SpeedStream

Router User's Guide

Model 4200

OPTUSnet BROADBAND

Part No. 007-4049-001

Table of Contents

Chapter 1 Introduction

Chapter 2 Installation

Chapter 3 Configuring User Profiles

Chapter 4 Configuring ISP Connection Settings

Chapter 5 Configuring Network Settings

Chapter 6 Configuring Security Features

Chapter 7 Monitoring Router Health

Chapter 8 Troubleshooting

Chapter 1 Introduction

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

SpeedStream 4200 (Ethernet and USB)

The SpeedStream 4200 can communicate through either an Ethernet or a USB connection.

Features of the SpeedStream® Router

The 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 Router can also be used to connect the corporate LAN to the Internet over the WAN.

Network (LAN) Features

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

Security Features

- **Password-protected Configuration**
  Password protection prevents unauthorized users from modifying the Router's configuration settings.
- **Firewall Security**
  Firewall security with four conveniently pre-set standard levels of security (Off, Low, Medium, High), an ICSA-compliant mode, and a custom setting for advanced users.
- **NAT Protection**
  Network Address Port Translation (NAPT) and a secure firewall to protect your data while your computer is connected to the Internet.
- **Attack Protection System**
  Attacks can flood your Internet connection with invalid data packets and connection requests, using so much bandwidth and so many resources that Internet access becomes unavailable. The Router incorporates protection against these types of attacks as well as other common hacker attacks.
- **Stateful Inspection Firewall**
  All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.
- **Virtual Private Network**
  Virtual Private Network allows remote users to establish a secure connection to a corporate network by setting pass-through of the three most commonly used VPN protocols: PPTP, L2TP, and IPSec.

Configuration & Management

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

Advanced Router Functions

- **DMZ**
  One computer on your local network can be configured to allow unrestricted two-way communication with servers or individual users on the Internet. This provides the ability to run programs that are incompatible with firewalls.
- **Port Forwarding**
  Port Forwarding provides flexibility by allowing you to change internal IP addresses without affecting outside access to your network.
- **Session Tracking**
  Some protocols, such as FTP, require secondary network connections on ports other than the main control port. These connections are usually made using port numbers in the dynamic range (> 1024). The firewall allows traffic on secondary sessions without manual configuration.

Minimum System Requirements

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

- DSL service and an Internet access account from an Internet Service Provider (ISP).
- Network cables for the device you intend to connect to the Router. Use standard CAT5 Ethernet cables with RJ45 connectors.
- TCP/IP network protocol must be installed on all computers.
- Ethernet connection method:
  - A network interface card (NIC) that supports Ethernet 10/100Base-T full-/half-duplex.
  - Operating system that supports TCP/IP.
  - Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later.
- USB connection method (if your router supports this method):
  - 32 MB RAM
  - Pentium-compatible 166 MHz processor (or faster).
  - 12 MB available hard disk space.
  - One of the following operating systems:
    - Windows 98, 98SE
    - Windows 2000
    - Windows ME or XP
    - Mac OS versions 8.6 through 10.2.4

General Safety Guidelines

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

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

Chapter 2 Installation

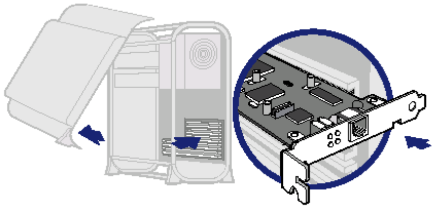
This chapter describes the steps you must take to install and configure the various components in your network to utilize the Siemens Broadband Internet Router. This includes setting up the hardware connections to the Internet router, configuring the PC to use the Internet router for Internet access, and setting up the router configuration.

Hardware Installation

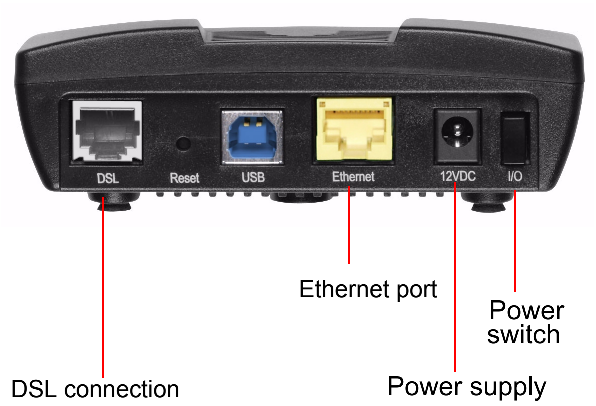
You may position the Siemens broadband router at any convenient location where it will be well ventilated. Do not stack it with other devices or place it on the carpet.

You can connect the router to an existing Ethernet port or USB port on your computer. Determine which connection method you want to use and follow the instructions below for the selected installation method: Ethernet or USB.

Ethernet Installation Method



To connect the SpeedStream device via the Ethernet interface, your computer must have an Ethernet adapter (also called a network interface card, or NIC) installed. If your computer does not have this adapter, install it before proceeding further. Refer to your Ethernet adapter documentation for complete installation instructions. Once you verify installation of an Ethernet adapter, perform the following procedure to connect the router to your computer.

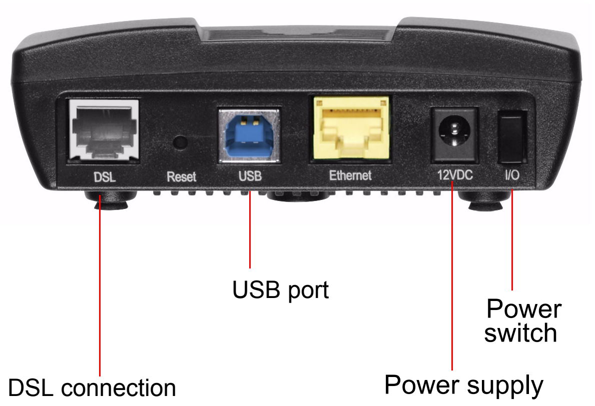


1. With the PC powered off, connect the Ethernet cable to the Ethernet port on the router.
2. Connect the other end of the Ethernet cable to the Ethernet port on the PC.
3. Connect the DSL cable (resembles a telephone cord) to the DSL port on the rear of the router. To reduce the risk of fire, use the supplied telephone cable or an ACA approved cable to connect your DSL port on your router to a DSL telephone jack.
4. Plug the other end of the DSL cable into the wall socket.
5. Connect the power adapter to the rear of the router.
6. Plug the power adapter into the electrical wall outlet.
7. Flip the power switch on the router.
8. Power on all connected computers.

You can now configure the TCP/IP settings as detailed in the PC Configuration section.

USB Installation Method

1. With your PC powered off, connect the USB cable to the USB port on the router.
2. Connect the other end of the USB cable to an open USB port on your PC.
3. Connect the DSL cable (resembles a telephone cord) to the DSL port on the router. To reduce the risk of fire, use the supplied telephone cable or an ACA approved cable to connect your DSL port on your router to a DSL telephone jack.
4. Plug the other end of the DSL cable into the wall socket.



5. Connect the power adapter to the rear of the router.
6. Plug the power adapter into the electrical wall outlet.
7. Power on all connected PCs.
8. Insert the USB driver CD-ROM into the CD-ROM drive of your PC.
9. When prompted, follow the on-screen instructions to complete the driver installation.
10. Flip the power switch to power on the router.

You can now configure the TCP/IP settings as detailed in the PC Configuration section.

PC Configuration

This section explains how to configure your personal computer to work with the Router.

To access the Internet through the SpeedStream Router, your PC must be configured to use the TCP/IP protocol suite over the Internet, and to accept Dynamic Host Configuration Protocol address assignments from the router.

The default network settings for the SpeedStream Router are:

IP Address:10.1.1.1

Subnet Mask:255.255.255.0

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

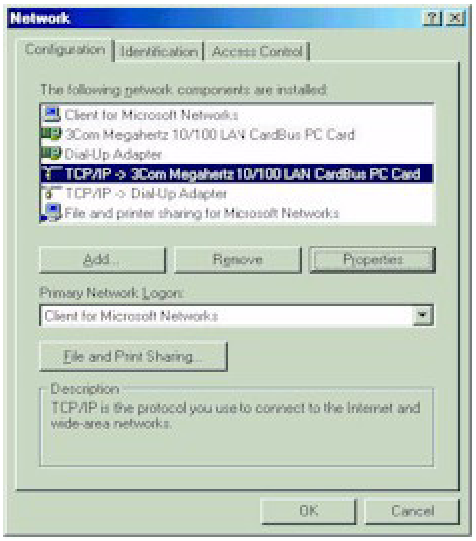
Although these are the default settings for the PC, it is a good idea to verify that they have not been changed. If TCP/IP is not already installed on your computer, refer to your system documentation or online help for instructions. Once installed, you should check the TCP/IP protocol settings to make sure they are correct for use with the Router.

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

- Checking TCP/IP Settings (Windows 9x/ME)
- Checking TCP/IP Settings (Windows 2000)
- Checking TCP/IP Settings (Windows XP)

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

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



Network

Configuration | Identification | Access Control

The following network components are installed:

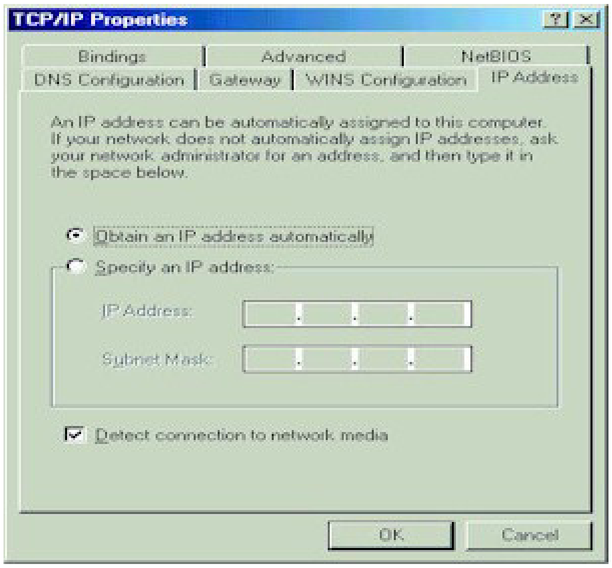
- Client for Microsoft Networks
- 3Com Megahertz 10/100 LAN CardBus PC Card
- Dial-Up Adapter
- TCP/IP -> 3Com Megahertz 10/100 LAN CardBus PC Card
- TCP/IP -> Dial-Up Adapter
- File and printer sharing for Microsoft Networks

Primary Network Logon:
Client for Microsoft Networks

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

2. Select the TCP/IP protocol for your network card.

3. Click **Properties**. This displays the TCP/IP Properties page.



TCP/IP Properties

Bindings | Advanced | NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

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:

IP Address: . . .

Subnet Mask: . . .

☑ Detect connection to network media

4. Click the **IP Address** tab.

5. Ensure that the **Obtain an IP address automatically** option is selected. This is the default Windows setting.

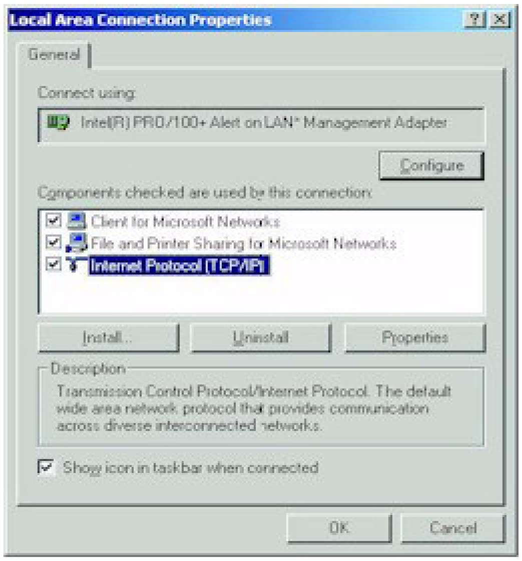
6. Close this page.

7. Restart your computer to ensure it obtains an IP address from the Router.

8. Configure internet access using the procedure described in Internet Access Configuration.

Checking TCP/IP Settings (Windows 2000)

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



Local Area Connection Properties

General

Connect using:

Intel(R) PRO/100+ Alert on LAN* Management Adapter

Components checked are used by this connection:

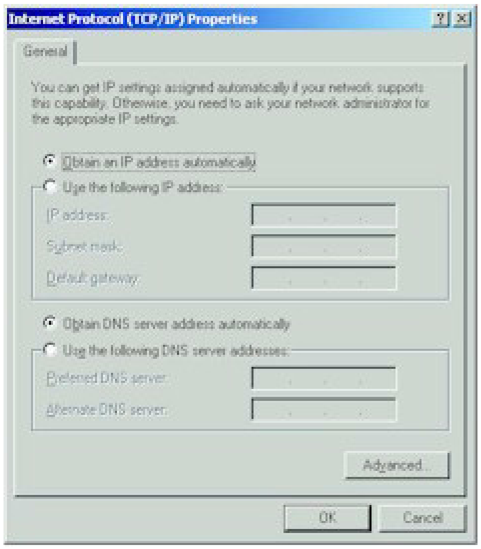
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

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

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



Internet Protocol (TCP/IP) Properties

General

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:

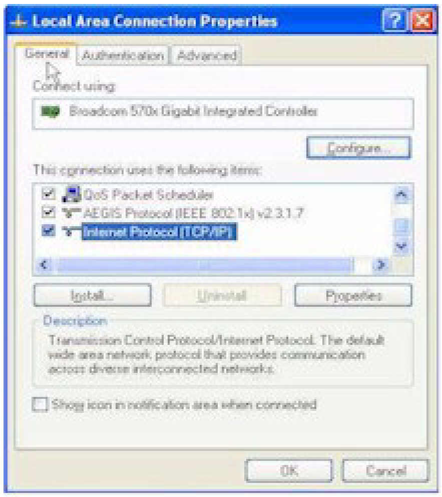
● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

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

Checking TCP/IP Settings (Windows XP)

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



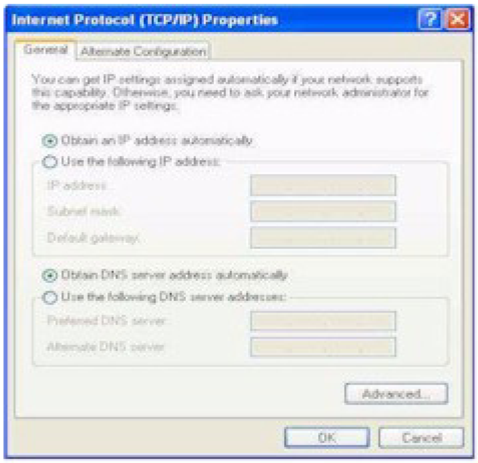
Connect using:
Broadcom 570x Gigabit Integrated Controller

This connection uses the following items:
☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v2.3.1.7
☑ 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 notification area when connected

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



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:

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

Internet Access Configuration

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

For Windows 9x/2000

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

For Windows XP

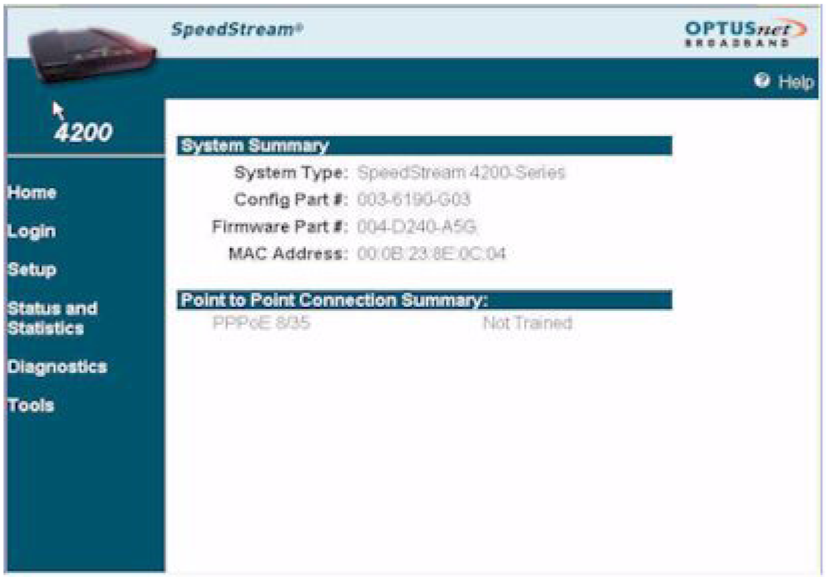
1. Select **Start**>**Control Panel**.
2. Double-click the **Internet Options** icon. This displays the Internet Options page.
3. Click the **Connections** tab.
4. Click **Setup**. This starts the **New Connection Wizard**.
5. Click **Next**.
6. Select **Connect to the Internet**, then click **Next**.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

Connecting to the Router

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

To establish a connection from your computer to the Router:

1. After installing the Router, start your computer. If your computer is already running, reboot it.
2. Open your Internet Explorer or Netscape Navigator Web browser.
3. In the **Address** bar, enter the default router IP address: **http://speedstream** and press **Enter**. This displays the Home page.



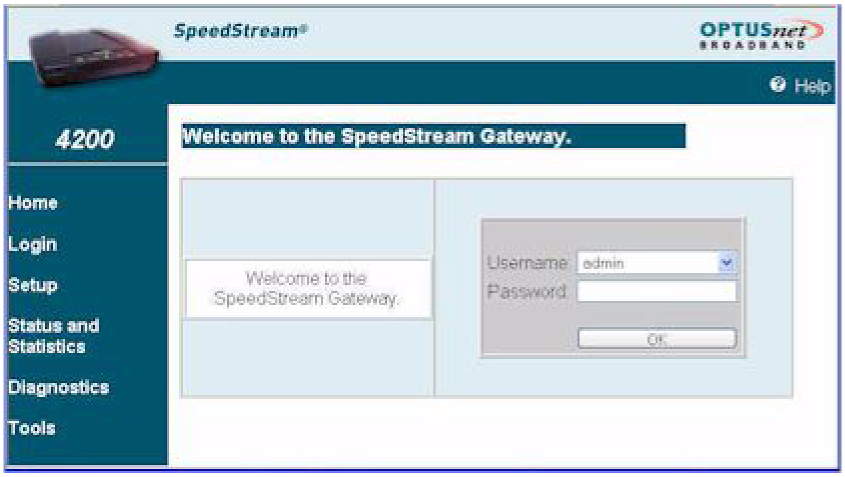
System Summary

System Type: SpeedStream 4200-Series
Config Part #: 003-6190-G03
Firmware Part #: 004-D240-A5G
MAC Address: 00:0B:23:8E:0C:04

Point to Point Connection Summary:

PPPoE 8/35 Not Trained

4. Click **Login** on the left navigation pane to log into the router. This displays the Login page.



Welcome to the SpeedStream Gateway.

Welcome to the SpeedStream Gateway.

Username: admin
Password:

5. By default the username is admin. There is no password set for the admin login. Click **OK**. This displays the Home page once again.
6. Click **OK**. This displays the screen for the menu option you selected.

7. Refer to the following chapters for information on how to use each of these options.
   - Refer to the Chapter titled "Installation", for details on adding, modifying, or deleting user profiles.
   - Refer to Chapter titled "Configuring ISP Connection Settings", for details on setting ISP configuration parameters. This should only be done when instructed by your ISP.
   - Refer to Chapter titled "Configuring Network Settings", for details on configuring network related information.
   - Refer to Chapter titled "Configuring Security Features", for details on adding security to your network.
   - Refer to Chapter titled "Monitoring Router Health", for details on viewing network statistics and connection status.

Chapter 3

Configuring User Profiles

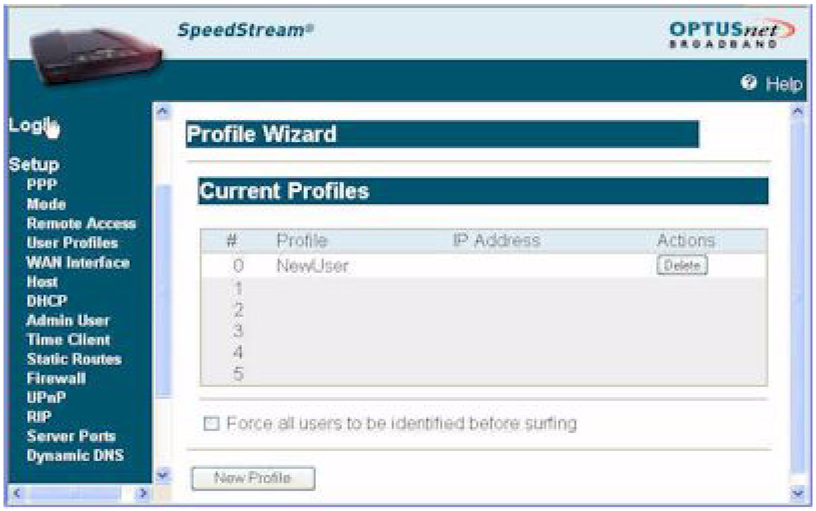
This chapter contains details for configuring users on the SpeedStream Router. User profiles are used as a means for controlling Router and network access by individual users. Access to the configuration and management of the Router should be restricted to authorized users only. This chapter describes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

- Add User Profiles
- Editing User Profiles
- Deleting User Profiles

Add User Profiles

To add a new user profile:

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



Profile Wizard

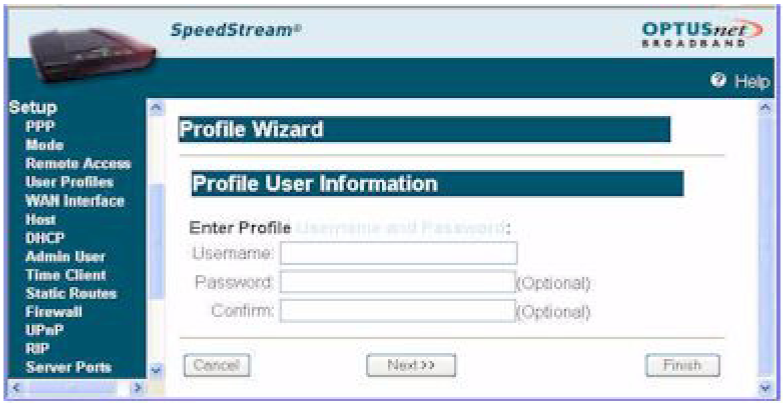
Current Profiles

#	Profile	IP Address	Actions
0	NewUser		Delete
1			
2			
3			
4			
5			

□ Force all users to be identified before surfing

New Profile

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



Profile Wizard

Profile User Information

Enter Profile Username and Password:

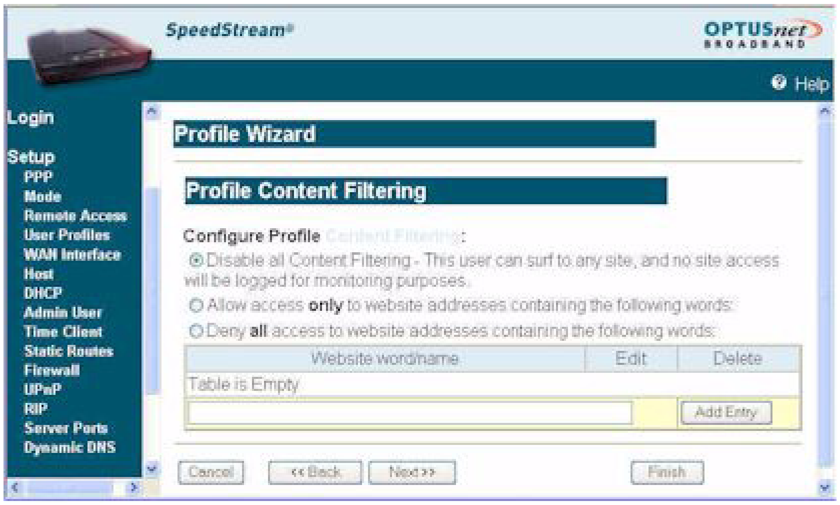
Username:

Password: (Optional)

Confirm: (Optional)

Cancel Next >> Finish

4. Enter a **Username** for the user you are adding.
5. Optionally enter a **Password** for the user and **Confirm** it.
6. Click **Next**. This displays the Profile Content Filtering page. Content filtering restricts access to undesirable Web sites and Web content.



Profile Wizard

Profile Content Filtering

Configure Profile Content Filtering:

● Disable all Content Filtering - This user can surf to any site, and no site access will be logged for monitoring purposes.

○ Allow access **only** to website addresses containing the following words:

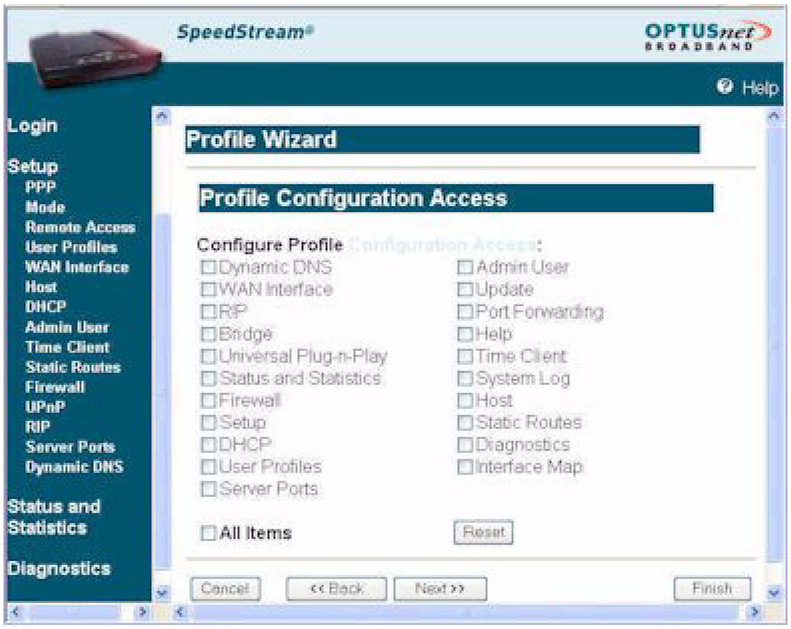
○ Deny **all** access to website addresses containing the following words:

Website word/name	Edit	Delete
Table is Empty		
		Add Entry

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

Note: The entries in the Website word/name table may be either modified or deleted at any time by clicking either **Edit** or **Delete** next to the corresponding word or Web address.

9. Click **Next**. This displays the Profile Configuration Access page. Profile configuration access defines the access permission for a user controlling what functions and features are available to that user.



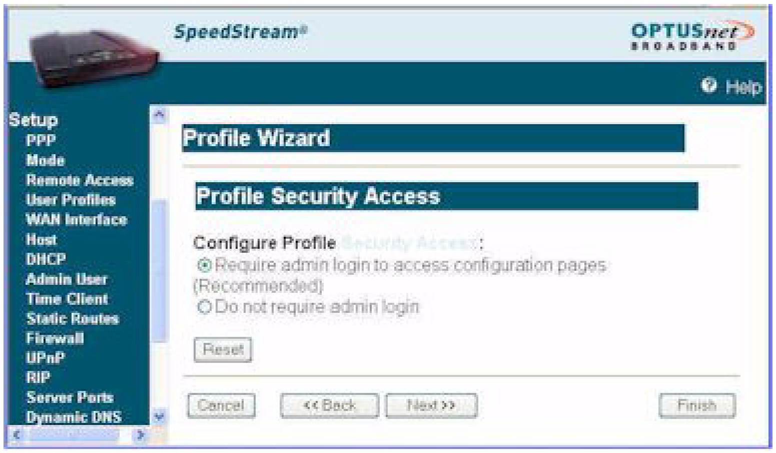
Profile Wizard

Profile Configuration Access

Configure Profile Configuration Access:

□ Dynamic DNS	□ Admin User
□ WAN Interface	□ Update
□ RIP	□ Port Forwarding
□ Bridge	□ Help
□ Universal Plug-n-Play	□ Time Client
□ Status and Statistics	□ System Log
□ Firewall	□ Host
□ Setup	□ Static Routes
□ DHCP	□ Diagnostics
□ User Profiles	□ Interface Map
□ Server Ports	
□ All Items	Reset

10. Optionally do one of the following:
    - Click one or more of the available features permitting the user to access that feature. This places a checkmark in the corresponding box. (Click again if you want to remove the checkmark and deny access).
    - Click **All Items** to select all features in the list.
    - Click **Reset** to clear all selected items and deny the user access to those feature.
11. Click **Next**. This displays the Profile Security Access page.



Profile Wizard

Profile Security Access

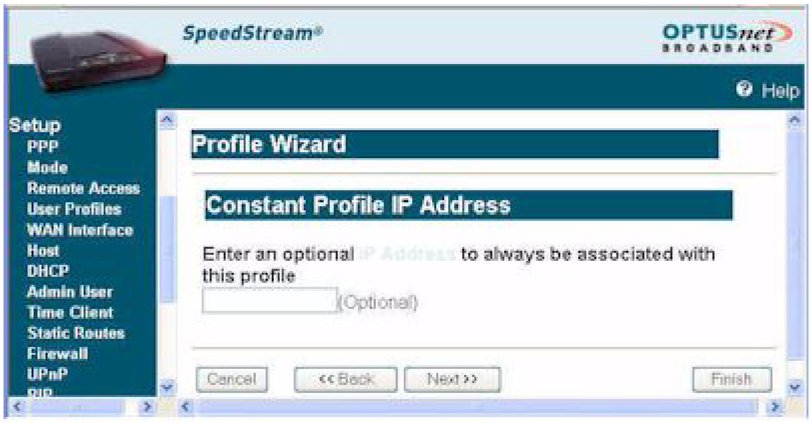
Configure Profile Security Access:

● Require admin login to access configuration pages (Recommended)

○ Do not require admin login

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

13. Click **Next**. This displays the Constant Profile IP Address page.



Profile Wizard

Constant Profile IP Address

Enter an optional IP Address to always be associated with this profile

(Optional)

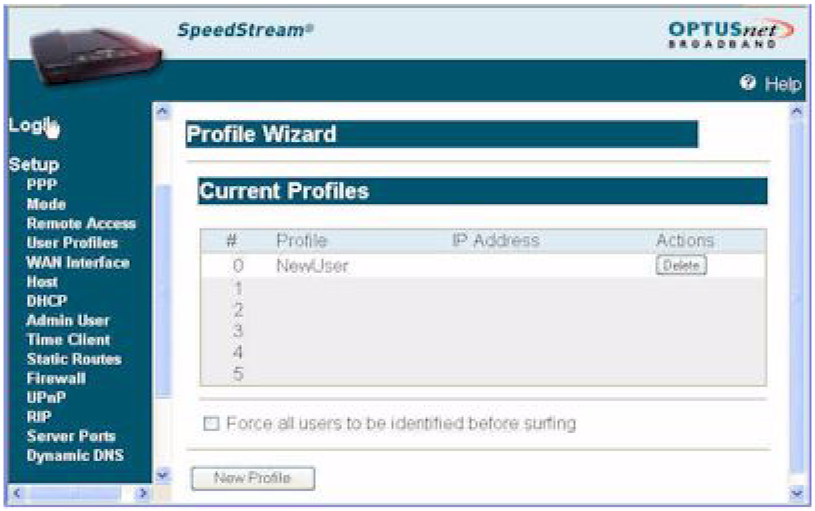
14. Optionally enter an **IP Address** to always be associated with this profile.
15. Click **Next**.
16. This completes the User Profile Wizard. Click **Finish** to close the Wizard and return to the Current Profiles page.

Editing User Profiles

This section describes how to edit a user.

To edit a user:

1. Select **Setup>User Profiles** from the left navigation pane of the Web interface. This displays the Current Profiles page listing all currently configured users.



Profile Wizard

Current Profiles

#	Profile	IP Address	Actions
0	NewUser		Delete
1			
2			
3			
4			
5			

□ Force all users to be identified before surfing

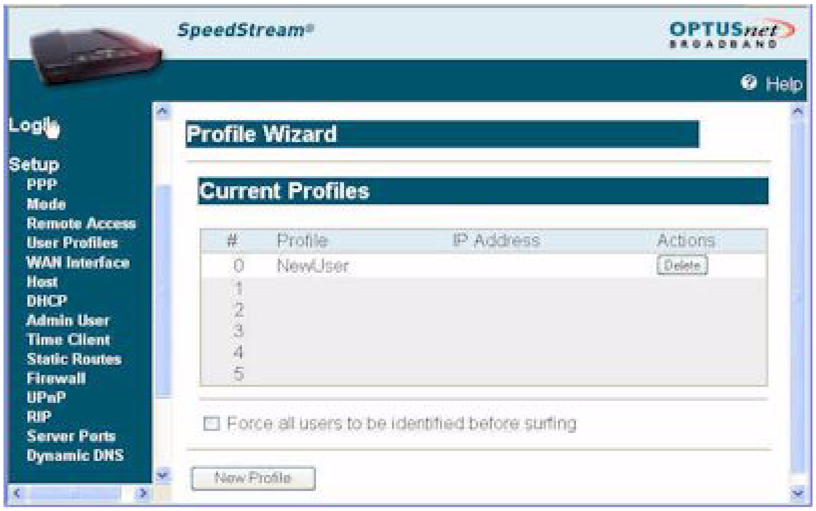
2. Click the name of the user you want to change. This displays the Profile User Information page. Make any desired changes.
3. Click **Next** to get to the next page you want to change. Make any desired changes.
4. Click **Finish** at any time when you are done making changes.

Deleting User Profiles

This section describes how to delete a user.

To delete a user:

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



Profile Wizard

Current Profiles

#	Profile	IP Address	Actions
0	NewUser		Delete
1			
2			
3			
4			
5			

□ Force all users to be identified before surfing

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

Chapter 4

Configuring ISP Connection Settings

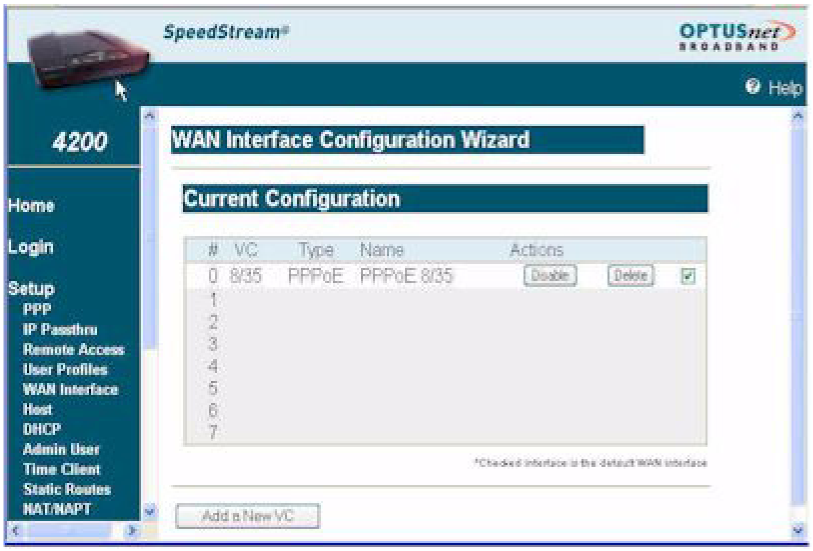
This chapter describes how to set advanced ISP connection settings. The options in this section should only be configured with the help and guidance of your ISP. Incorrect changes to any of these options could result in the failure of your internet connection.

The ISP connection options are listed below.

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

WAN Interface

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



WAN Interface Configuration Wizard

Current Configuration

#	VC	Type	Name	Actions		
0	8/35	PPPoE	PPPoE 8/35	Disable	Delete	☑
1						
2						
3						
4						
5						
6						
7						

*Checked interface is the default WAN interface

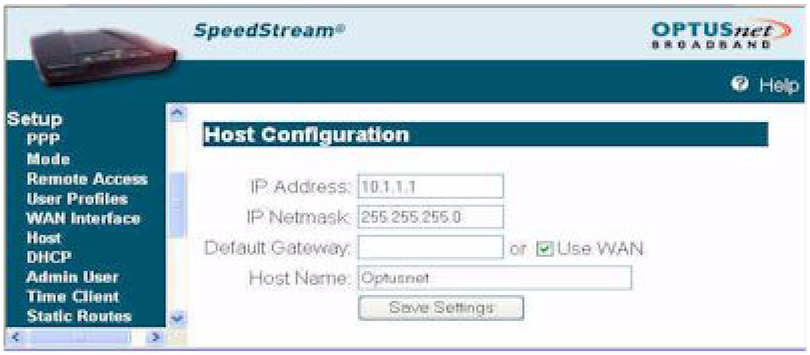
Add a New VC

Host

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

To specify host configuration settings:

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



Host Configuration

IP Address: 10.1.1.1
IP Netmask: 255.255.255.0
Default Gateway: or ☑ Use WAN
Host Name: Optusnet

2. Change settings as specified by your ISP.

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

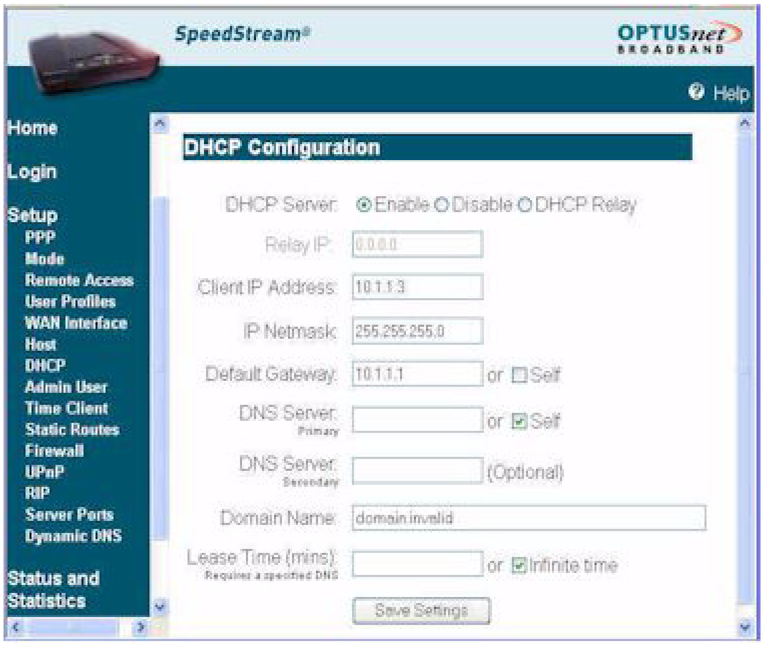
DHCP

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

Note: All addresses must be entered as an Ipv4 subnet mask in dotted-decimal notation (for example, 255.255.255.0).

To configure the DHCP feature:

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



DHCP Configuration

DHCP Server: ● Enable ○ Disable ○ DHCP Relay

Relay IP: 0.0.0.0

Client IP Address: 10.1.1.3

IP Netmask: 255.255.255.0

Default Gateway: 10.1.1.1 or □ Self

DNS Server Primary: or ☑ Self

DNS Server Secondary: (Optional)

Domain Name: domain.invalid

Lease Time (mins): Requires a specified DNS or ☑ Infinite time

2. Select one of the following:

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

  The DHCP operating mode defaults to **Enable**, and the system auto-generates the current IP address range, IP netmask, and default router. Do not change these default settings unless directed by your ISP.
- **Disable**
  Disables DHCP. If you are using a static IP address, you may need to disable DHCP and enter different addresses in the text boxes.
- **DHCP Relay**
  Instead of getting an IP address from the Router, the IP address is gotten from the computer as defined in **Relay IP**. Used when DHCP information is received from a DHCP server on the WAN side. DHCP requests are forwarded to the WAN side to **Relay IP**, and DHCP responses are forwarded back to the LAN side.

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

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

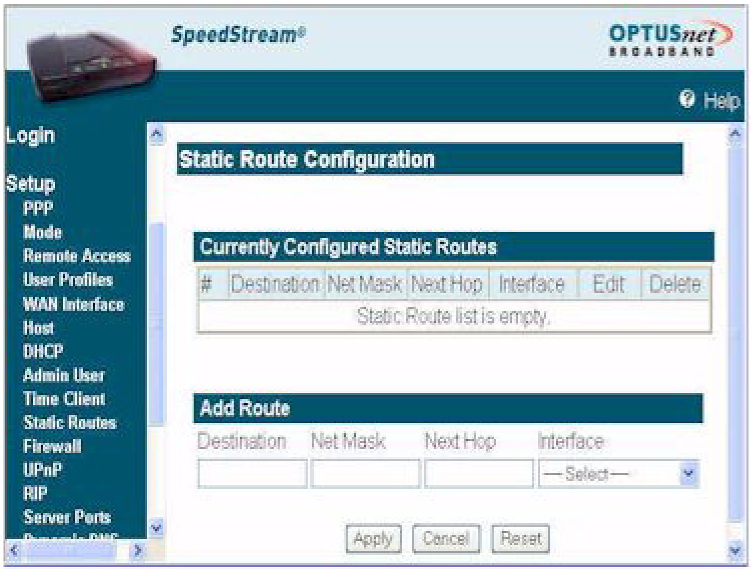
Static Routes

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

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

To configure a static route:

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



Static Route Configuration

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 —

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

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

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

Chapter 5 Configuring Network Settings

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

Mode — Configure the operation mode for the router.

UPnP (Universal Plug and Play) — Configure and control UPnP inter operability and security.

RIP (Routing Information Protocol) — Activate and control RIP functionality. Using RIP, the Router is able to determine the shortest distance between two points on the network based on the addresses of the originating devices.

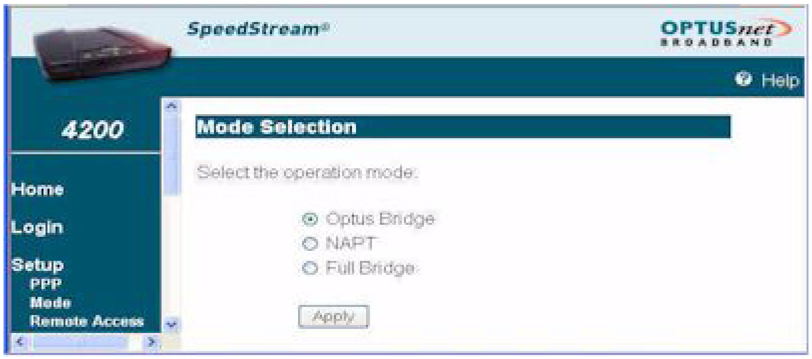
Server Ports — Specify server ports used by common applications such as HTTP (Web site traffic), FTP, and Telnet.

Dynamic DNS — Set up Dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names. For example, an IP address of 333.136.249.80 could be translated into siemens.com.

Mode

To select the operation mode for the router:

1. Select **Mode** from the left navigation pane of the Web interface. This displays the Mode selection page.



Mode Selection

Select the operation mode:

● Optus Bridge
○ NAPT
○ Full Bridge

2. Select one of the following operation modes. Upon selection, all associated parameters are set automatically for the router to operate according to the selected mode.
   - **Optus Bridge**
     Select this option if you are connected to one device.
   - **NAPT**
     Hosts located on a Local Area Network (LAN) are often required to use private IP addresses as opposed to public IP addresses. Private IP addresses, however, are not known on the public Wide Area Network (WAN). In order to expose LAN-side hosts assigned private IP addresses to the public WAN, the Router can be configured to use Network Address Port Translation (NAPT). NAPT can expose multiple LAN-side hosts.
   - **Full Bridge**
     The router acts as a bridge. Point-to-Point (PPP) connections are not available under the bridge mode of operation.

Important!ISwitching to Full Bridge will lose access to the Web interface.

3. Click **Apply**.

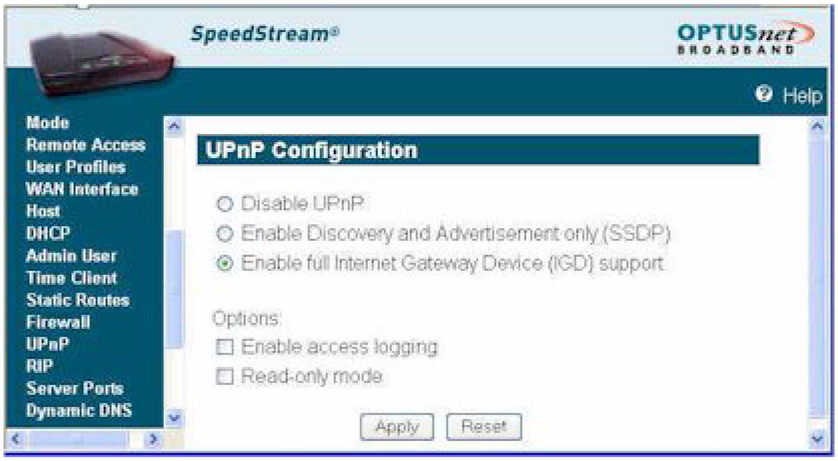
UPnP (Universal Plug and Play)

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

Only certain versions of Windows XP and computer support the UPnP (Universal Plug and Play) function. Before configuring this option, you must ensure that the UPnP component is installed on your computer and enabled.

To enable UPnP functionality:

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



UPnP Configuration

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

Options:
□ Enable access logging
□ Read-only mode

2. Select one of the following control options.
   - **Disable UPnP**
     Prevents the Router from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
   - **Enable Discovery and Advertisement only (SSDP)**
     Sends information about new devices (hardware) detected only. No information concerning software applications or services is transmitted.
   - **Enable full Internet Gateway Device (IGD) support**
     Allows the Router to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required.
3. Select one of the following options:
   - **Enable access logging**
     Generates a system log message whenever an UPnP client accesses the router.
   - **Read-only mode**
     Restricts the kind of access an UPnP client can have into the router. Only requests in the UPnP protocol that query the status of the router are allowed. Any requests that could potentially modify the router's behavior are blocked.
4. Click **Apply** to accept the settings. This displays the UPnP Finish page.

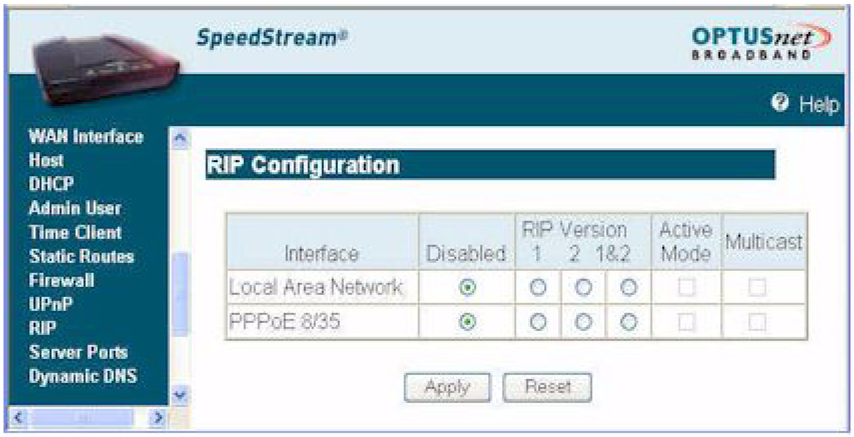
RIP (Routing Information Protocol)

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

Using RIP, the Router is able to determine the shortest distance between two points on the network based on the addresses of the originating devices. RIP is based on distance algorithms to calculate the shortest path using information in the routing table. The shortest path is based on the number of hops between two points.

To activate the RIP option:

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



RIP Configuration

Interface	Disabled	RIP Version			Active Mode	Multicast
		1	2	1&2		
Local Area Network	◉	○	○	○	□	□
PPPoE 8/35	◉	○	○	○	□	□

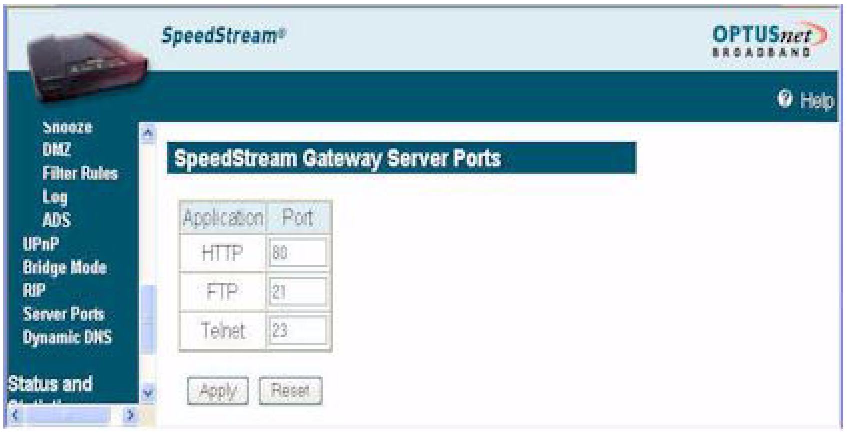
2. Select one of the following options from under the **RIP Version** heading next to the connection of your choice:
   - **1**: Provides essential RIP packet formatting for routing information packets.
   - **2**: Provides enhanced packet formatting for routing information packets by providing the following: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

Server Ports

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

To configure the server port option:

1. Select **Setup>Server Ports** from the left navigation pane of the Web interface. This displays the SpeedStream Gateway Server Ports page.



SpeedStream Gateway Server Ports

Application	Port
HTTP	80
FTP	21
Telnet	23

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

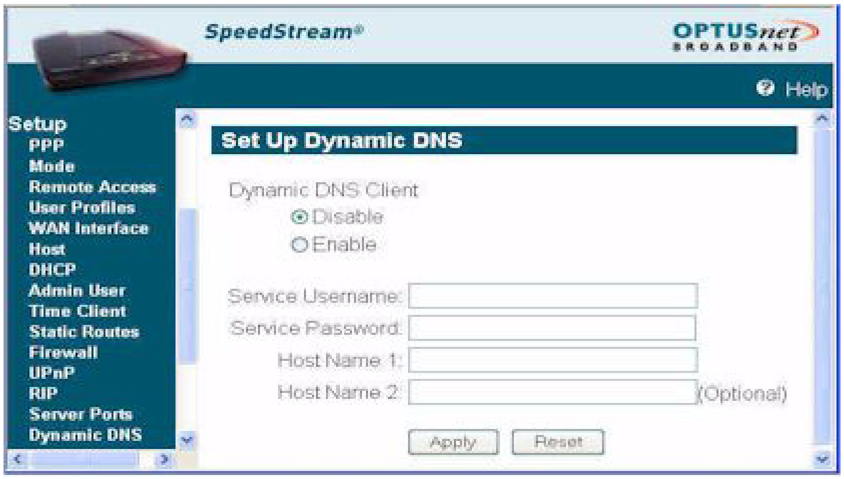
Dynamic DNS

Use the dynamic DNS advanced option to set up Dynamic DNS. Dynamic DNS translates IP addresses into alphanumeric names. For example, an IP address of 211.29.132.105 could be translated into www.optusnet.com.au. To use the DDNS service, you must register for the service. You can register from the following web page: www.dydns.org/services/dydns.

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

To set up Dynamic DNS on the Router:

1. Select **Setup>Dynamic DNS** from the left navigation pane of the Web interface. This displays the Set Up Dynamic DNS page.



Set Up Dynamic DNS

Dynamic DNS Client

● Disable

○ Enable

Service Username:

Service Password:

Host Name 1:

Host Name 2: (Optional)

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

Chapter 6

Configuring Security Features

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

Admin User — Manage administrator login name and password.

Time Client — Configure network-based date and time functionality. An accurate date and time is of use when logging system and firewall events and is a requirement for some firewall functionality (e.g., ICSA-compliant firewall operation).

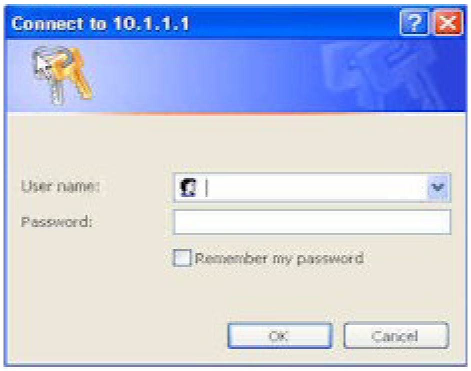
Firewall — Configure and control the internal firewall. Many of these features require a thorough understanding of networking principles and firewall operations. The firewall options are listed below.

Admin User

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

To configure administrator settings:

1. Select **Setup>Admin User** from the left navigation pane of the Web interface. This displays the Login page.



Connect to 10.1.1.1

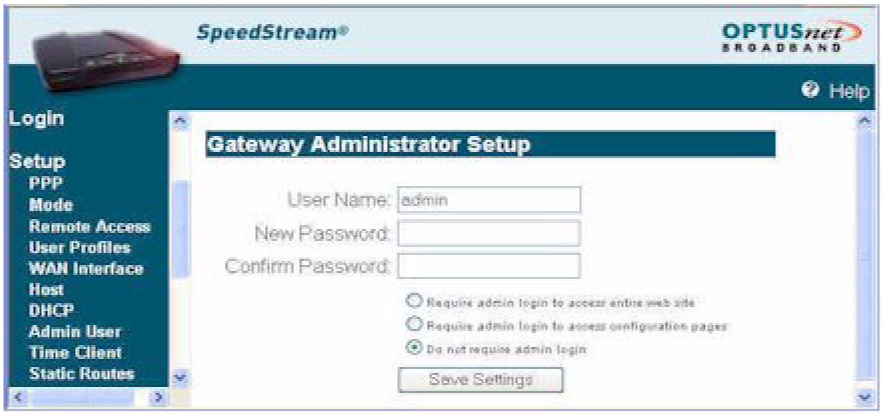
User name:

Password:

□ Remember my password

2. Do one of the following:
   - If this is the initial setup, enter **admin** in **User name** and click **OK**. (By default, the admin account does not have a Password defined.)
   - If you have already defined a password for the admin account, enter **admin** in **User Name** and the assigned password in **Password**. Then click **OK**.

   This displays the Gateway Administrator Setup page.



Gateway Administrator Setup

User Name: admin

New Password:

Confirm Password:

○ Require admin login to access entire web site

○ Require admin login to access configuration pages

● Do not require admin login

3. Specify a user name for the administrator. You may accept the default user name, admin, or enter a new user name in **User Name**. The user name is case-sensitive.
4. Enter a password in **New Password**; then enter the same password in **Confirm New Password**. The password field is case-sensitive.
5. Select a login security level from one of the following:
   - **Require admin login to access entire Web site**
     Before you can access any screen in the Web interface, you must log in with your network user name and password. (Security level = High)

- **Require admin login to access configuration pages**
  Before you can access any screen in the Web interface that allows you to make configuration changes, you must log in with your network user name and password. (Security level = Medium)
- **Do not require admin login**
  After you log in for the first time, you will not be required to log in again at any screen. (Security level = Low)

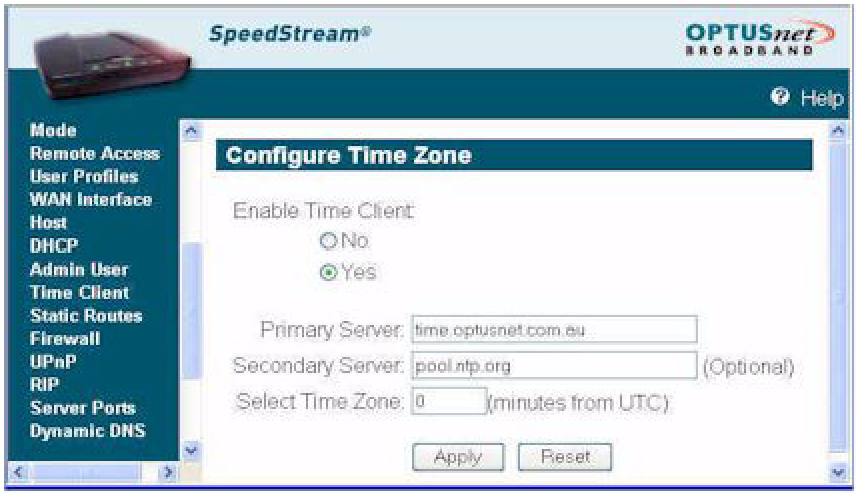
6. Click **Save Settings**.

Time Client

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

To configure the time client:

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



Configure Time Zone

Enable Time Client
○ No
● Yes

Primary Server: time.optusnet.com.au
Secondary Server: pool.ntp.org (Optional)
Select Time Zone: 0 (minutes from UTC)

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

Firewall

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

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

Level — Set the firewall security level.

Snooze — Temporarily disable the firewall. It is important to note that when the firewall is snoozing all protection provided by the firewall is disabled.

DMZ — Configure firewall DMZ for controlling a virtual DMZ on the Local Area Network. The purpose of the DMZ is to redirect suspicious network traffic received from a public WAN to a secured LAN-side host dedicated to this purpose.

Filter Rules — Add and delete custom inbound and outbound firewall rules.

Log — View log listing of firewall activity including records of denial of access, reason codes, and descriptions.

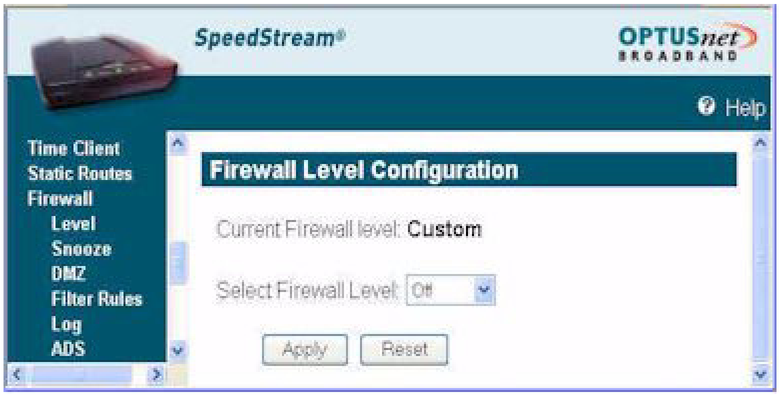
ADS — Configure what events the internal Attack Detection System (ADS) will protect against and log from a list of well-known attacks initiated on the Wide Area Network.

Level

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

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

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



Firewall Level Configuration

Current Firewall level: Custom

Select Firewall Level: Off

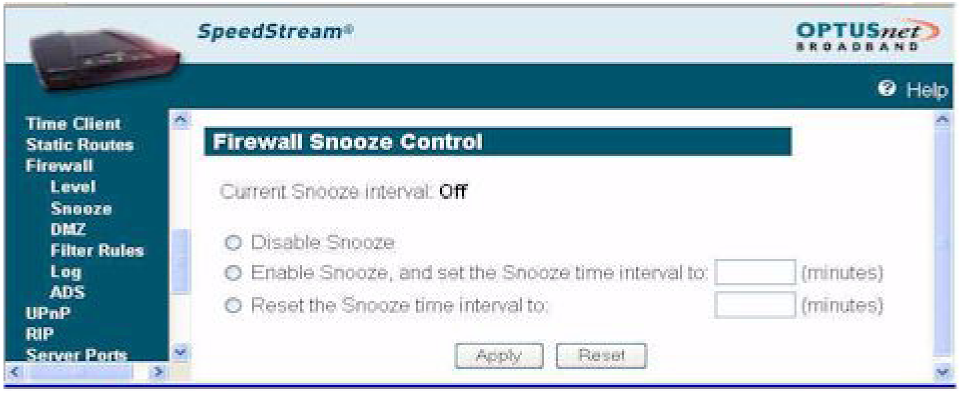
2. Select one of the following from the **Select Firewall Level** drop-down menu.
   - **Off**
     No restrictions are applied to either inbound or outbound traffic. In addition, Network Address Port Translation (NAPT) functionality is disabled. Because there is no address/port translation when the firewall is placed in this mode, all LAN-side connected hosts must be assigned a valid public IP address.
   - **Low**
     Minimal restrictions with respect to outbound traffic. Outbound traffic is allowed for all supported IP-based applications and Application Level Gateways (ALGs). The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host.
   - **High**
     High restrictions with respect to outbound traffic. Outbound traffic is allowed only for a very restricted set of supported IP-based applications and ALGs. The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host and permitted by this firewall mode.
   - **Custom**
     Allows advanced users to add, modify, and delete their own firewall rules. If you select this option, you must set customized rules for both inbound and outbound traffic using the IP Filtering option.
3. Click **Apply**.

Snooze

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

To enable and configure snooze control:

1. Select **Setup>Firewall>Snooze** from the left navigation pane of the Web interface. This displays the Firewall Snooze Control page.



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)

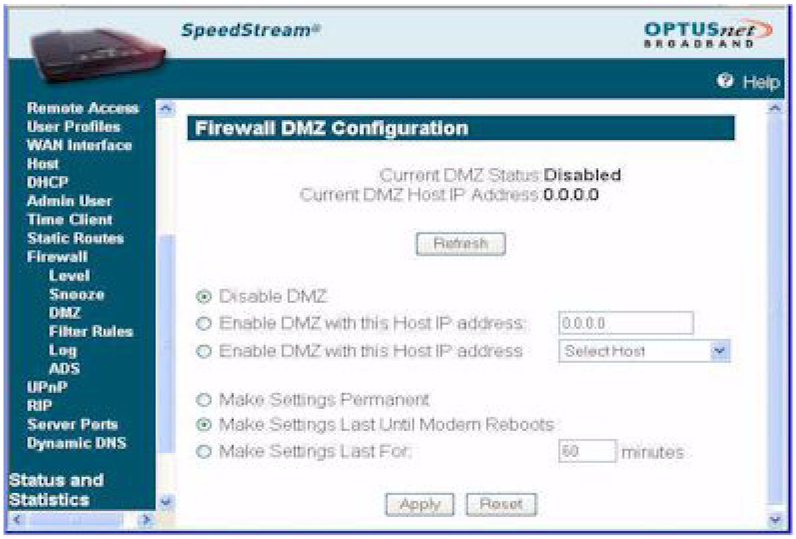
2. Select one of the following:
   - **Disable Snooze**
     Disables all snooze control. In this mode, the firewall is not disabled.
   - **Enable Snooze, and set the Snooze time interval to**
     Enables snooze for a specified time period. Be sure to enter the number of minutes to define how long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

DMZ

The firewall supports virtual DMZ. Virtual DMZ redirects traffic to a specified IP address rather than a physical port. Because this redirection is a logical application rather than physical, it is called "virtual DMZ.". Using virtual DMZ, a single node on the LAN can be made "visible" to the WAN IP network. Any incoming network traffic not handled by port forwarding rules is automatically forwarded to an enabled DMZ node. Outbound traffic from the virtual DMZ node circumvents all firewall rules. The DMZ feature allows a computer on your home network to circumvent the firewall and have direct access to the internet. This feature is primarily used for gaming. Under this mode of operation all network traffic received from the WAN that is not destined for a host specifically exposed through NAT or for a server exposed through Port Forwarding will be redirected to the designated DMZ host. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host.

This function is recommended for use only when you require this special level of unrestricted access as it leaves your Router and network exposed to the Internet with no firewall protection. To enable and configure the DMZ:

1. Select **Setup>Firewall>DMZ** from the left navigation pane of the Web interface. This displays the Firewall DMZ Configuration page.



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 IP address Select Host

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

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

Filter Rules

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

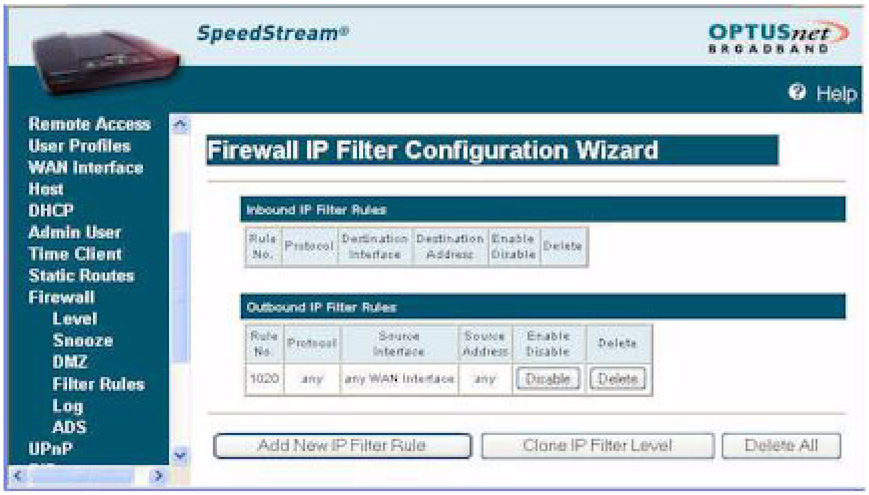
Rules can be filter-based on any of the following:

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

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

To define inbound and outbound IP filter rules:

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



Firewall IP Filter Configuration Wizard

Inbound IP Filter Rules

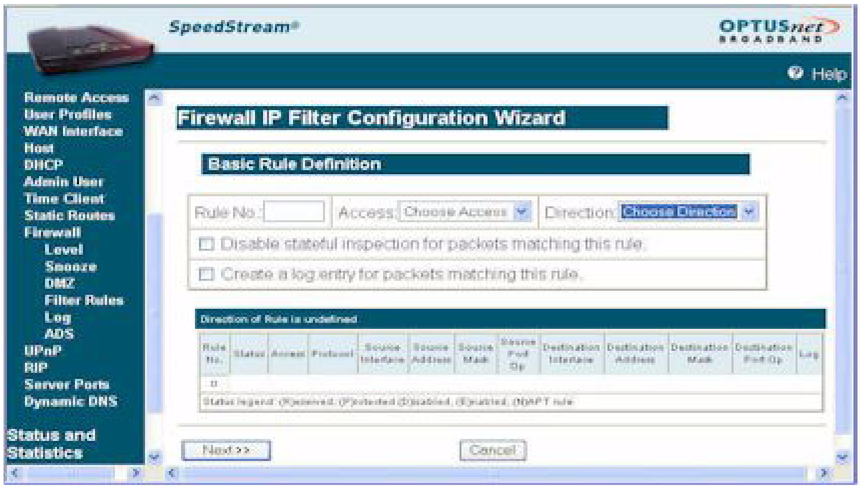
Rule No.	Protocol	Destination Interface	Destination Address	Enable Disable	Delete

Outbound IP Filter Rules

Rule No.	Protocol	Source Interface	Source Address	Enable Disable	Delete
1020	any	any WAN Interface	any	Disable	Delete

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

Create Custom IP Filter Rules



Firewall IP Filter Configuration Wizard

Basic Rule Definition

Rule No: Access: Choose Access Direction: Choose Direction

□ Disable stateful inspection for packets matching this rule.

□ Create a log entry for packets matching this rule.

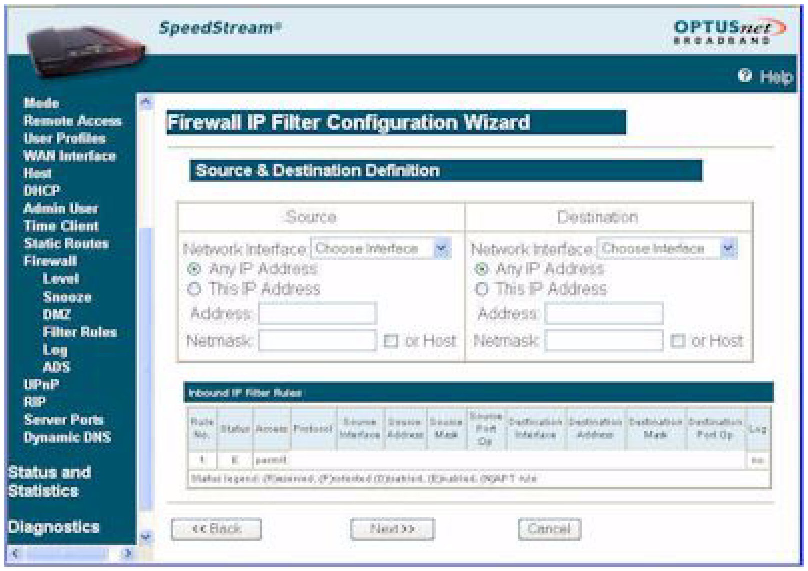
Direction of Rule is undefined

Rule No.	Status	Access	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Log
0												

Status legend: (R)eserved, (P)rotected (D)isabled, (E)nabled, (N)APT rule

To add a new rule:

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



Firewall IP Filter Configuration Wizard

Source & Destination Definition

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

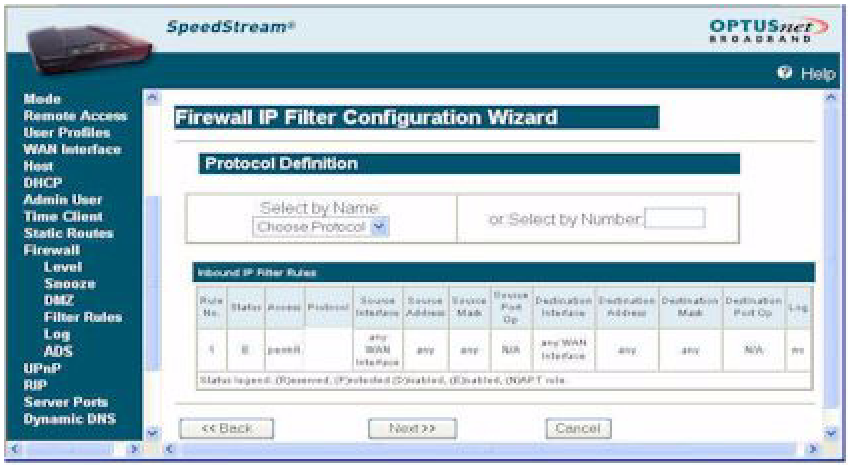
Inbound IP Filter Rules

Rule No.	Status	Access	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Log
1	E	permit										no

Status legend: (R)eserved, (P)rotected (D)isabled, (E)nabled, (N)APT rule

7. Under the **Source** heading, select a network connection from the **Network Interface** drop-down menu.

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



Firewall IP Filter Configuration Wizard

Protocol Definition

Select by Name: Choose Protocol | or Select by Number

Inbound IP Filter Rules

Rule No.	Status	Access	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Log
1	E	permit		any WAN Interface	any	any	N/A	any WAN Interface	any	any	N/A	no

Status legend: (R)eserved, (P)rotected (D)isabled, (E)nabled, (N)APT rule

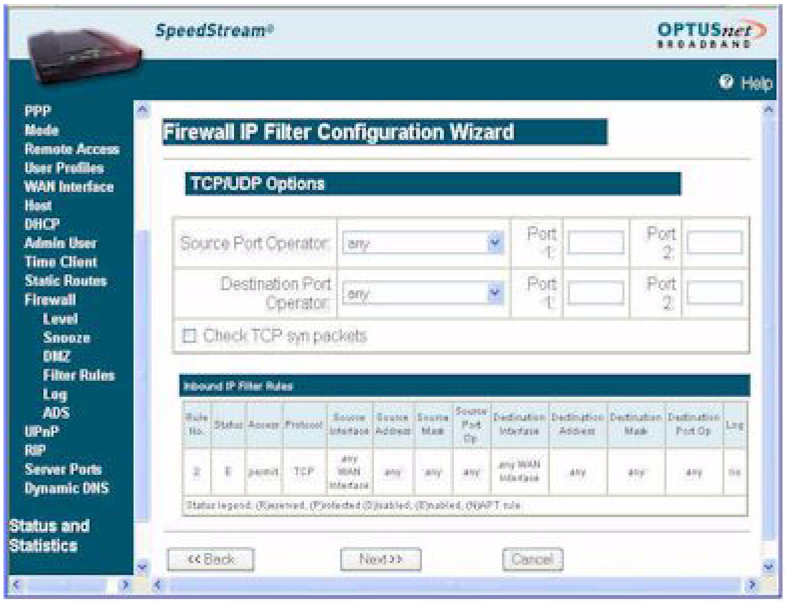
14. Do one of the following:
    - Select one of the following protocol options from the **Select by Name** drop-down menu. This defines the types of packets filtered.
      - **Any Protocol**
      - **TCP (Transmission Control Protocol)**
        Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users. Click **Next** to display the "TCP/UDP Options Page".
      - **UDP** (User Datagram Protocol)
        Provides for the exchange of datagrams without acknowledgement or guaranteed delivery. Click **Next** to display the "TCP/UDP Options Page".

  - **ICMP** (Internet Control Message Protocol)
    A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command. Click **Next** to display the "ICMP Options Page".
  - **GRE** (Generic Routing Encapsulation):
    A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
- Type a protocol number in the **Select by Number** field.

15. Click **Next**. This displays the Finish page.
16. Click **Finish**.

TCP/UDP Options Page

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



Firewall IP Filter Configuration Wizard

TCP/UDP Options

Source Port Operator: any | Port 1: | Port 2:

Destination Port Operator: any | Port 1: | Port 2:

□ Check TCP syn packets

Inbound IP Filter Rules

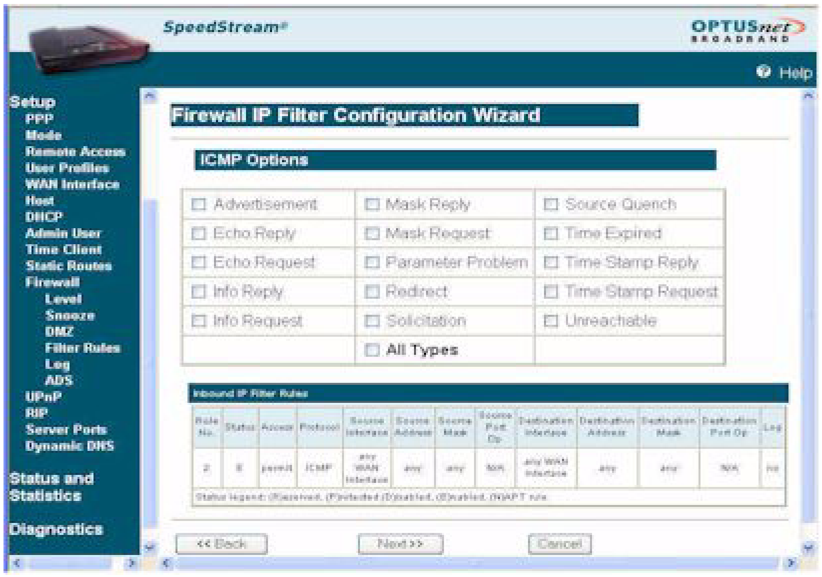
Rule No.	Status	Access	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Log
2	E	permit	TCP	any WAN interface	any	any	any	any WAN interface	any	any	any	no

Status legend: (R)eserved, (P)rotected (D)isabled, (E)nabled, (N)APT rule

1. Select one of the following options from the **Source Port Operator** drop-down menu and the **Destination Port Operator** drop-down menu:
   - **any**
     Any port is acceptable as the source/destination port.
   - **less than or equal to**
     A port less than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **equal to**
     A port equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **greater than or equal to**
     a port greater than or equal to the numeric value in the **Port 1** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** field.
   - **range**
     Any port between the value of the entry in the **Port 1** field and the value in the **Port 2** field is acceptable as the source/destination port. Be sure to provide a value in the **Port 1** and **Port 2** fields.
2. Optionally, select the **Check TCP syn packets** checkbox if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
3. Click **Next**.
4. Click **Finish**.

ICMP Options Page

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



Firewall IP Filter Configuration Wizard

ICMP Options

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

Inbound IP Filter Rules

Rule No.	Status	Access	Protocol	Source Interface	Source Address	Source Mask	Source Port Op	Destination Interface	Destination Address	Destination Mask	Destination Port Op	Log
2	E	permit	ICMP	any WAN Interface	any	any	N/A	any WAN Interface	any	any	N/A	no

Status legend: (R)eserved, (P)rotected (D)isabled, (E)nabled, (N)APT rule

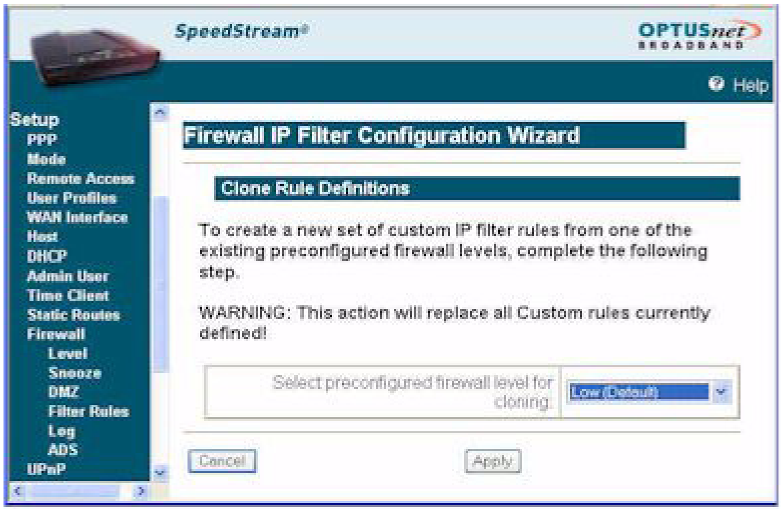
1. Do one of the following:
   - Select any of the ICMP options you wish to filter.
   - Select the **All Types** checkbox to filter all options.
2. Click **Next**.
3. Click **Finish**.

Clone IP Filter Rules

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

To clone IP filter rules:

1. Click **Clone IP Filter Level** from the Firewall IP Filter Configuration Wizard page. This displays the Clone Rule Definition page.



Firewall IP Filter Configuration Wizard

Clone Rule Definitions

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!

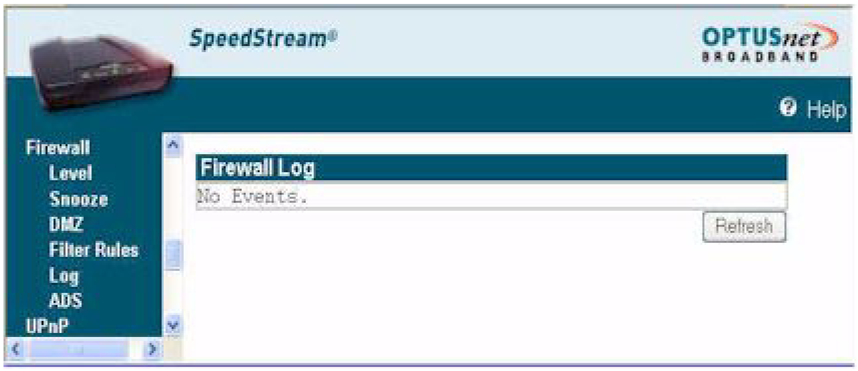
Select preconfigured firewall level for cloning: Low (Default)

2. Select one of the following from the **Select preconfigured firewall level for cloning** drop-down menu.
   - **Low**
     Clones low-level IP filter rules, which provide minimal restrictions with respect to outbound traffic. Outbound traffic is allowed for all supported IP-based applications and Application Level Routers (ALGs). The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host. This is the default.
   - **Medium**
     Clones medium-level IP filter rules, which provides moderate restrictions with respect to outbound traffic. Outbound traffic is allowed for most supported IP-based applications and Application Level Routers (ALGs). The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host.
   - **High**
     Clones high-level IP filter rules, which provide high restrictions with respect to outbound traffic. Outbound traffic is allowed only for a very restricted set of supported IP-based applications and ALGs. The only inbound traffic allowed is traffic received within the context of an outbound session initiated on the local host and permitted by this firewall mode.
   - **ICSA 3.0a-compliant**
     Clones ICSA 3.0a-compliant filter rules, which supports the ICSA Labs criteria for firewall behavior. (For more information, visit the ICSA site at http://www.icsalabs.com).
3. Click **Apply**. This displays the Firewall IP Filter Configuration Wizard page with the selected rule set showing in the Rule Definition table.
4. Disable or delete any rule as desired.

Log

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

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



Firewall Log

```
No Events.
```

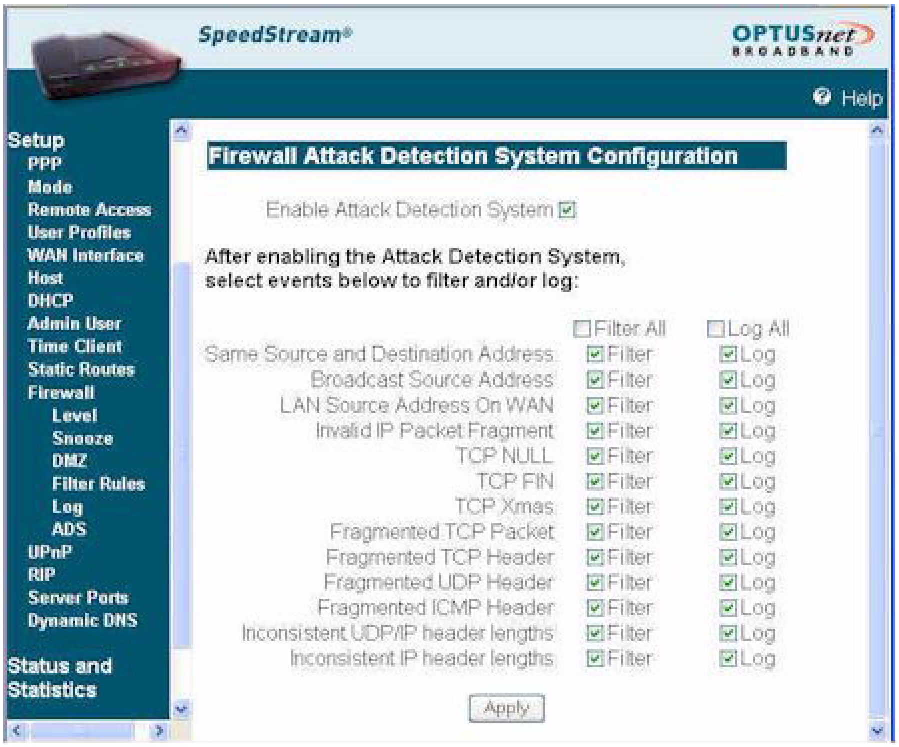
ADS

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

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

To enable and configure the attack detection feature:

1. Select **Setup>Firewall>ADS** from the left navigation pane of the Web interface. This displays the Firewall Attack Detection System page.



Firewall Attack Detection System Configuration

Enable Attack Detection System ☑

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

	□ Filter All	□ Log All
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
Inconsistent UDP/IP header lengths	☑ Filter	☑ Log
Inconsistent IP header lengths	☑ Filter	☑ Log

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

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

- **Same Source and Destination Address**
  An outside device can send a SYN (synchronize) packet to a host with the same source and destination address (including port) causing the system to hang. When the receiving host tries to respond to the source

address in the packet, it ends up just sending it back to itself. This packet could ping-pong back and forth over 200 times (consuming CPU resources) before being discarded.

- **Broadcast Source Address**
  An outside device can send a ping to your Router broadcast address using a forged source address. When your system responds to these pings, it is brought down by echo replies.
- **LAN Source Address on LAN**
  An outside device can send a forged source address in an incoming IP packet to block trace back.
- **Invalid IP Packet Fragment**
  An outside device can send fragmented data packets that can bring down your system. IP packets can be fairly large in size. If a link between two hosts transporting a packet can only handle smaller packets, the large packet may be split (or fragmented) into smaller ones. When the packet fragments get to the destination host, they must be reassembled into the original large packet like pieces of a puzzle. A specially crafted invalid fragment can cause the host to crash
- **TCP NULL**
  An outside device can send an IP packet with the protocol field set to TCP but with an all null TCP header and data section. If your Router responds to this attack, it will bring down your system.
- **TCP FIN**
  An outside device can send an attack using TCP FIN. This attack never allows a data packet to finish transmitting and brings down your system.
- **TCP XMAS**
  An outside device can send an attack using TCP packets with all the flags set. This causes your system to slow to a halt.
- **Fragmented TCP Packet**
  An outside device can send an attack using fragmented packets to allow an outside user Telnet access to a device on your network.
- **Fragmented TCP Header**
  An outside device can send an attack using TCP packets with only a header and no payload. When numerous packets are sent through the Router in this manner, your system slows and halts.
- **Fragmented UDP Header**
  An outside device can send an attack using fragmented UDP headers to bring down a device on your network.
- **Fragmented ICMP Header**
  An outside device can send an attack using fragmented ICMP headers to bring down a device on your network.
- **Inconsistent UDP/IP header lengths**
  An outside device can send an attack using inconsistent UDP/IP headers to bring down a device on your network.
- **Inconsistent IP header lengths**
  An outside device can send an attack using changes in the IP header to zero the fragment offset field. This will be treated as a complete packet when received and cause your system to halt.

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						√		√		
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				√		√		√		√
Tiberian Sun				√		√		√		
Traceroute		√		√		√		√		
Ultima Online				√		√		√		
Unreal Tournament				√		√		√		
VNC						√		√		
Warcraft				√		√		√		
Windows Media Player		√		√		√		√		
XDM						√		√		
Yahoo Messenger						√		√		

Chapter 7 Monitoring Router Health

This chapter describes how to monitor the health of the Router. The Router health options listed below are used to gauge the Router's health.

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

Status and Statistics

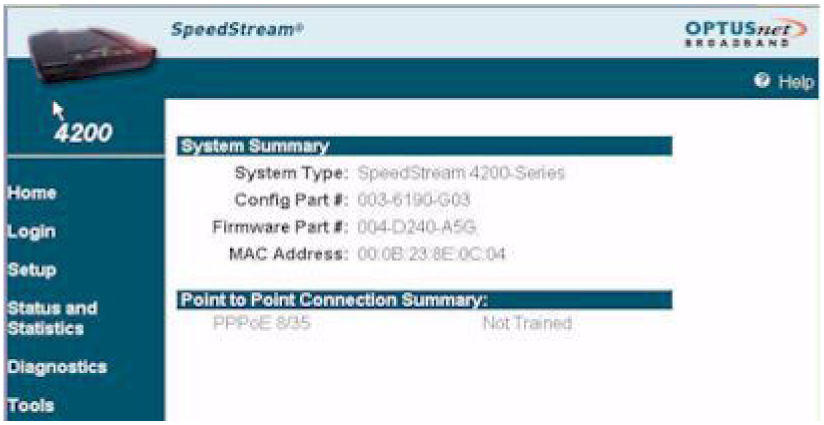
You can display statistics for the Internet, Home Networking, Security, and Logging.

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

System Summary

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

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



System Summary

System Type: SpeedStream 4200-Series
Config Part #: 003-6190-G03
Firmware Part #: 004-D240-A5G
MAC Address: 00:0B:23:8E:0C:04

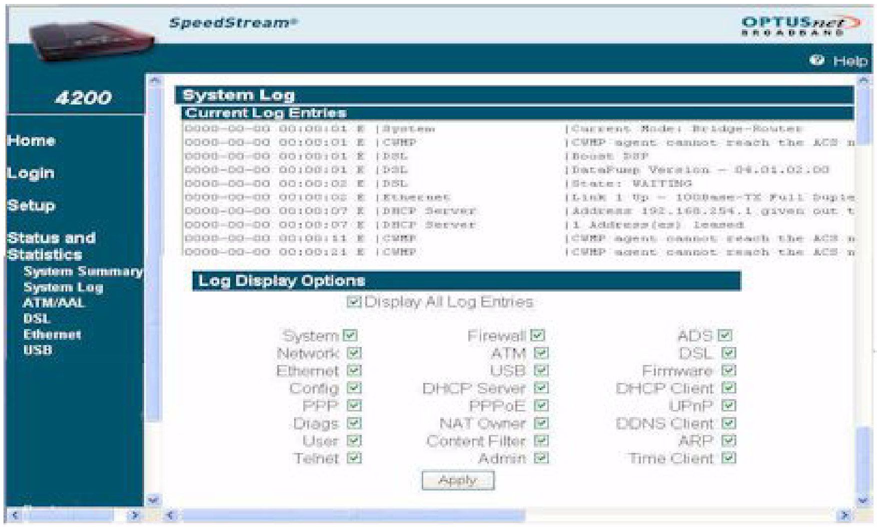
Point to Point Connection Summary:

PPPoE 8/35 Not Trained

System Log

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

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



System Log

Current Log Entries

```
0000-00-00 00:00:01 E |System          |Current Mode: Bridge-Router
0000-00-00 00:00:01 E |CWMP            |CWMP agent cannot reach the ACS n
0000-00-00 00:00:01 E |DSL             |Boost DSP
0000-00-00 00:00:01 E |DSL             |DataPump Version - 04.01.02.00
0000-00-00 00:00:02 E |DSL             |State: WAITING
0000-00-00 00:00:02 E |Ethernet        |Link 1 Up - 100Base-TX Full Duple
0000-00-00 00:00:07 E |DHCP Server     |Address 192.168.254.1 given out t
0000-00-00 00:00:07 E |DHCP Server     |1 Address(es) leased
0000-00-00 00:00:11 E |CWMP            |CWMP agent cannot reach the ACS n
0000-00-00 00:00:21 E |CWMP            |CWMP agent cannot reach the ACS n
```

Log Display Options

☑ Display All Log Entries

System ☑	Firewall ☑	ADS ☑
Network ☑	ATM ☑	DSL ☑
Ethernet ☑	USB ☑	Firmware ☑
Config ☑	DHCP Server ☑	DHCP Client ☑
PPP ☑	PPPoE ☑	UPnP ☑
Diags ☑	NAT Owner ☑	DDNS Client ☑
User ☑	Content Filter ☑	ARP ☑
Telnet ☑	Admin ☑	Time Client ☑

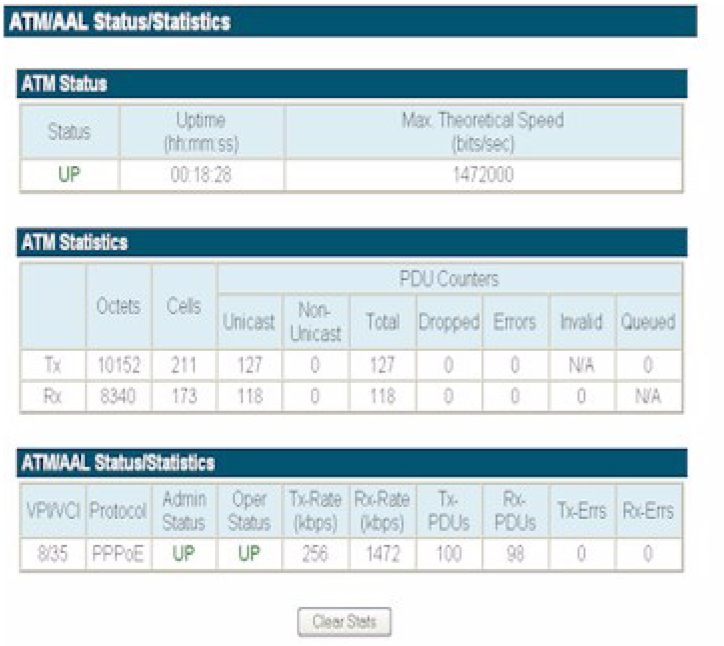
Apply

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

ATM Statistics

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

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



ATM/AAL Status/Statistics

ATM Status

Status	Uptime (hh:mm:ss)	Max. Theoretical Speed (bits/sec)
UP	00:18:28	1472000

ATM Statistics

	Octets	Cells	PDU Counters						
			Unicast	Non-Unicast	Total	Dropped	Errors	Invalid	Queued
Tx	10152	211	127	0	127	0	0	N/A	0
Rx	8340	173	118	0	118	0	0	0	N/A

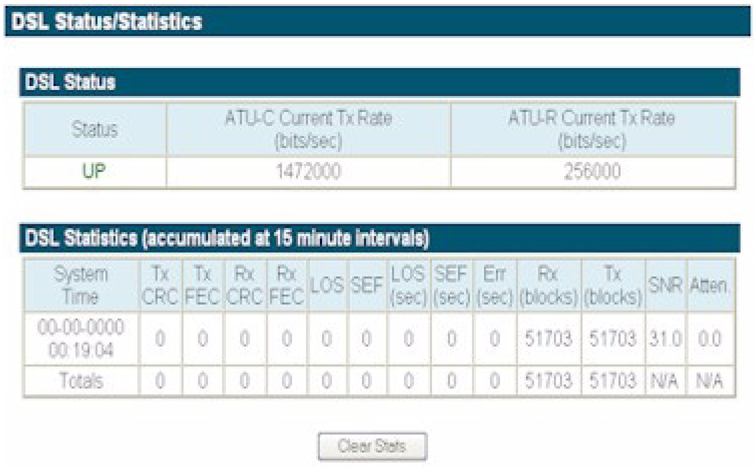
ATM/AAL Status/Statistics

VPI/VCI	Protocol	Admin Status	Oper Status	Tx-Rate (kbps)	Rx-Rate (kbps)	Tx-PDUs	Rx-PDUs	Tx-Errs	Rx-Errs
8/35	PPPoE	UP	UP	256	1472	100	98	0	0

DSL Statistics

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

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



DSL Status/Statistics

DSL Status

Status	ATU-C Current Tx Rate (bits/sec)	ATU-R Current Tx Rate (bits/sec)
UP	1472000	256000

DSL Statistics (accumulated at 15 minute intervals)

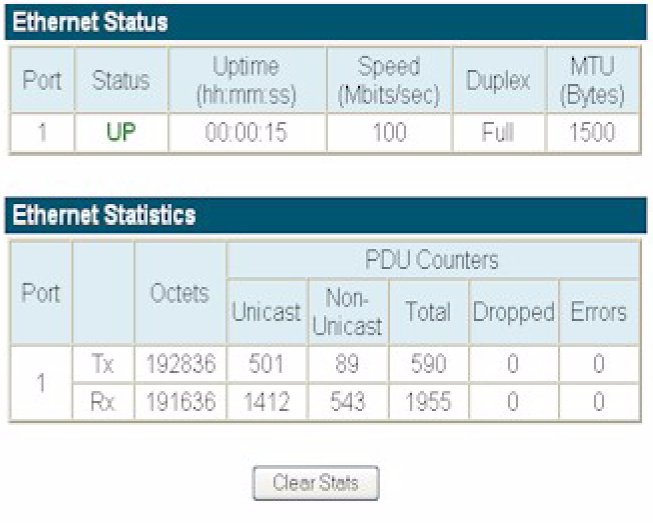
System Time	Tx CRC	Tx FEC	Rx CRC	Rx FEC	LOS	SEF	LOS (sec)	SEF (sec)	Err (sec)	Rx (blocks)	Tx (blocks)	SNR	Atten
00-00-0000 00:19:04	0	0	0	0	0	0	0	0	0	51703	51703	31.0	0.0
Totals	0	0	0	0	0	0	0	0	0	51703	51703	N/A	N/A

Ethernet Statistics

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

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

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



Ethernet Status

Port	Status	Uptime (hh:mm:ss)	Speed (Mbits/sec)	Duplex	MTU (Bytes)
1	UP	00:00:15	100	Full	1500

Ethernet Statistics

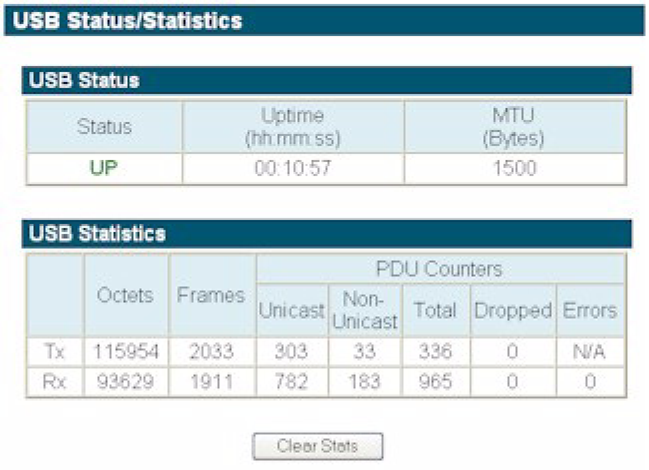
Port		Octets	PDU Counters				
			Unicast	Non-Unicast	Total	Dropped	Errors
1	Tx	192836	501	89	590	0	0
	Rx	191636	1412	543	1955	0	0

USB Statistics

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

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

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



USB Status/Statistics

USB Status

Status	Uptime (hh:mm:ss)	MTU (Bytes)
UP	00:10:57	1500

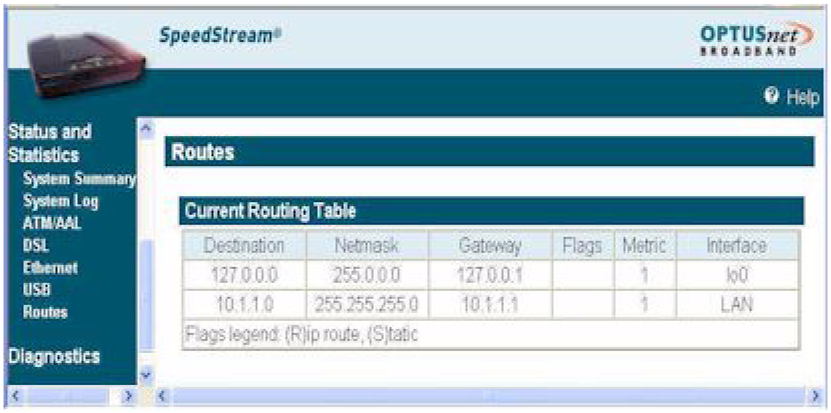
USB Statistics

	Octets	Frames	PDU Counters				
			Unicast	Non-Unicast	Total	Dropped	Errors
Tx	115954	2033	303	33	336	0	N/A
Rx	93629	1911	782	183	965	0	0

Routes

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

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



Routes

Current Routing Table

Destination	Netmask	Gateway	Flags	Metric	Interface
127.0.0.0	255.0.0.0	127.0.0.1		1	lo0
10.1.1.0	255.255.255.0	10.1.1.1		1	LAN

Flags legend: (R)ip route, (S)tatic

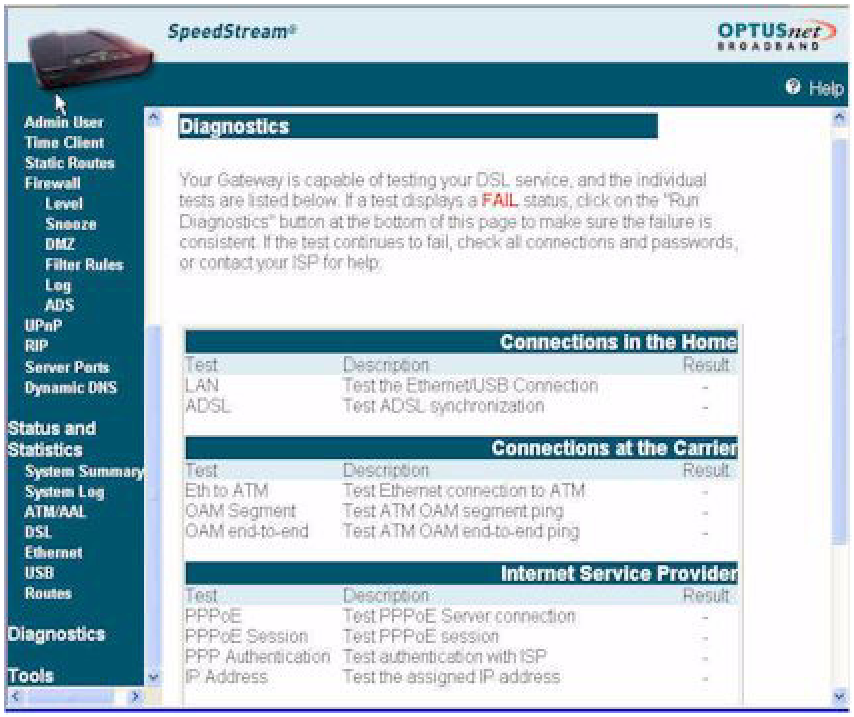
Diagnostics

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

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

To run diagnostics:

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



Diagnostics

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

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

Connections at the Carrier		
Test	Description	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	-

Internet Service Provider		
Test	Description	Result
PPPoE	Test PPPoE Server connection	-
PPPoE Session	Test PPPoE session	-
PPP Authentication	Test authentication with ISP	-
IP Address	Test the assigned IP address	-

2. Select the connection you want to test from the **Connection to Test** drop-down menu.
3. Click **Run Diagnostics**. The test results display under the **Results** column.

   If one of the following failed, contact OptusNet.

   - **Connections at the Carrier**
   - Independent Service Provider
   - Internet Connectivity
4. If a test displays a **FAIL** status for any other reason then listed above, click **Run Diagnostics** again to confirm the failure.
5. If the test still displays a **FAIL** status, check all connections and passwords; then click **Run Diagnostics** again.
6. If the test still displays a **FAIL** status, contact OptusNet for further assistance.

Tools

This section describes how to use the tools listed below.

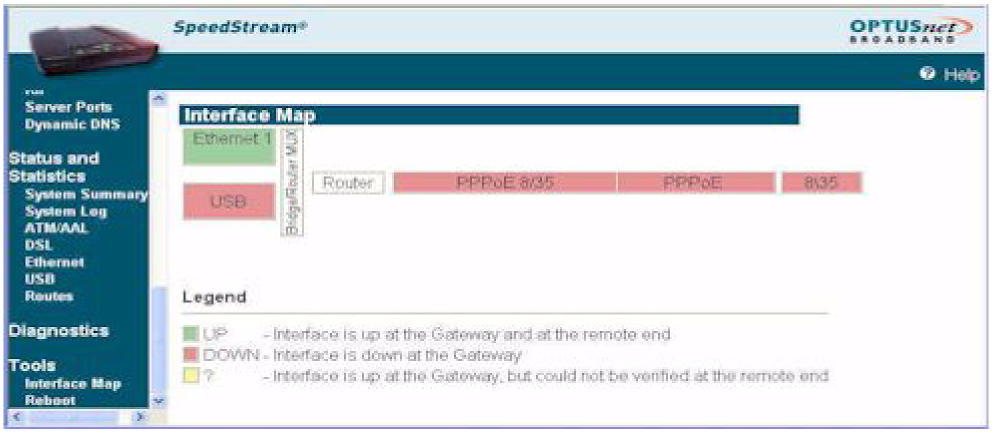
Interface Map	View a graphical representation of the current LAN and WAN configurations.
Reboot	Reboot the Router.

Interface Map

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

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

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



🟩 UP - Interface is up at the Gateway and at the remote end

🟥 DOWN - Interface is down at the Gateway

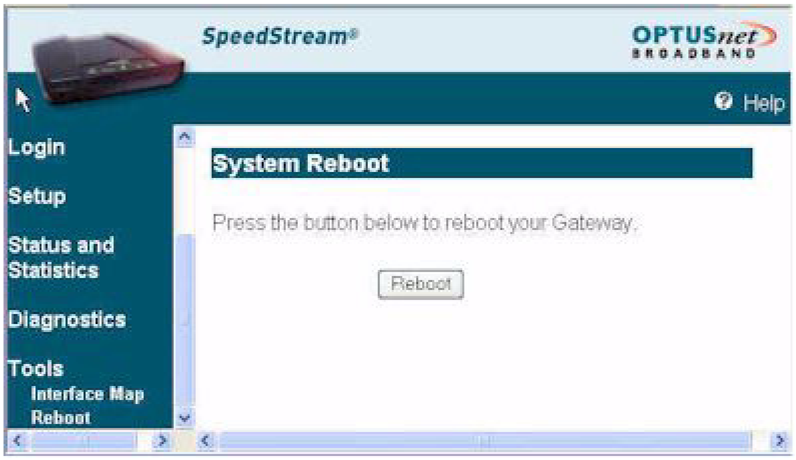
🟨 ? - Interface is up at the Gateway, but could not be verified at the remote end

Reboot

You can reboot the Router using the Reboot option, or you can reset the Router to factory defaults using the Reset option. Reboot should be used when the Router needs to be restarted without losing your current configuration settings.

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

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



System Reboot

Press the button below to reboot your Gateway.

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

Reset to system defaults:

Reset the Router to system defaults should be done when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the Router does not appear to be working properly. **Important**: This option resets all custom settings, users, and passwords on your Router.

To reset the Router:

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

To cancel the reset:

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

Chapter 8 Troubleshooting

Connection problems usually occur when the Router’s software configuration contains incomplete or incorrect information. The Router’s diagnostic tools can help yo identify and solve many of these problems. 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	Ethernet	DSL	USB	Activity
Off	Power not applied	– Power not applied – Ethernet link not connected	– Power not applied – DSL signal not detected	– Power not applied – No USB connection	– Power not applied – No PPP connection
Green	Normal system operation	Ethernet link connected	DSL line is trained and ready for traffic	USB connected	PPPoE session established
Blinking Green	N/A	Ethernet traffic flowing in either direction	DSL is training	USB user traffic flowing in either direction	Establishing PPPoE session
Red	Self-test failure if red for more than 30 sec	N/A	N/A	N/A	N/A
Blinking Red Green	Flash write in progress	N/A	N/A	N/A	N/A

Resolving Specific Issues

Power LED Not Lit

If the 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.

Ethernet 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 *Power* LED)

POST is the router's "power-on self-test." When you power on or reboot the router, the Power 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 Power LED changes to solid green.
- If the initial POST diagnostic tests fail, the Power 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 Siemens Australia Technical Support during the hours of 8:00 to 5:00 PM EST//EDST.

Telephone: 03 9721 2173 or 03 9721 2183

Email: ic.services@siemens.com.au

Internet: http://www.siemens.com.au/modems

To assist you with any technical queries for your Optusnet Internet connection, please contact us on Optus Support on 1300 309 333 AEST between:

8.00 am - 9.00pm Monday to Friday

8.30am - 7.00pm Saturday