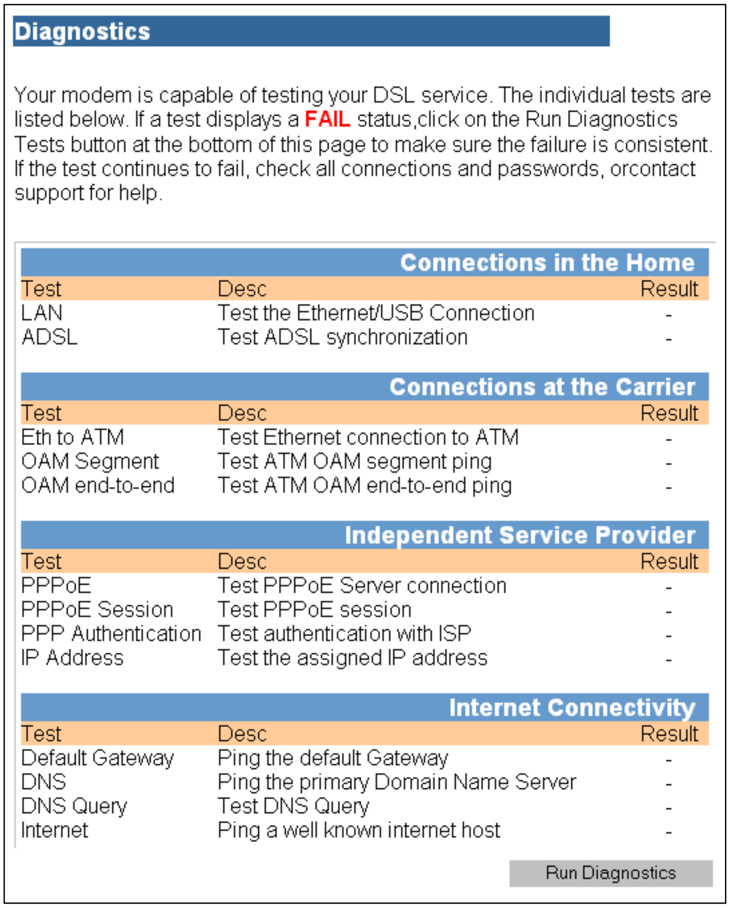
   The test results display under the Results column.

3. If a test displays a **FAIL** status, click **Run Diagnostics** again to confirm the failure.

4. If the test still displays a **FAIL** status, check all connections and passwords; then click **Run Diagnostics** again.

   For failures of **Connections at the Carrier**, **Independent Service Provider**, or **Internet Connectivity** contact your Service Provider.

5. For tests other than those mentioned above, if no change in status after running the diagnostics a second time, contact your Service Provider for further assistance.



Diagnostics

Your modem is capable of testing your DSL service. The individual tests are listed below. If a test displays a **FAIL** status,click on the Run Diagnostics Tests 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, orcontact support for help.

Connections in the Home

Test	Desc	Result
LAN	Test the Ethernet/USB Connection	-
ADSL	Test ADSL synchronization	-

Connections at the Carrier

Test	Desc	Result
Eth to ATM	Test Ethernet connection to ATM	-
OAM Segment	Test ATM OAM segment ping	-
OAM end-to-end	Test ATM OAM end-to-end ping	-

Independent Service Provider

Test	Desc	Result
PPPoE	Test PPPoE Server connection	-
PPPoE Session	Test PPPoE session	-
PPP Authentication	Test authentication with ISP	-
IP Address	Test the assigned IP address	-

Internet Connectivity

Test	Desc	Result
Default Gateway	Ping the default Gateway	-
DNS	Ping the primary Domain Name Server	-
DNS Query	Test DNS Query	-
Internet	Ping a well known internet host	-

Viewing Status Screens

The SpeedStream router's Web management interface provides several screens from which you can monitor various system status and statistics:

- The **System Summary** screen displays router and PPP connection(s) information.
- The **Interface Map** displays a graphical depiction of system connections.
- The **Firewall Log** screen displays activity occurring with data passing to or from the firewall.
- The **Status and Statistics** screens allow you to view the current status for the system, ATM/AAL, DSL and Ethernet connections.
- The **System Log** screen displays system activity.

Additionally, several screens that allow you to change configuration settings also display the current settings (please refer to the previous section for detailed instructions on configuring specific settings):

- The **Firewall – DMZ Configuration** screen displays the current DMZ status and host IP address.
- The **Firewall – Snooze Control** screen displays the current snooze interval.
- The **Port Forwarding Configuration** screen displays the current port forwarding configurations.
- The **Static Routes** screen displays currently configured static routes.
- The **Time Client Configuration** screen displays the current primary and secondary server IP addresses.
- The **UPnP Configuration** screen displays the current UPnP mode.

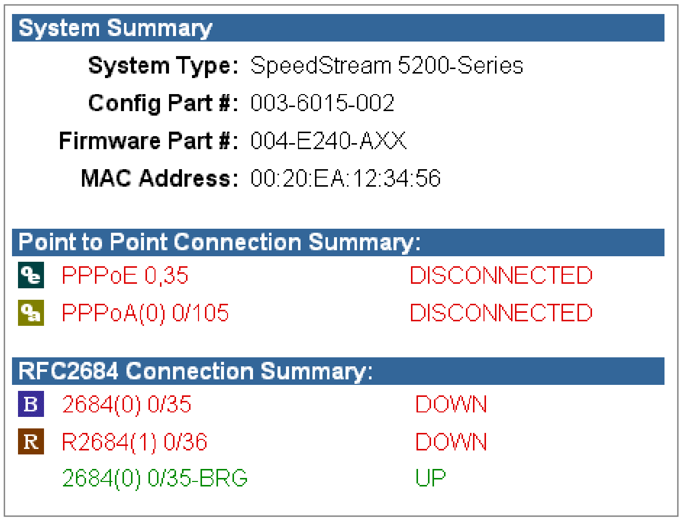
System Summary

The **System Summary** screen 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.

To display the *System Summary* screen:

- From the main menu, click **Status and Statistics**, and then click **System Summary**.

  The **System Summary** screen displays.



System Summary

System Type: SpeedStream 5200-Series
Config Part #: 003-6015-002
Firmware Part #: 004-E240-AXX
MAC Address: 00:20:EA:12:34:56

Point to Point Connection Summary:

PPPoE 0,35 DISCONNECTED
PPPoA(0) 0/105 DISCONNECTED

RFC2684 Connection Summary:

B 2684(0) 0/35 DOWN
R R2684(1) 0/36 DOWN
2684(0) 0/35-BRG UP

Interface Map

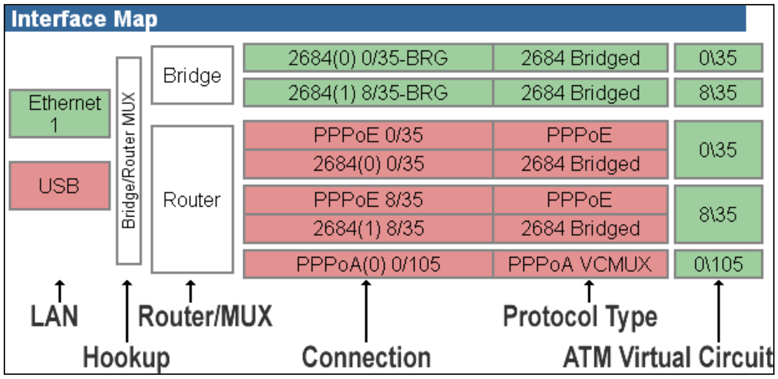
Note This option may not be available on your router configuration.

The **Interface Map** screen provides a graphical representation of the current LAN and WAN configurations of your SpeedStream router. It 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.

To display the Interface Map:

- On the main menu, click **Tools**, and then click **Interface Map**.

  The **Interface Map** screen displays.



Firewall Log

When the Attack Detection System (ADS) is enabled, various checks are performed, according to the criteria you designate. For example:

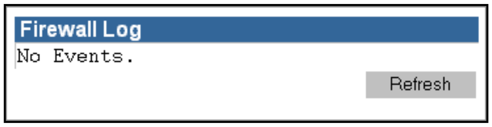
- If an attack is detected, that information can be displayed in the **Firewall Log**.
- Any denials of access by the firewall can be logged with a reason code and a description string.
- Syslog-formatted messages can be sent to another node on the LAN.

The Firewall Log contains a maximum of 200 entries; each entry may contain a maximum of 200 characters.

To display the *Firewall Log* screen:

- From the main menu, click **Advanced Setup**, then click **Firewall**, and then click **Log**.

  The **Firewall Log** screen displays.


Firewall Log

```
No Events.
```

System Log

The **System Log** screen 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.

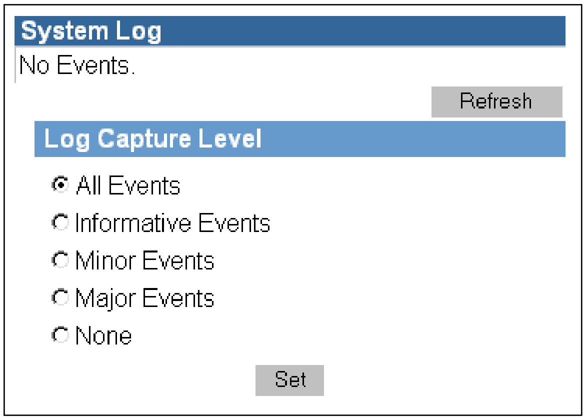
To display the *System Log* screen:

- From the main menu, click **Status and Statistics**, and then click **System Log**.

  The **System Log** screen displays.

To update the display :

- Click **Refresh**.



System Log

No Events.

Log Capture Level

● All Events
○ Informative Events
○ Minor Events
○ Major Events
○ None

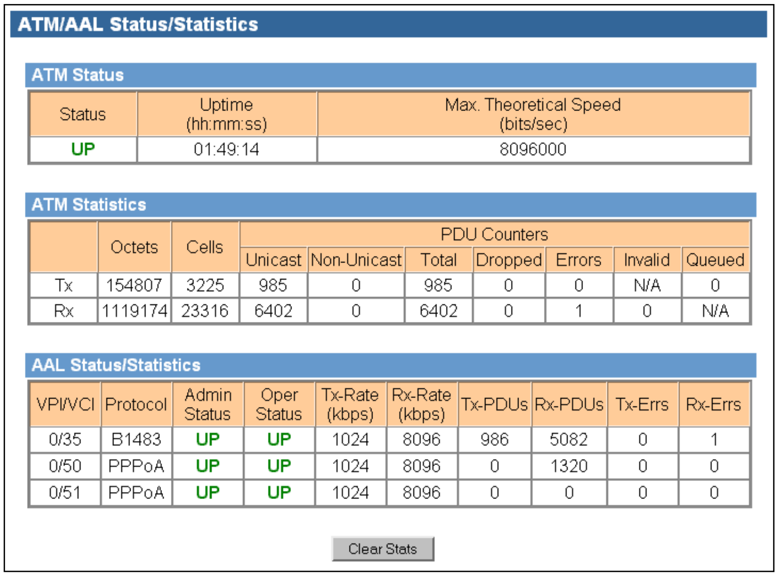
Status and Statistics Screens

These screens display data pertaining to ATM/AAL, DSL, Ethernet and USB traffic, including whether the connection is Up (green) or Down (red).

ATM/AAL Status/Statistics

- From the main menu, click **Status and Statistics**, and then click **ATM/AAL**.

  The **ATM/AAL Status/Statistics** screen displays.



ATM/AAL Status/Statistics

ATM Status

Status	Uptime (hh:mm:ss)	Max. Theoretical Speed (bits/sec)
UP	01:49:14	8096000

ATM Statistics

	Octets	Cells	PDU Counters						
			Unicast	Non-Unicast	Total	Dropped	Errors	Invalid	Queued
Tx	154807	3225	985	0	985	0	0	N/A	0
Rx	1119174	23316	6402	0	6402	0	1	0	N/A

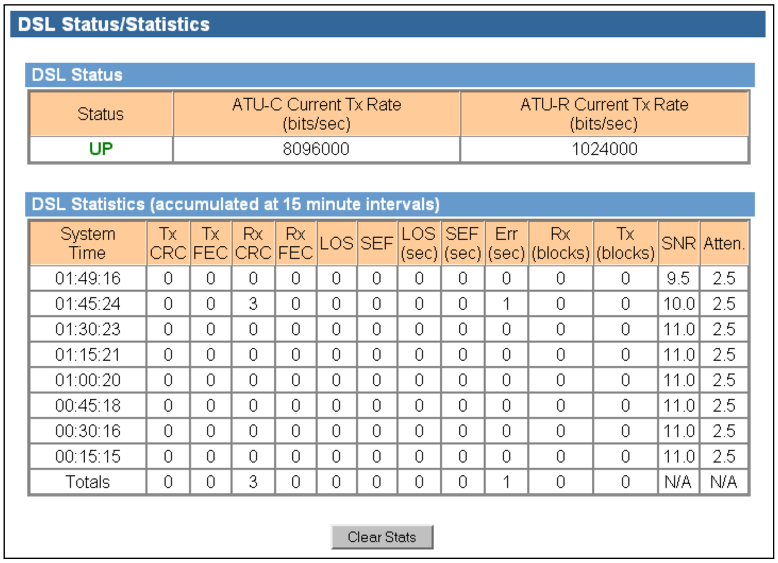
AAL Status/Statistics

VPI/VCI	Protocol	Admin Status	Oper Status	Tx-Rate (kbps)	Rx-Rate (kbps)	Tx-PDUs	Rx-PDUs	Tx-Errs	Rx-Errs
0/35	B1483	UP	UP	1024	8096	986	5082	0	1
0/50	PPPoA	UP	UP	1024	8096	0	1320	0	0
0/51	PPPoA	UP	UP	1024	8096	0	0	0	0

DSL Status/Statistics

- From the main menu, click **Status and Statistics**, and then click **DSL**.

  The **DSL Status/Statistics** screen displays.



DSL Status/Statistics

DSL Status

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

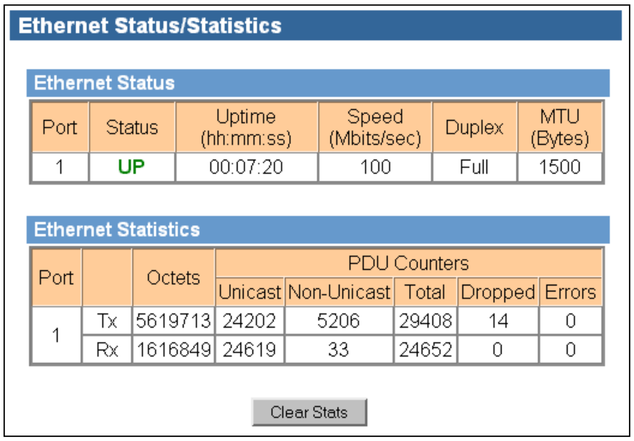
DSL Statistics (accumulated at 15 minute intervals)

System Time	Tx CRC	Tx FEC	Rx CRC	Rx FEC	LOS	SEF	LOS (sec)	SEF (sec)	Err (sec)	Rx (blocks)	Tx (blocks)	SNR	Atten.
01:49:16	0	0	0	0	0	0	0	0	0	0	0	9.5	2.5
01:45:24	0	0	3	0	0	0	0	0	1	0	0	10.0	2.5
01:30:23	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
01:15:21	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
01:00:20	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
00:45:18	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
00:30:16	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
00:15:15	0	0	0	0	0	0	0	0	0	0	0	11.0	2.5
Totals	0	0	3	0	0	0	0	0	1	0	0	N/A	N/A

Ethernet Status/Statistics

- From the main menu, click **Status and Statistics**, and then click **Ethernet**.

  The **Ethernet Status/Statistics** screen displays.



Ethernet Status/Statistics

Ethernet Status

Port	Status	Uptime (hh:mm:ss)	Speed (Mbits/sec)	Duplex	MTU (Bytes)
1	UP	00:07:20	100	Full	1500

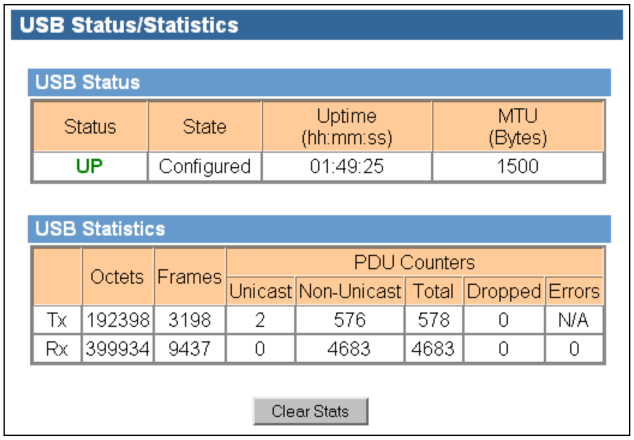
Ethernet Statistics

Port		Octets	PDU Counters				
			Unicast	Non-Unicast	Total	Dropped	Errors
1	Tx	5619713	24202	5206	29408	14	0
	Rx	1616849	24619	33	24652	0	0

USB Status/Statistics

- From the main menu, click **Status and Statistics**, and then click **USB**.

  The **USB Status/Statistics** screen displays.



USB Status/Statistics

USB Status

Status	State	Uptime (hh:mm:ss)	MTU (Bytes)
UP	Configured	01:49:25	1500

USB Statistics

	Octets	Frames	PDU Counters				
			Unicast	Non-Unicast	Total	Dropped	Errors
Tx	192398	3198	2	576	578	0	N/A
Rx	399934	9437	0	4683	4683	0	0

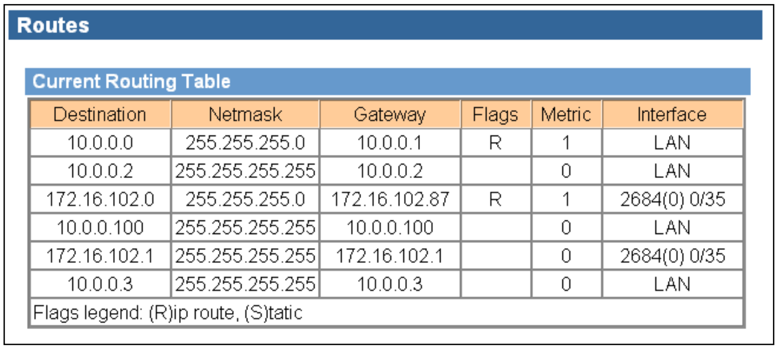
Routes

The Routes screen displays the current routing table which contains the data pertaining to all currently known static and dynamic IP routes.

Note Please refer to the Online Help for description of the fields in the Current Routing Table.

- From the main menu, click **Status and Statistics**, and then click **Routes**.

  The **USB Status/Statistics** screen displays.



Routes

Current Routing Table

Destination	Netmask	Gateway	Flags	Metric	Interface
10.0.0.0	255.255.255.0	10.0.0.1	R	1	LAN
10.0.0.2	255.255.255.255	10.0.0.2		0	LAN
172.16.102.0	255.255.255.0	172.16.102.87	R	1	2684(0) 0/35
10.0.0.100	255.255.255.255	10.0.0.100		0	LAN
172.16.102.1	255.255.255.255	172.16.102.1		0	2684(0) 0/35
10.0.0.3	255.255.255.255	10.0.0.3		0	LAN
Flags legend: (R)ip route, (S)tatic					

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*
Off	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)
Green	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
Blinking Green	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
Blinking Red/Green	Flash Write in progress	N/A	N/A	N/A
Red	- POST tests in progress (first 30 sec. after powering on or rebooting) - POST error occurred	N/A	N/A	N/A

***Note** The 5100 and 5400 series SpeedStream routers have one Ethernet LED; the 5200 and 5500 series have four Ethernet LEDs, one for each Ethernet port.

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:	+1 (972) 852-1000
Fax:	+1 (972) 852-1001
Email:	support@efficient.com
Internet:	http://www.support.efficient.com

Appendix A:
Configuration Data Sheets

Your router is preconfigured with settings specific to your network. We strongly suggest that you record these settings in case you need to reestablish your original configuration.

Administrative User Setup

Parameter	Default Value	Your Value
User Name	admin	
Password		

Attack Detection System

Parameter	Default Value		Your Value	
Enable ADS				
Same Source/Destination Address	Filter:	Log:	Filter:	Log:
Broadcast Source Address	Filter:	Log:	Filter:	Log:
LAN Source Address On WAN	Filter:	Log:	Filter:	Log:
Invalid IP Packet Fragment	Filter:	Log:	Filter:	Log:
TCP NULL	Filter:	Log:	Filter:	Log:
TCP FIN	Filter:	Log:	Filter:	Log:
TCP Xmas	Filter:	Log:	Filter:	Log:
Fragmented TCP Packet	Filter:	Log:	Filter:	Log:
Fragmented TCP Header	Filter:	Log:	Filter:	Log:
Fragmented UDP Header	Filter:	Log:	Filter:	Log:
Fragmented ICMP Header	Filter:	Log:	Filter:	Log:

DHCP

Parameter	Default Value	Your Value
DHCP Server		
Start IP Range		
End IP Range		
IP Netmask		
Default Gateway		
Or Self		
DNS Server		
Or Use Wan		
Domain Name		
Lease Time (Mins)		
Or Infinite Time		

Firewall – Custom IP Filter Configuration

Parameter	Default Value	Your Value
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		

Parameter	Default Value	Your Value
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		
Rule #		
Status		
Access		
Direction		
Protocol		
Source Interface		
Source Address		
Source Mask		
Destination Port Operator		
Enable/Disable		

Firewall - DMZ

Parameter	Default Value	Your Value
Status		
Enable With Host IP Address		
Enable With Host Name		
Settings Duration		

Firewall – Level

Parameter	Default Value	Your Value
Level		

Firewall – Snooze Control

Parameter	Default Value	Your Value
Snooze Control		
Disable		
Enable, Set Time Interval To:		
Reset Time Interval To		

Host

Parameter	Default Value	Your Value
IP Address		
IP Netmask		
Default Router		
Host Name		

LAN IP

Parameter	Default Value	Your Value
IP Address Subnet Mask		

NAT/NAPT

Parameter	Default Value	Your Value
Interface 1		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 2		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 3		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		

Parameter	Default Value	Your Value
NAPT Enabled		
Interface 4		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 5		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 6		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 7		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		
Interface 8		
NAT/NAPT Disabled		
NAT Enabled		
Internal (LAN) IP Address		
NAPT Enabled		

Port Forwarding

Parameter	Default Value	Your Value

PPP Login

Parameter	Default Value	Your Value
Connection 1		
User Name		
Password		
Access Connection		

Parameter	Default Value	Your Value
Service Name		
Auto-Connect On Disconnect		
Use Idle Time-Out		
Connection 2		
User Name		
Password		
Access Connection		
Service Name		
Auto-Connect On Disconnect		
Use Idle Time-Out		
Connection 3		
User Name		
Password		
Access Connection		
Service Name		
Auto-Connect On Disconnect		
Use Idle Time-Out		
Connection 4		
User Name		
Password		
Access Connection		
Service Name		
Auto-Connect On Disconnect		
Use Idle Time-Out		

RIP

Parameter	Default Value	Your Value

Static Route

Parameter	Default Value	Your Value
Destination		
Netmask		
Next Hop		
Interface		

System Log

Parameter	Default Value	Your Value
Log Capture Level		

Time Client

Parameter	Default Value	Your Value
Disabled		
Primary Server IP Address		
Secondary Server IP Address		

UPnP

Parameter	Default Value	Your Value
Disabled		
Discovery and Advertisement Only		
Full IGD-Supported		
Enable Access Logging		
Read-Only Mode		

Appendix B:
Technical Specifications

AAL and ATM Support:	VCI 0-65535 address range VPI 0-255 address range AAL5 support
Bridging:	IEEE 802.1.d Transparent Learning Bridge (dynamic learning of up to 255 addresses) Spanning Tree support
Certifications:	FCC Part 15, Class B CE certification
Connectors:	DSL interface: RJ-11 or RJ-45 (Europe) Ethernet interface: RJ-45 USB Type B interface (5200, 5500 series)
Diagnostic LEDs:	Power, DSL, Activity, Ethernet status; USB status (5200, 5500 series)
Management:	Intuitive, Web-based GUI management access SNMP support Comprehensive hardware diagnostics
Media Interface:	RJ-11 or RJ-45 (European) DSL WAN connection 10/100Base-T RJ-45 Ethernet LAN connection USB Type B LAN connection (5200, 5500 series)
Power:	12V power supply included, 700ma max. 5400/5500 - 12 VDC, 1000ma max.
Routing:	DHCP server/DHCP client Network Address Port Translation (NAPT) Network Address Translation (NAT) Packet filtering RFC 2364 Point-to-Point Protocol over ATM PVCs (PPPoA) RFC 2516 Point-to-Point Protocol over Ethernet (PPPoE) RFC 2684 (formerly 1483) Bridged Ethernet and routed encapsulation Routing
Standards Compliance:	IEEE 802.3 USB 1.1 T1.413 issue 2 G.992.1 (G.DMT) G.992.2 (G.Lite)

Appendix C:
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						√		√		
Asherons 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						√		√		
H.323						√		√		
Half Life				√		√		√		
Heretic II				√		√		√		
Hexen II				√		√		√		
HTTP		√		√		√		√		√
HTTPS		√		√		√		√		√
ICMP		√		√		√		√		
ICQ 2000						√		√		

Application/ Protocol	Security									
	High		Medium		Low		NAPT Off		ICSA-Compliant	
	In	Out	In	Out	In	Out	In	Out	In	Out
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				√		√		√		
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				√		√		√		√

Application/ Protocol	Security									
	High		Medium		Low		NAPT Off		ICSA-Compliant	
	In	Out	In	Out	In	Out	In	Out	In	Out
Tiberian Sun				√		√		√		
Traceroute		√		√		√		√		
Ultima Online				√		√		√		
Unreal Tournament				√		√		√		
VNC						√		√		
Warcraft				√		√		√		
Windows Media Player		√		√		√		√		
XDM						√		√		
Yahoo Messenger						√		√		

Appendix D:
Acronyms and Technical Concepts

Acronyms

AAL5	ATM Adaption Layer 5
ADS	Attack Detection System
ATM	Asynchronous Transfer Mode
ATU	ADSL Termination Unit
ATU-C	ADSL Termination Unit - Central Office; refers to location at the CO aggregation point.
ATU-R	ADSL Termination Unit - Remote; refers to location at the customer premises
CHAP	Challenge-Handshake Authentication Protocol
CRC	Cycle Redundancy Checking
CO	Central Office
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
Ethernet	Network standard for LAN communications
FEC	Forward Equivalence Class
firmware	Software, in binary form, stored within a flash PROM
frames	Data packet
Gateway	Router
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
IGD	Internet Gateway Device
IPCP	IP Control Protocol
ISP	Internet Service Provider
LCP	Link Control Protocol
LLC	Logical Link Control layer

LOS	Loss of Signal
MAC address	Media Access Control address; a network device's unique identifier
MTU	Maximum Transmission Unit
NAP	Network Access Provider
NAPT	Network Address Port Translation
NAT	Network Address Translation
NCP	Network-layer Control Protocol
NSP	Network Service Provider
OCD	Out-of-cell Delineation (ATM error condition)
octet	8 bytes
PAP	Password Authentication Protocol
POST	Power-On Self Test
PDU	Protocol Data Unit
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTT	Post Telephone and Telegraph (European Telco)
PVC	Permanent Virtual Circuit
RFC	Request for Comment
RIP	Routing Information Protocol
RT	Remote Termination
Rx Cells	(ATM) Number of cells received and passed through to the ATM layer.
Rx Errors	(ATM) Number of SDUs received.
Rx Invalid	(ATM) Number of cells that are dropped because they are not associated with an existing connection.
Rx Packets	(DSL, Eth, USB) Count of all encoded blocks received on this channel since router reset.
RX PDUs	(ATM) Number of Protocol Data Units (PDUs) that are received and passed to upper layers.
SDU	Service Data Unit
SEF	Severely Errored Frame
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio

SSDP	Simple Service Discovery Protocols
Tx Cells	(ATM) Number of cells transmitted through the ATM layer to the wire.
Tx Errors	(ATM) Number of SDUs that could not be transmitted due to errors.
Tx Packets	(DSL, Ethernet, USB) Count of all encoded blocks transmitted on this channel since router reset.
Tx PDUs	(ATM) Number of PDUs transmitted on connection.
Unicast	Communication between a single sender and a single receiver across a network
VC	Virtual Channels
VCI	Virtual Channel Identifiers
VCMux	Virtual Channel Multiplexor
VPI	Virtual Path Identifiers

Technical Concepts

This section provides very brief descriptions of some of the features available on the SpeedStream Router.

AAL5 (ATM Adaption Layer 5)

AAL5 is a network layer for adapting data traffic into the format of ATM fixed-length packet networks.

ATM (Asynchronous Transfer Mode)

ATM is a fast, cell-based technology defined by the ITU-T. It works by taking an ordinary, variable-length data packet and segmenting it into 53-byte cells prior to transmission. The data is transmitted over *virtual channels* that are designated by specific unique identifiers (virtual channel identifiers or VCIs). There can be multiple VCIs in one *virtual path*. The virtual path also has a unique virtual path identifier (VPI). Data transmitted over ATM VCs is routed by ATM switches. At the destination node, the cells are reassembled into packets. Only one virtual path is supported on the device. In router mode, only one virtual channel is supported. However, in bridge mode, up to 16 virtual channels can be configured to be used as individual bridge ports.

Cloning IP Filter Rules

Defining a complete set of firewall IP filter rules can be a tedious process. To aide our SpeedStream router users, Efficient Networks includes the capability to “clone” an existing set of rules as a starting point in the process.

There are four preconfigured firewall levels: Low, Medium, High and ICSA-compliant. Each of these levels has its own set of predefined firewall rules. If you Want to create a set of Custom rules that are similar to one of the preconfigured levels, you can do this through cloning. When you clone one of the preconfigured levels, the new set of custom rules is an exact replica of the cloned level; only the rule numbers have been changed.

When you clone a set of rules, any existing Custom rules are deleted and a new set of Custom rules (a replica of the cloned level) is created. When you click **Clone Rule Set** on the **Firewall – Custom IP Filter Configuration** screen, the Current IP Filter Rules table refreshes with the new rules set. You can edit, add or delete this new set of rules.

Rule Numbering

If you select a specific Firewall Level (e.g., Low) and then examine the list of rules displayed in the Current IP Filter Rules table, you will notice that the numbers start at xx20; e.g., Low starts at 120, not 100. The numbers preceding xx20 (1-19) are skipped to allow you extra space at the front of the list to add new rules. Additionally, the preconfigured rules are not consecutively numbered - Low, for example, is numbered as 120, 122, 124 – allowing you to easily interject new rules between the existing ones.

Important! The rule numbers represent the priority with which the rules will be applied in filtering IP packets. Consequently, rule number 120 would be applied before rule number 122. If, for example, rule 120 denies all inbound traffic, it would render all other inbound rules useless – no inbound traffic allowed!

This numbering/priority scheme applies independently to the two categories of rules, *inbound* and *outbound.* Inbound rules are applied only to inbound packets; outbound rules are applied only to outbound packets.

The display of rules in the table is ordered by the Direction category. Inbound rules are displayed first; outbound rules display second.

DHCP (Dynamic Host Configuration Protocol)

The router provides two user-configurable Dynamic Host Configuration Protocol (DHCP) modes: DHCP server (enabled by default from the factory) and DHCP relay agent.

DHCP Relay

The router can be configured to operate as a DHCP relay agent. This allows local machines on the LAN to acquire their IP addresses via DHCP requests and replies that are forwarded through the router to/from a DHCP server on the WAN. In this case, the DHCP requests are forwarded to a specific DHCP server on the WAN network and the DHCP reply is forwarded back to the LAN network.

The DHCP relay agent can be configured with a Primary and a Secondary DHCP Server IP address. The Secondary address is only used if the Primary is unreachable. Any DHCP requests that are received by the router are relayed to the Primary DHCP server at the specified IP address.

This DHCP server is then responsible for assigning the DHCP information to the DHCP client. Typically, this DHCP server will exist in the WAN space.

DHCP Server

When operating as a DHCP server, the router will dynamically assign IP addresses to LAN nodes. The DHCP server verifies a device’s identity, leases it an IP address for a predetermined period of time, and reclaims the address for reassignment at the end of the lease period. The DHCP server supports DHCP client hosts on the LAN side only. The router will ignore all DHCP requests which arrive from the WAN interface.

Note You have the option to change the router's Ethernet IP address without rebooting the router. If you have configured a specific set of IP addresses for the DHCP server, then you change the Ethernet IP address to something that is on a different subnet than your DHCP server's addresses, and you do not reboot, the router will not recognize the change. The DHCP server will not be able to hand out addresses. Be sure to reboot the router when you change the Ethernet IP address in this manner.

DNS (Domain Name Service)

The router supports Domain Name Service (DNS) which provides hostname-to-IP address resolution for LAN-side clients. There are two distinct DNS functions provided by the router: the *DNS resolver and the DNS server.*

DNS Resolver

The DNS resolver is the entity that creates a DNS request for transmission to a DNS server (which may be co-located in the router or be an external DNS server). The DNS resolver is only used by certain user interface commands that allow a hostname argument as well as an IP address argument.

The DNS resolver requires the user to configure a single DNS server IP address to which to direct DNS requests. This IP address may be the router itself in the situation where the DNS server is enabled on the router or it may be any reachable IP address at which a DNS server is available.

DNS Server

The DNS server is the entity that responds to DNS requests. The DNS server provides IP address-to-hostname resolution and hostname-to-IP address resolution for LAN clients via DNS requests. The DNS server also supports hostname-to-IP address resolution for user interface commands where appropriate in response to requests submitted by the DNS resolver.

The DNS server is enabled by default from the factory and provides the router with the default hostname "**ENI-Router".**

DSL (Digital Subscriber Line)

DSL describes a family of digital services provided by local telephone companies to local subscribers. There are many forms of DSL: Asymmetric DSL (DSL), Symmetric (or single pair) DSL (SDSL), and many others. The router supports DSL, which provides rates of up to 6 Mbps downstream from the customer and up to 640 Kbps upstream from the customer. DSL can carry voice and data signals at the same time in both directions.

Encapsulation Methods: PPP and RFC 1483

The 5600 series router transmits data via ATM Virtual Channels (VCs). The data is encapsulated using methods Point-to-Point Protocol (PPP) or RFC 1483 encapsulation. A brief explanation of these two encapsulation methods follows.

ICSA 3.0a-compliancy

ICSA Labs, a division of TruSecure Corporation, tests and defines firewall security criteria, providing certification to products that meet their exacting standards. For more information, go to http://www.icsalabs.com/html/communities/firewalls/index.shtml.

PPP (Point-to-Point Protocol)

PPP is a single or multi-link interface between two packet switching devices, such as a bridge or router. PPP has built-in negotiation for addresses and connection parameters and can route multiple protocols over a single link. One benefit of using PPP is it offers interoperability of multi-vendor equipment as well as support for dynamic configuration between the connecting devices.

Public and Private Networks and the Use of NAPT

An IP address must be unique among all networks reachable from a given host using the IP protocols. The *Internet Registry* in the United States that ensures the uniqueness of the IP addresses on the Internet. The Internet Registry assigns an entire IP network number to each site connected to the Internet. Each IP address at a site is unique as long as the site assigns a different host number to each host on its network. Thus each host is ensured a globally unique IP address that is known as a *public* IP address.

However, there has been concern over the eventual exhaustion of the public address space. This has LED the Registry to set aside IP network numbers for *private* addressing. These numbers are not assigned to anyone by the Internet Registry and are open for use by any site. IP addresses are unique within the private address space, but two private address spaces are not guaranteed unique.

Use of private address spaces has some disadvantages including the need to re-address any host that must change from a private address to a public address. Plus the privately addressed hosts are unable to communicate with all hosts in an internet. These problems can be handled by the use of *Network Address Port Translation* (NAPT).

NAPT is an extension to *Network Address Translation* (NAT). With NAT, a network address translator (the router, in this case) sits between an organization’s network and the Internet, or between two organization’s networks and translates IP addresses from private internal addresses to globally unique external addresses. NAPT, however, allows many network addresses and their TCP/UDP ports to be translated to a single network address and its TCP/UDP ports. With NAPT, a few of your internal hosts can share a single public address. When a host needs to access the Internet, the router will translate an address for it. When packets from the host are sent to the Internet, the router replaces the internal address with the external address. When packets come back for that address, the router reverses the substitution.

RFC 2684

Request for Comment (RFC) 2684, which supplants RFC 1483, is an interoperability specification set by the Internet Engineering Task Force (IETF) that outlines methods for multiprotocol encapsulation over ATM. RFC 2684 describes two encapsulation methods for carrying network interconnect traffic over ATM Adaptation Layer 5 (AAL5): Logical Link Control (LLC)/SNAP encapsulation and VC multiplexing.

By default, the router uses the first method, LLC Encapsulation, which allows multiplexing of multiple protocols over a single ATM virtual circuit. The second method, VC multiplexing, uses a separate VC for each carried protocol.

The router supports two types of encapsulation: *routed* and *bridged*. RFC 2684 Routed encapsulation operates at the IP layer and will route only IP packets. If the router will be handling non-IP packets, you may WAN to use RFC 2684 bridged encapsulation.

Index