

SpeedStream®

Wireless DSL Gateway User's Guide

Model 6200/6300

REV 2.55



Part No. 007-0939-002

© Copyright 2003, Efficient Networks, Inc.

All rights reserved. Printed in the U.S.A.

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

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

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

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

Software License

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

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

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

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

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

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

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

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

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

Limited Warranty

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

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

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

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

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

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

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

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

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

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

5. Limitations.

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

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

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

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

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

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

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

General Provisions

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

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

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

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

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

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

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

Contents

CHAPTER 1 INTRODUCTION	1
Features of the Wireless DSL Gateway	1
Network (LAN) Features	1
Security Features	2
Configuration & Management	2
Advanced Gateway Functions	2
Minimum System Requirements	3
USB Driver-Related Requirements	3
Package Contents.....	3
Physical Details	4
LEDs.....	4
Rear Panel.....	5
General Safety Guidelines.....	7
CHAPTER 2 INSTALLATION.....	8
Minimum System Requirements	8
Hardware Installation	8
Basic Installation Procedure	8
Wireless Card Installation (Model 6200)	9
Installing Line Filters.....	9
In-Line Filter	9
Wall-Mount Filter.....	10
Two-to-One Adapter	10
Installation Methods	10
Ethernet Installation Method	10
USB Installation Method (Microsoft Windows)	12
USB Driver Installation (Macintosh Systems)	13
CHAPTER 3 OPERATING SYSTEM CONFIGURATION.....	14
Overview.....	14
Windows Configuration	14
Checking TCP/IP Settings (Windows 9x/ME).....	14
Checking TCP/IP Settings (Windows 2000).....	15
Checking TCP/IP Settings (Windows XP).....	17
Internet Access	18
For Windows 9x/2000.....	18
For Windows XP.....	19
Macintosh Configuration	19
Checking TCP/IP Settings (MAC OS 8.6 through 9.x).....	19
Checking TCP/IP Settings (MAC OS X)	20
CHAPTER 4 SPEEDSTREAM GATEWAY SETUP	21
Overview.....	21
Configuration Program.....	21
Preparation.....	22

Connecting to the Gateway.....	22
Using UPnP (Windows XP and Me).....	22
Using your Web Browser.....	22
Setup Wizard.....	23
Gateway Setup Wizard.....	23
Wireless Setup WEP 64-Bit Option.....	26
Wireless Setup WEP 128-Bit Option.....	28
Wireless Setup WPA PSK Option.....	30
Gateway Environment.....	32
Home Window.....	32
Menu Bar.....	32
Toolbar.....	33
Logging into the Gateway.....	33
Logging out of the Gateway.....	34
Gateway Options.....	34
CHAPTER 5 GATEWAY CONFIGURATION OPTIONS.....	35
Overview.....	35
Users.....	35
Adding a User.....	36
Content Filtering (Optional).....	37
Profile Configuration Access (Optional).....	38
Profile Time Settings (Optional).....	39
Associated Computer/Connected Device (Optional).....	39
Customized Profile Icon (Optional).....	40
Editing a User.....	41
Deleting a User.....	42
Viewing User Logs.....	43
Devices.....	44
Gateway.....	45
ISP Connection.....	45
Advanced Internet Options.....	47
ATM Virtual Circuits.....	47
Static Routes.....	47
Routing Table.....	49
Dynamic DNS.....	49
RIP (Routing Information Protocol).....	54
Home Network.....	55
IP Network.....	56
Server Ports.....	57
LAN/WAN Port.....	58
Wireless Network (Optional).....	59
Wireless Setup WEP 64-Bit Option (Advanced Home Networking).....	61
Wireless Setup WEP 128-Bit Option (Advanced Home Networking).....	63
Wireless Setup WPA PSK Option (Advanced Home Networking).....	65

Wireless Filter and Options Configuration.....	67
UPnP (Universal Plug and Play)	69
About UPnP	70
Security	72
Firewall	73
Security Level.....	73
Attack Detection	74
IP Filtering	76
DMZ	77
Snooze Control	79
Administrator Password	80
Address Translation.....	80
Gateway Health	82
Statistics.....	83
Internet Stats	83
Home Networking Stats	84
Security Stats	84
Logging.....	85
Update Firmware	85
Diagnostics	86
Customize	87
Color Palette	88
Language	89
Time Zone	89
Reboot / Reset.....	90
Reboot	90
Reset	91
APPENDIX A TROUBLESHOOTING	92
Overview	92
General Issues	92
Internet Access	92
Contacting Technical Support.....	93
APPENDIX B SPECIFICATIONS	94

© 2003 Efficient Networks, Inc., A Siemens Company. All rights reserved. Efficient Networks, its logos and SpeedStream are registered and unregistered trademarks of Efficient Networks, Inc. All other trademarks are held by their respective companies. Efficient Networks reserves the right to make changes to product specifications at any time without notice.

All trademarks and trade names are the properties of their respective owners.

Chapter 1

Introduction



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

Congratulations on the purchase of your new SpeedStream SS6000 Series Wireless DSL Gateway (“Gateway”). The Gateway is a multi-function device providing the following services:

- *Built-in DSL Modem* provides shared Internet access for multiple users.
- *Five-port 10/100 Ethernet Switch* for 10Base-T or 100Base-T connections.
- *Custom Controls* that allow you to configure the SpeedStream DSL Gateway to best meet your specific security and Internet-sharing needs.
- *802.11 Wireless Expansion Slot* (Model 6200) that allows you to add a wireless interface. Your unit may include a wireless card. If it does not, contact your Internet Service Provider for details and availability of expansion cards.
- *Built-in Wireless Interface* (Model 6300) that provides a wireless interface built into the unit. (If you attempt to access or alter the unit components, any warranties may be voided.)

Features of the Wireless DSL Gateway

The SpeedStream SS6000 Series Gateways incorporate many advanced features, carefully designed to provide sophisticated functions while being easy to use.

Network (LAN) Features

1. **Five-Port 10/100 Ethernet Switch**

The SpeedStream Gateway incorporates a five-port 10/100 Ethernet switch, making it easy to create or extend your network. Optionally, you can configure the fifth port as a WAN port for connection of another broadband device.

2. **DHCP Server Support**

Dynamic Host Configuration Protocol (DHCP) provides a dynamic, “upon request,” IP address to computers and other networked devices. Your SpeedStream Gateway can act as a **DHCP Server** for devices on your local network.

3. **Network Status and Statistics**

Using these diagnostic tools, you can easily monitor the status of each network connection and evaluate network performance.

Security Features

24. Password-protected Configuration

Password protection is provided to prevent unauthorized users from modifying the Gateway's configuration data and settings.

25. NAT Protection

An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all your network users to share a single IP address, the location and even the existence of each computer is hidden. From the external viewpoint, there is no network, only a single device - the SpeedStream DSL Gateway.

26. 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.

27. DoS Attack Protection

DoS (Denial of Service) 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 DSL Gateway incorporates protection against DoS attacks as well as other common hacker attacks.

Configuration & Management

- **Easy Setup**

Use your Web browser for quick and easy configuration.

- **UPnP Support**

Universal Plug and Play (UPnP) allows automatic discovery and configuration of the SpeedStream Gateway. UPnP is supported by Windows Me, XP, or later operating systems.

Advanced Gateway Functions

- **DMZ**

One computer on your local network can be configured to allow unrestricted two-way communication with servers or individual users on the Internet. This provides the ability to run programs that are incompatible with firewalls.

- **Firewall "Snooze"**

Temporarily disable firewall protection to limit interference with games and other applications incompatible with firewalls.

- **Content Filter**

Use the Content Filter to block user access to undesirable Web sites.

- **Time of Day Use Restrictions**

Limit the time of day during which individual users have access to the Internet.

- **Advanced Wireless Controls**

The SpeedStream 6300 model has a built-in wireless interface, and the 6200 model offers an

optional wireless expansion card. Custom configuration options include wireless access control, 128-bit wireless encryption, disable SSID broadcast, and pass phrase key generation for added security.

Minimum System Requirements

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

- **Ethernet connection method:**
 - A network interface card (NIC) that supports 10/100 Ethernet
 - Operating system that supports TCP/IP
 - Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later
- **USB connection method:**
 - Available built-in USB port
 - Microsoft Internet Explorer or Netscape Navigator versions 5.0 or later

USB Driver-Related Requirements

Additional USB driver-related requirements depend on the operating system and architecture:

- **Windows operating system:**
 - Pentium-compatible 166 MHz (or faster) processor
 - 32 MB RAM
 - 12 MB available hard drive space
 - Windows 98 or later operating system
- **Macintosh operating system version 8.6 to 9.x:**
 - 100MHz PowerPC or better
 - 32 MB RAM
 - 10 MB available hard disk space
- **Macintosh operating system X:**
 - 300MHz PowerPC G3 or better
 - 128 MB RAM
 - 110 MB available hard disk space (large space requirement due to the Macintosh OS X needing up to 100 MB of additional disk space for system organization after install)

Package Contents

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

- Model SS6000 Series SpeedStream Wireless DSL Gateway

- Power adapter
- CAT-5 Ethernet cable for LAN connections
- RJ11 cable for DSL connection
- USB cable for optional USB installation
- Quick Start Guide
- CD-ROM containing USB driver software and user documentation

Physical Details

Before installing, we recommend that you take a moment to familiarize yourself with the SpeedStream Gateway by referring to the illustrations below.

LEDs



Figure 1. Front Panel

The front panel contains the following LEDs:

Power	<p>Green Power is on.</p> <p>Off Power is off.</p> <p>Red The Power LED briefly shows red during power-up. This indicates that the SpeedStream is conducting the POST (Power-On Self Test) that is run each time the SpeedStream is powered on. During normal operations, the LED will show green.</p>
Ethernet Ports 1 - 5	<p>Each Ethernet LAN port on the back of the router has two corresponding LEDs: Link and Activity.</p> <ul style="list-style-type: none"> • Link <ul style="list-style-type: none"> - On Corresponding LAN port is active. - Off No active connection on the corresponding LAN port. • Activity <ul style="list-style-type: none"> - Off No data being transmitted or received via the corresponding LAN port. - Flashing Data is being transmitted or received via the corresponding LAN port.

DSL Port	<p>For the DSL connection, there are 2 LEDs:</p> <ul style="list-style-type: none"> • Link <ul style="list-style-type: none"> - On DSL connection is active. - Off No active DSL connection. • Activity <ul style="list-style-type: none"> - Off No data being transmitted or received via the DSL connection. - Flashing Data is being transmitted or received via the DSL connection.
USB	<p>For the USB port, there are 2 LEDs:</p> <ul style="list-style-type: none"> • Link <ul style="list-style-type: none"> - On USB connection to computer is active. - Off No active USB connection to computer. • Activity <ul style="list-style-type: none"> - Off No data being transmitted or received via the USB port. - Flashing Data is being transmitted or received via the USB port.
802.11	<p>For the 802.11 wireless connection, there are 2 LEDs:</p> <ul style="list-style-type: none"> • Link <ul style="list-style-type: none"> - On Wireless connection is active. - Off No active wireless connection detected. • Activity <ul style="list-style-type: none"> - Off No data being transmitted or received via the wireless connection. - Flashing Data is being transmitted or received via the wireless connection.
Status	Reserved for future functionality

Rear Panel

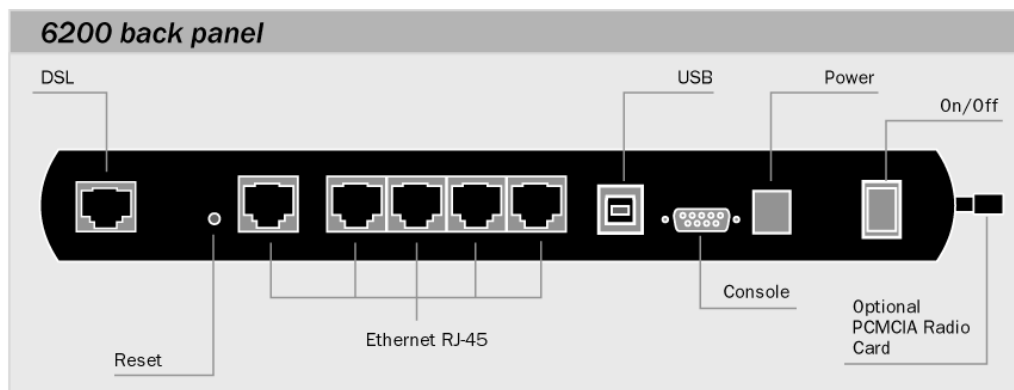


Figure 2: Model 6200 Rear Panel

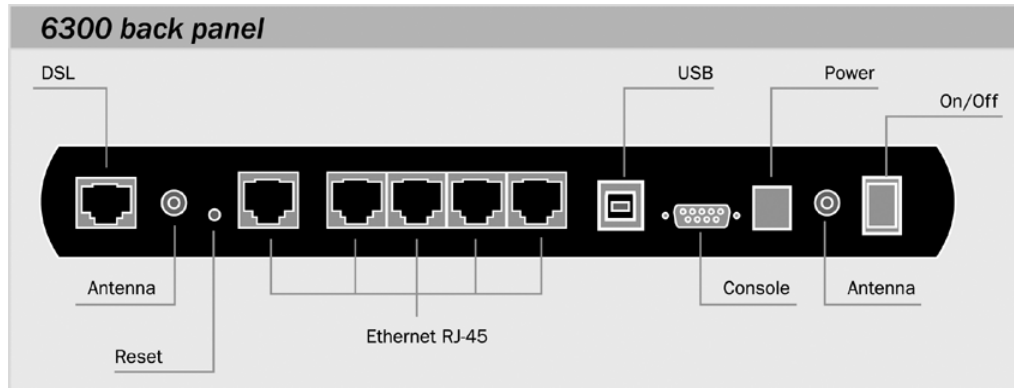


Figure 3: Model 6300 Rear Panel

DSL Port (RJ11)

Connect the RJ11 DSL cable (looks like a telephone cord) here to use your DSL connection through an existing phone line.

Reset Button

This button can be used to clear all data and restore all settings to the factory default values. Note:

To clear all data and restore the factory default values:

7. Power off the Gateway.
8. Hold the **Reset** button down for 5-10 seconds.
9. Continue holding the **Reset** button until the **Power** LED blinks alternating red and green.
10. Release the **Reset** button.

The factory default configuration has now been restored, and the SpeedStream Gateway is ready for use.

10/100 Ethernet Ports 1 - 5

Use standard CAT5 Ethernet cables (with RJ45 connectors) to connect your computers, hubs, or switches to the DSL Gateway. Both 10Mbps and 100Mbps connections are supported.

Note: You can configure port #5 for use as either a fifth switched network port or as a WAN port for connection to another broadband WAN device.

USB Port

Use the USB cable provided with the SpeedStream Gateway to connect the USB port on the SpeedStream Gateway to an open USB port on your computer. When using the USB connection method, the USB driver software must be installed from the provided CD-ROM.

Console Port

For use by service provider technician.

Power Adapter Port

Connect the supplied power adapter here. Use only the power adapter supplied.

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

Wireless Expansion Card Slot (Model 6200) Consult your Internet Service Provider for 802.11 wireless card options and availability.

Use only the wireless card recommended by your Service Provider. Attempting to use any other wireless card may damage the Gateway and will void your manufacturer's warranty.

General Safety Guidelines

When using the SpeedStream Gateway, 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; otherwise, you risk dangerous overloading of the power circuit.

Chapter 2

Installation



This chapter covers the physical installation of the SpeedStream Wireless DSL Gateway.

Minimum System Requirements

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

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

- For wireless access (Model 6200), you must have a wireless card. If one did not come with your SpeedStream Gateway, contact your Internet Service Provider for options and availability.

Hardware Installation

You may position the SpeedStream Gateway at any convenient location in your office or home. No special wiring or cooling requirements are needed; however, you should comply with the safety guidelines specified in the [General Safety Guidelines](#) on page 7.

Basic Installation Procedure

1. If applicable, install the wireless expansion card.
2. Install line filters if necessary.
3. Connect the cables.
4. Plug the Gateway into the electrical outlet, power on the Gateway, and verify port status.
5. Install USB drivers if necessary.
6. Configure network settings on your computer.
7. Configure the Gateway via the Web-based management interface.
8. Reboot the computer if prompted.

Note Whenever you are required to reboot the Gateway, allow five seconds between turning off the unit and powering it back on.

Wireless Card Installation (Model 6200)

If your SpeedStream Gateway came with a wireless expansion card, install this card in the PCMCIA expansion slot on the side of the Gateway before proceeding further with the installation.

1. Remove the wireless card from the anti-static bag.
2. Remove the protective cover from the PCMCIA expansion slot on the side of the Gateway.
3. Insert the expansion card in the slot with the colored label facing up.
4. Ensure that the card is inserted fully and seated securely.
5. After powering on the Gateway, verify that the 802.11 Link LED is lit.

Installing Line Filters

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

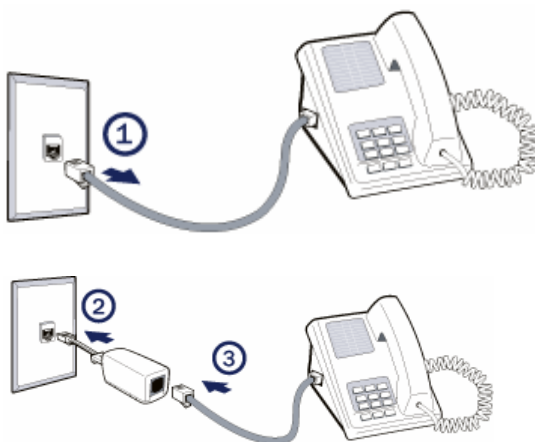
Because DSL shares your telephone line, you may need to separate the two signals so they do not interfere with each other. A line filter (may be included with some models) prevents DSL traffic from disrupting the voice signal on the telephone line, and vice versa. Follow the procedures below to install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

You will need one of these type filters to connect between the telephone and the wall plate:

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

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

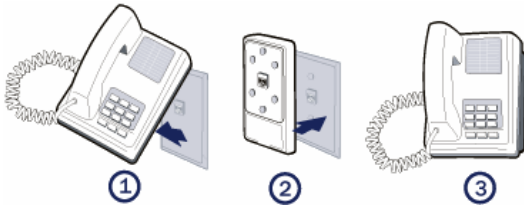
Important! DSL performance may be significantly degraded if the line filters are not installed in the correct direction, as illustrated below.



In-Line Filter

For each device sharing the same telephone line:

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



Wall-Mount Filter

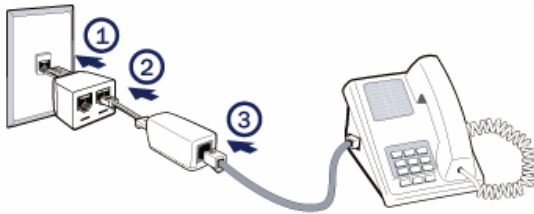
For a wall-mounted telephone, install a wall mount filter:

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

Two-to-One Adapter

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

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



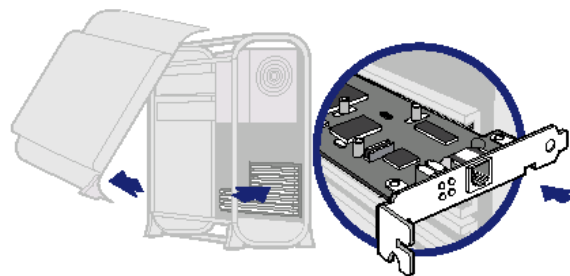
Installation Methods

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

Ethernet Installation Method

To connect the SpeedStream Gateway 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, you will need to install it before proceeding further. Refer to your Ethernet adapter documentation for complete installation instructions.



Note: For wireless connectivity, your SpeedStream Gateway may require an optional wireless interface card. If your Gateway did not come with this card, contact your Internet Service Provider for options and accessibility.

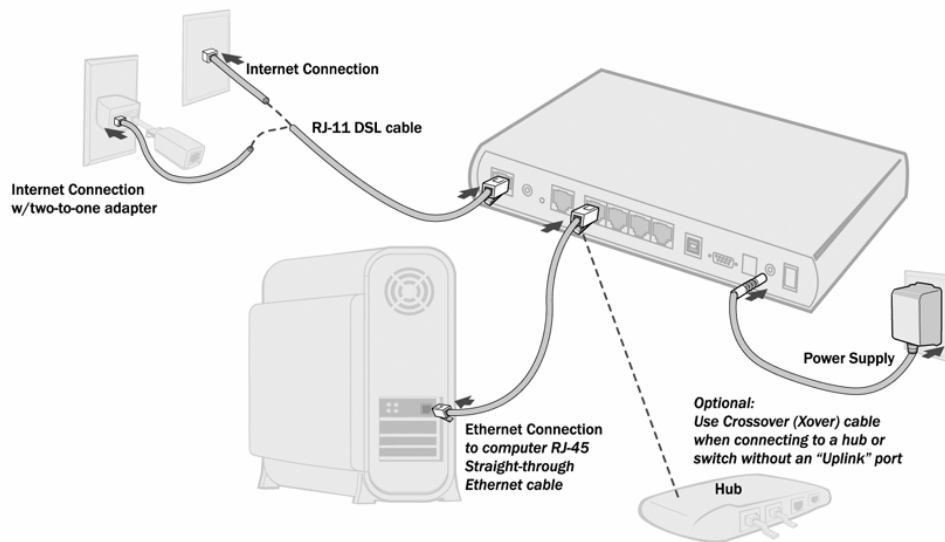


Figure 4: (Model 6200) Ethernet Connection Installation

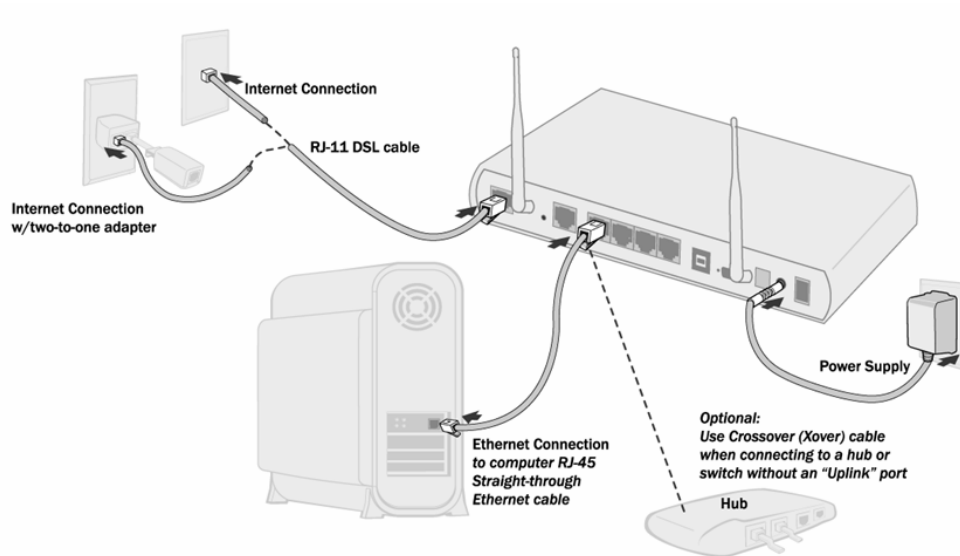


Figure 5: (Model 6300) Ethernet Connection Installation

1. Connect the Ethernet cable(s):

- 1) With your computer powered off, connect the Ethernet cable to an Ethernet port (1-5) on the SpeedStream Gateway.
- 2) Connect the other end of the Ethernet cable to the Ethernet port on your computer.
- 3) If desired, use standard 10/100 CAT5 Ethernet cables to connect additional computers to the remaining Ethernet ports on the rear of the SpeedStream Gateway.

2. Connect the DSL cable:

- 1) Connect the DSL cable (resembles a telephone cord) to the DSL port on the rear of the SpeedStream Gateway.
- 2) Plug the other end of the DSL cable into the phone jack.

3. Connect the power:

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

4. Check the LEDs:

- 1) For each active Ethernet connection, the LAN Link LED for the corresponding port number should be lit.
- 2) The DSL and Power LEDs should be lit. (For more information, refer to *LEDs* in *Chapter 1*.)

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

You can now configure the TCP/IP settings as detailed in *Chapter 3, SpeedStream Gateway Setup*.

USB Installation Method (Microsoft Windows)

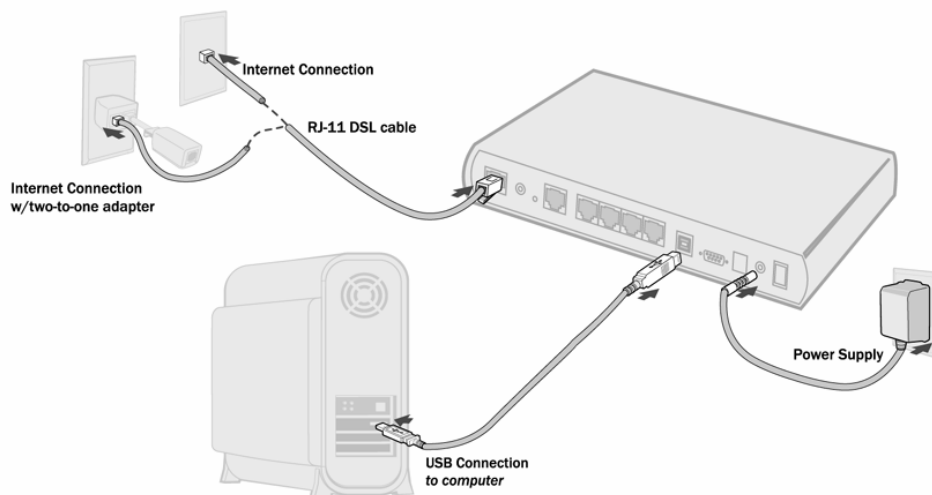


Figure 6: USB Connection Installation Diagram

1. Connect the USB Cable

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

2. Connect the DSL Cable

- 1) Connect the DSL cable (resembles a telephone cord) to the DSL port on the rear of the Gateway.
- 2) Plug the other end of the DSL cable into the phone jack.

3. Connect the Power

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

4. Install USB Driver Software

- 1) Insert the SpeedStream Gateway driver CD-ROM into the CD-ROM drive of your computer.
- 2) When prompted, follow the on-screen instructions to complete the driver installation.
- 3) No driver software is required for computers connected to the Gateway using Ethernet cables.

5. Check the LEDs

- The DSL, USB, and Power LEDs should be lit. (For more information, refer to *LEDs* in *Chapter 1, Introduction*.)

USB Driver Installation (Macintosh Systems)

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

- **Macintosh Classic (versions 8.6, 9.x)**

1. To “unstuff” the installer to the **EFNTClassic110** directory, run **EFNTClasic110.sit**
2. In the **English** directory, run the **SpeedStream 5x OS9 Installer-en**
- or -
In the **French** directory, run the **SpeedStream 5x OS9 Installer-f2**

- **Macintosh OS X (versions 10.1.x, 10.2.x)**

1. To “unstuff” the installer to the **EFNTOSX110** directory, run **EFNTOSX110.sit**
2. In the **EFNT0SX110** directory, run the **SpeedStream 5x Installer**

Chapter 3

Operating System Configuration

This chapter details the configuration required for each computer on your network.

Overview

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

Windows Configuration

This section describes how to configure computers to share Internet access through the SpeedStream Gateway:

The first step is to check each computer's TCP/IP protocol settings. Because the Gateway uses the TCP/IP network protocol for all functions, it is essential that the TCP/IP protocol be installed and configured properly on each computer.

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

By default, the Gateway 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.

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

1. Select **Control Panel >Network**. The system responds with the “Network” window.

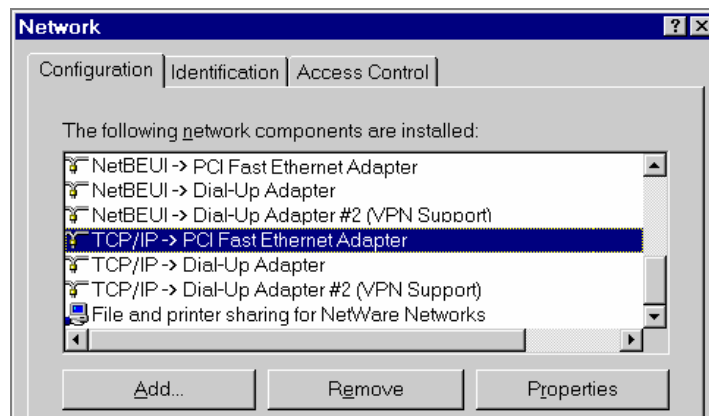


Figure 7: Network Configuration

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

3. Click **Properties**. The system responds with the “TCP/IP Properties” window.
4. Ensure that the **Obtain an IP address automatically** option is selected. This is the default Windows settings.

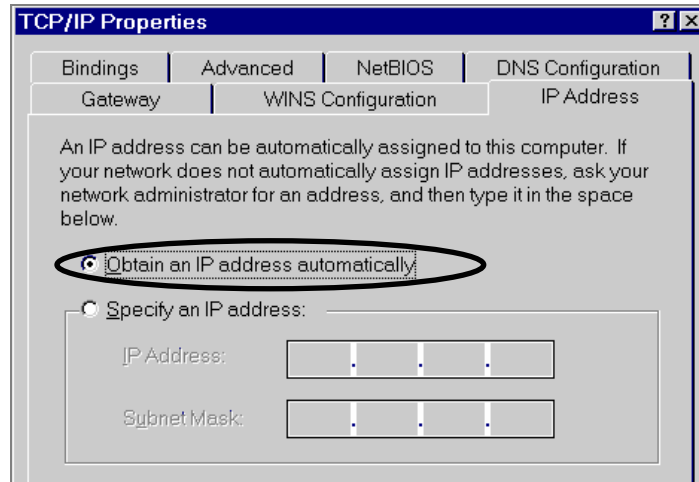


Figure 8: IP Address (Win 9x)

5. Restart your computer to ensure it obtains an IP address from the Gateway.

Checking TCP/IP Settings (Windows 2000)

1. On the Windows taskbar click **Start>Control Panel**. The system responds with the “Control Panel” window.
2. Double-click **Network and Dial-up Connections**. The system responds with the “Network and Dial-up Connections” window.
3. Right-click **Local Area Connection** and select **Properties**. The system responds with the “Local Area Connections Properties” window.
4. Select the TCP/IP protocol for your network card.

- Click **Properties**. The system responds with the “Internet Protocol (TCP/IP) Properties” window.

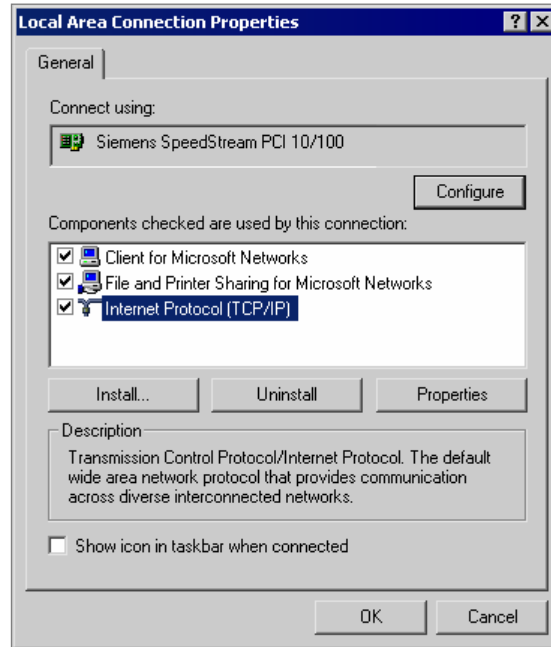


Figure 9: Network Configuration (Win 2000)

- Select the “Obtain an IP address automatically” option.

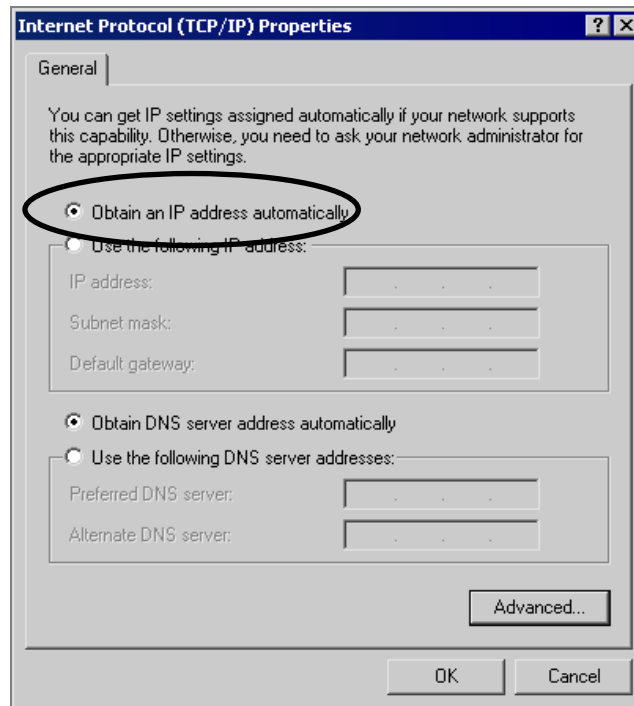


Figure 10: TCP/IP Properties Window (Win 2000)

- Restart your computer to ensure it obtains an IP address from the Gateway.

Checking TCP/IP Settings (Windows XP)

1. On the Windows taskbar click **Start>Control Panel >Network Connection**.
2. Right-click **Local Area Connection**; then click **Properties**. The system responds with the “Local Area Connection Properties” window.

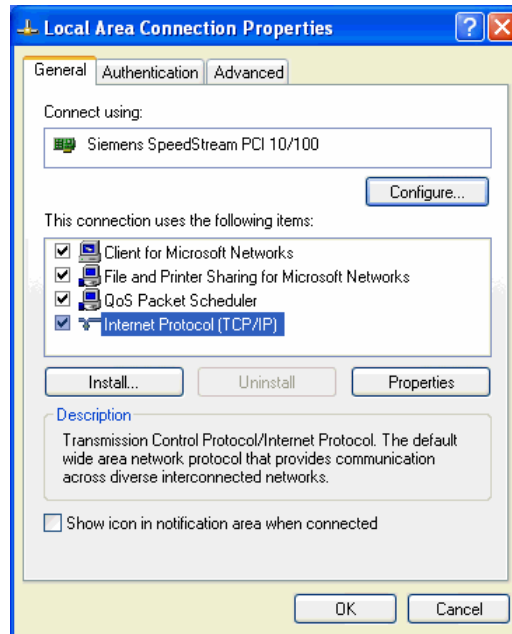
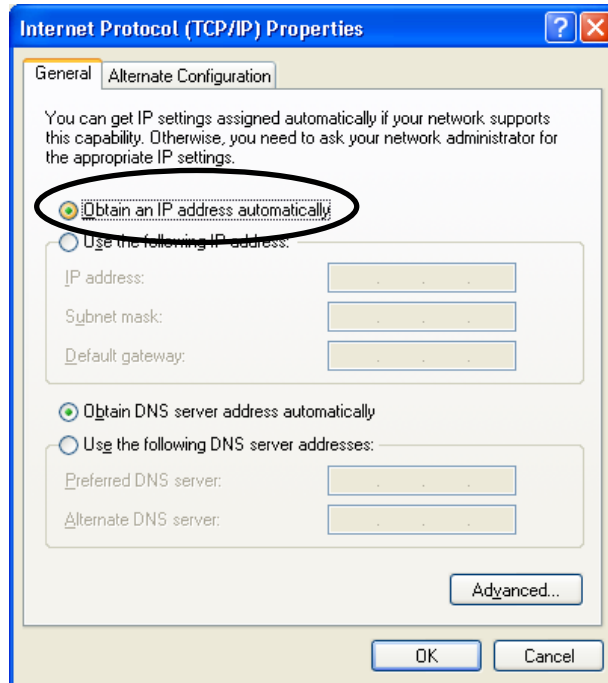


Figure 11: Network Configuration (Windows XP)

3. Select the TCP/IP protocol for your network card.
4. Click **Properties**. The system responds with the “Internet Protocol (TCP/IP) Properties” window.
5. Ensure that the radio button **Obtain an IP address automatically** is selected.

- Restart your computer to ensure it obtains an IP address from the Gateway.



Properties (Windows XP)

Figure 12: TCP/IP

Internet Access

To configure your computers to use the Gateway for Internet access, ensure that the Gateway is installed correctly and the DSL line is functional. Then follow the 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

- Select **Start Menu >Settings > Control Panel > Internet Options**.
- Select the **Connection** tab, and click **Setup**.
- Select **I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)** option. Click **Next**. The system responds with the “Setting up your Internet Connection” window.
- Select **I connect through a local area network (LAN)** option and click **Next**. The system responds with the “Local Area Network Internet Configuration” window.
- Ensure all of the boxes are **deselected** and click **Next**. The system responds with the “Set Up your Internet Mail Account” window.
- Select the “No” option and click **Next**. The system responds with the “Completing the Internet Connection Wizard” window.
- Click **Finish** to close the Internet Connection Wizard. Setup is now complete.

For Windows XP

1. Select **Start Menu - Control Panel - Network and Internet Connections**.
2. Select **Set up or change your Internet Connection**.
3. Select the **Connection** tab, and click **Setup**.
4. Cancel the pop-up **Location Information** screen.
5. Click **Next** on the **New Connection Wizard** screen.
6. Select **Connect to the Internet** and click **Next**.
7. Select **Set up my connection manually** and click **Next**.
8. Check **Connect using a broadband connection that is always on** and click **Next**.
9. Click **Finish** to close the New Connection Wizard. Setup is now complete.

Macintosh Configuration

This section describes how to configure computers running Macintosh operating system versions 8.6 through 10.2 to share Internet access through the SpeedStream Gateway:

The first step is to check each computer's TCP/IP protocol settings. Because the Gateway uses the TCP/IP network protocol for all functions, it is essential that the TCP/IP protocol be installed and configured properly on each computer.

By default, the Gateway will act as a DHCP server, automatically providing a suitable IP address and related information to each computer when the computer boots up.

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

1. Select **Apple Menu - Control Panel - TCP/IP**.
2. Open the TCP/IP control panel. You should see a screen like the following:

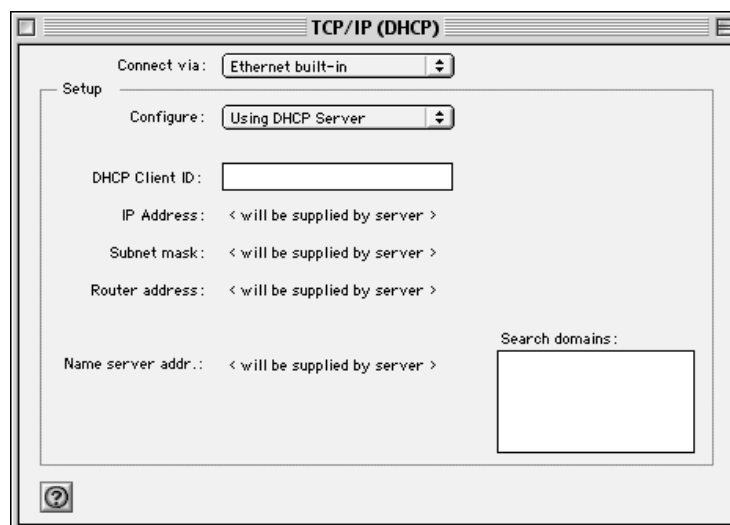


Figure 13: TCP/IP Control Panel (Mac OS 8.6-9.x)

3. Set the following values:
 - Connect via: Ethernet Built-in
 - Configure: Using DHCP Server
 - Leave the remaining fields blank
4. Close the TCP/IP Control Panel and click **Save**.
5. Reboot when configuration is saved. Once rebooted, the computer will pull an IP address from the DHCP server on the Gateway.

Checking TCP/IP Settings (MAC OS X)

1. Select **Apple Menu – System Preferences – Network**.
2. Select the **TCP/IP** tab. You should see a screen like the following:

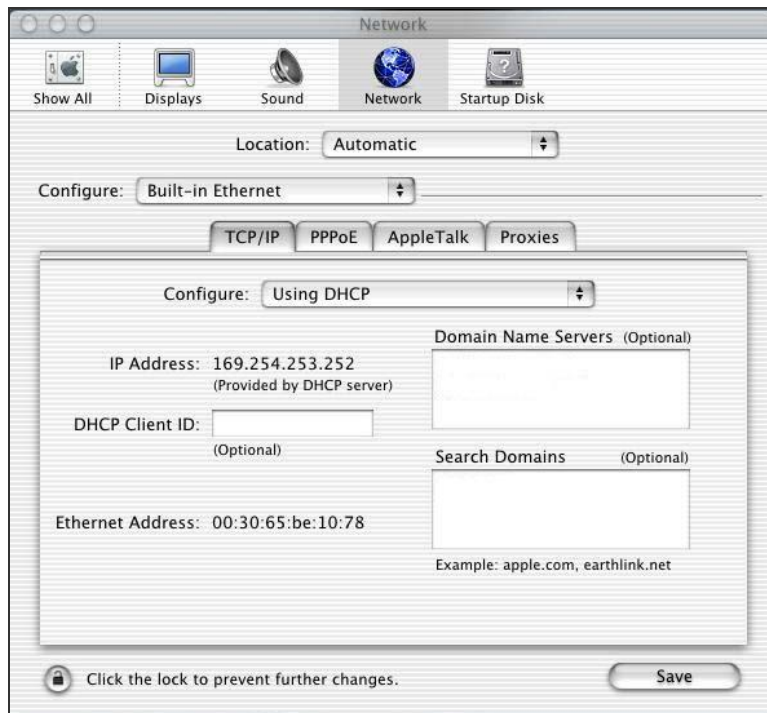


Figure 14: TCP/IP Control Panel (Mac OS X)

3. Set **Configure TCP/IP** to **Using DHCP**, leave the optional fields blank. Click **Save**.
4. Reboot to save the configuration. Once rebooted, the computer will pull an IP address from the DHCP server on the Gateway.

Chapter 4

4

SpeedStream Gateway Setup

This chapter provides details of the setup processes.

Overview

This chapter describes the basic setup procedures for configuring your computer and establishing Internet access.

Some computers on your network may require additional configuration to share an Internet connection through the Gateway. For more information, please see the section in this document titled [Chapter 3. Operating System Configuration](#).

Other configuration may also be required, depending on which features and functions of the SpeedStream Gateway you wish to use. Use the table below to locate detailed instructions for the required functions.

To do this:	Refer to:
Check settings or configure computers on your network.	<i>Chapter 3. Operating System Configuration</i>
Use any of the following advanced features: <ul style="list-style-type: none">• User Profiles• Content Filtering• Server Ports• Wireless Configuration (Optional)• Security and Firewall settings• Dynamic DNS• DMZ	<i>Chapter 5. Gateway Configuration Options</i>

Configuration Program

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

Preparation

Before attempting to configure the Gateway, please ensure that:

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

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

Connecting to the Gateway

Using UPnP (Windows XP and Me)

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

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

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

Using your Web Browser

To establish a connection from your computer to the Gateway:

1. After installing the Gateway, start your computer. If your computer is already running, reboot it.
2. Open your Internet Explorer or Netscape Navigator Web browser.
3. In the **Address** bar, type <http://speedstream> and press the **ENTER** key. The system responds with the "Setup" window.
4. Please see the section below titled "Setup Wizard" for more information on setting up the Gateway.

Setup Wizard

The first time you connect to the Gateway via Web browser, the Setup Wizard runs automatically. (The Setup Wizard also runs if the Gateway's default settings are restored.) Proceed through the entire Setup wizard to ensure accuracy of the installation. **Note:** You will need to know the username and password for Internet service provided by your ISP. Check the information supplied by your ISP for details.

Gateway Setup Wizard

1. The first screen of the Setup Wizard is the **Welcome** window. Click **Next**. The system responds with the “Gateway Administrator Setup” window.
2. An administrator account is necessary to allow access to the person who is to make Gateway changes. **Optionally**, change the “admin” user name to a different administrative name by typing the new administrative name in the “User Name” box. If you wish, simply leave the “admin” user name in the “User Name” box. Type a password in the “New Password” box.
3. Re-type the password in the “Confirm Password” box and click **Next**.

Efficient NETWORKS

Welcome to the SpeedStream DSL Gateway

HELP

SETUP

- 1 Gateway Password
- 2 Time Zone
- 3 Wireless Setup
- 4 Finish

Gateway Administrator Setup

Your Gateway requires someone to be the **Gateway Administrator**. This person has responsibility for adding user profiles, setting each person's access rights, and configuring the Gateway.

Please create a user name and password for the Gateway administrator.

REMEMBER THIS INFORMATION!!! This will be needed for future access and configuration of the Gateway.

User Name: (required)

New Password: (required)

Confirm Password: (required)

Next >>

Figure 15: Gateway Administrator Setup Window

- The “Configure Time Zone” window allows you to set the time zone of the area of the world in which you live. Select the “Yes” option from under the “Enable Time Client” heading.
- Select your time zone from the “Select Time Zone” drop-down and click **Next**.

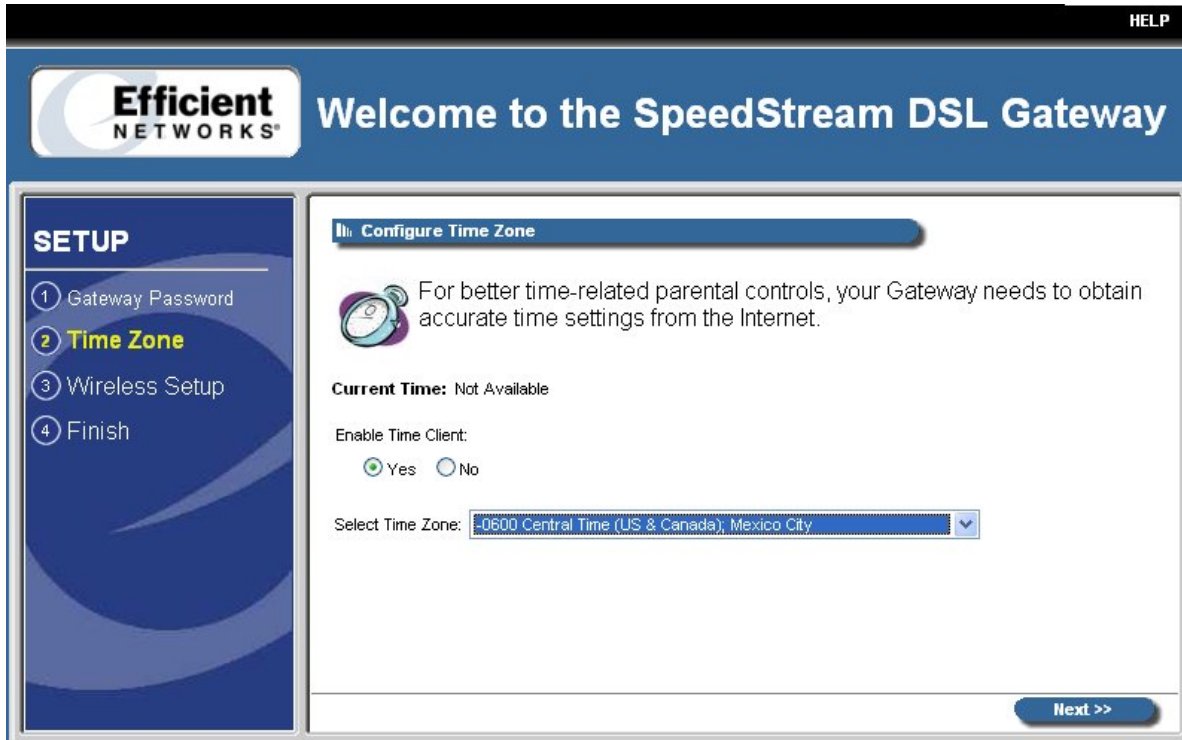


Figure 16. Setup Wizard Time Zone Window

- The Wireless Setup Configuration window allows you to set up wireless clients on your gateway. Select the “Enable” option under the “Wireless Interface” heading to setup the wireless part of the Gateway. Select the “Disable” option if you do not wish to setup the wireless portion of the Gateway. **Note:** If you select the “Disable” option and click **Next**, the system responds with the “Finish” window.
- Type your wireless network ID in the “SSID” (Service Set Identifier) box. This value is the name of your network.
- Optionally**, select a channel from the “Channel” drop-down. The channel is a path of communication that is used across your network. **Note:** Depending on your area and gateway configuration, the channel may default to only one value.

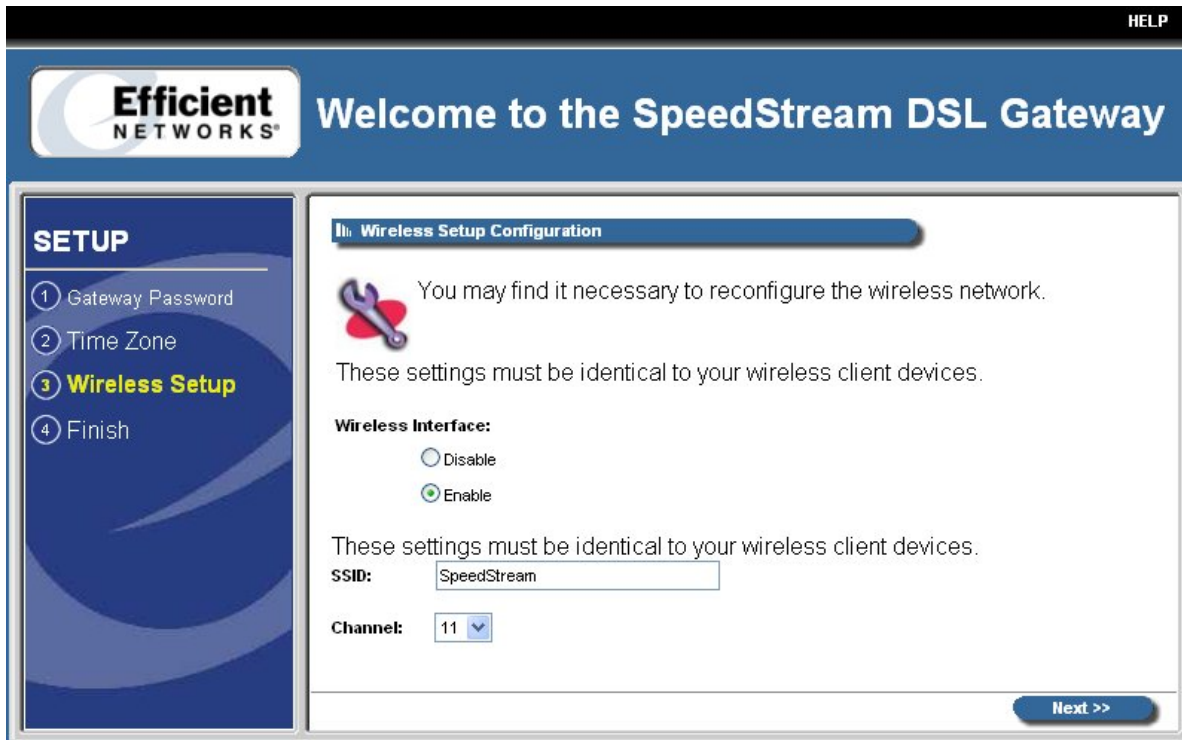
9. Click **Next**.

Figure 17. Wireless Setup Configuration Window

10. The “Wireless Security Configuration” window allows you to set the wireless security level you wish to use. All wireless devices attached to the gateway **MUST** have the same wireless security settings for your network to have proper communications and security. If you own the 6200 series gateway, the “Wireless Security Configuration” window does not appear. From the “Security Mode” drop-down, select one of the following options:

- **WEP 64-bits:** (Wireless Equivalency Privacy): WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled [Wireless Setup WEP 64-Bit Option](#) for more information.
- **WEP 128-bits:** (Wireless Equivalency Privacy): WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled [Wireless Setup WEP 128-Bit Option](#) for more information.
- **WPA PSK:** (Wi-Fi Protected Access) WPA security changes encryption keys after a specified amount of time. This is the **most secure option** for wireless networks. Please see the section in this document titled [Wireless Setup WPA PSK Option](#) for more information.

Wireless Setup WEP 64-Bit Option

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. This section assumes you currently have the “Wireless Security Configuration” window displayed on your computer.

To use the WEP 64-bit option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. Click **Next**.

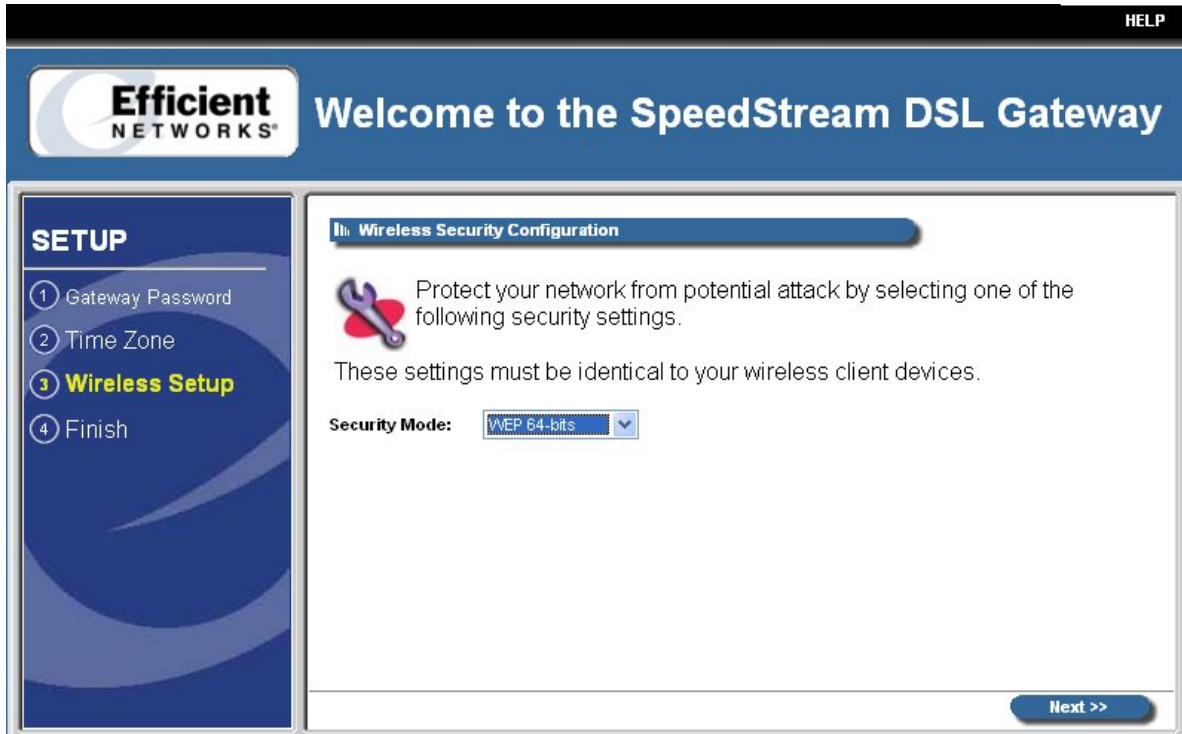


Figure 18. WEP 64-Bit Encryption

3. The “Wireless 64-bit WEP Configuration” window allows you to configure the security for the 64-bit WEP option. Select one of the following options:
 - **Open System:** Open system keys are always authenticated at the device level. After authentication, data is then encrypted between the gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
 - **Shared Key:** Shared keys accept a string of unencrypted data from a device. The gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in the “Passphrase” box. The passphrase is used to generate the 64-bit key. The passphrase must at least be one character with a maximum of 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under the “Passphrase” box.

6. Click **Next**.

The screenshot shows the configuration interface for the SpeedStream DSL Gateway. The title bar includes the Efficient Networks logo and the text "Welcome to the SpeedStream DSL Gateway". A "HELP" button is in the top right corner. On the left, a "SETUP" sidebar lists four steps: 1 Gateway Password, 2 Time Zone, 3 Wireless Setup (highlighted in yellow), and 4 Finish. The main content area is titled "Wireless 64-bit WEP Configuration". It features a wrench icon and text explaining that WEP will secure the network by 64-bit (10 hex digit) encryption of all traffic using a static key. A note states: "These settings must be identical to your wireless client devices." Below this, there are radio buttons for "Authentication": "Open System" (selected) and "Shared Key". A "Passphrase:" label is followed by an empty text input field and a "Generate Keys" button. Underneath, there are four radio buttons for "64 Bit Key" selection, each followed by a 5-column grid of hexadecimal characters:

- 64 Bit Key 1:

eb	f3	2f	34	eb
----	----	----	----	----
- 64 Bit Key 2:

9e	70	f0	7a	ea
----	----	----	----	----
- 64 Bit Key 3:

e2	cd	89	11	af
----	----	----	----	----
- 64 Bit Key 4:

de	29	f3	07	25
----	----	----	----	----

A "Next >>" button is located at the bottom right of the configuration area.

Figure 19. Wireless 64-Bit WEP Configuration Window

7. On the “Congratulations” window, click **Finish**. The system responds with the “What do I do now?” window. From this window you may either:
- Click **Surf Now**. Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the Gateway’s configuration interface at anytime should you choose to further configure the Gateway.
 - Click **Continue**. The system responds with the Home window where you can create usage profiles/rules for different users, change the level or type of security used on the Gateway or define/configure your network to be managed by the Gateway. Please see the section in this document titled [Gateway Environment](#).

Wireless Setup WEP 128-Bit Option

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the “Wireless Security Configuration” window displayed on your computer.

To use the WEP 64-bit option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. Click **Next**.

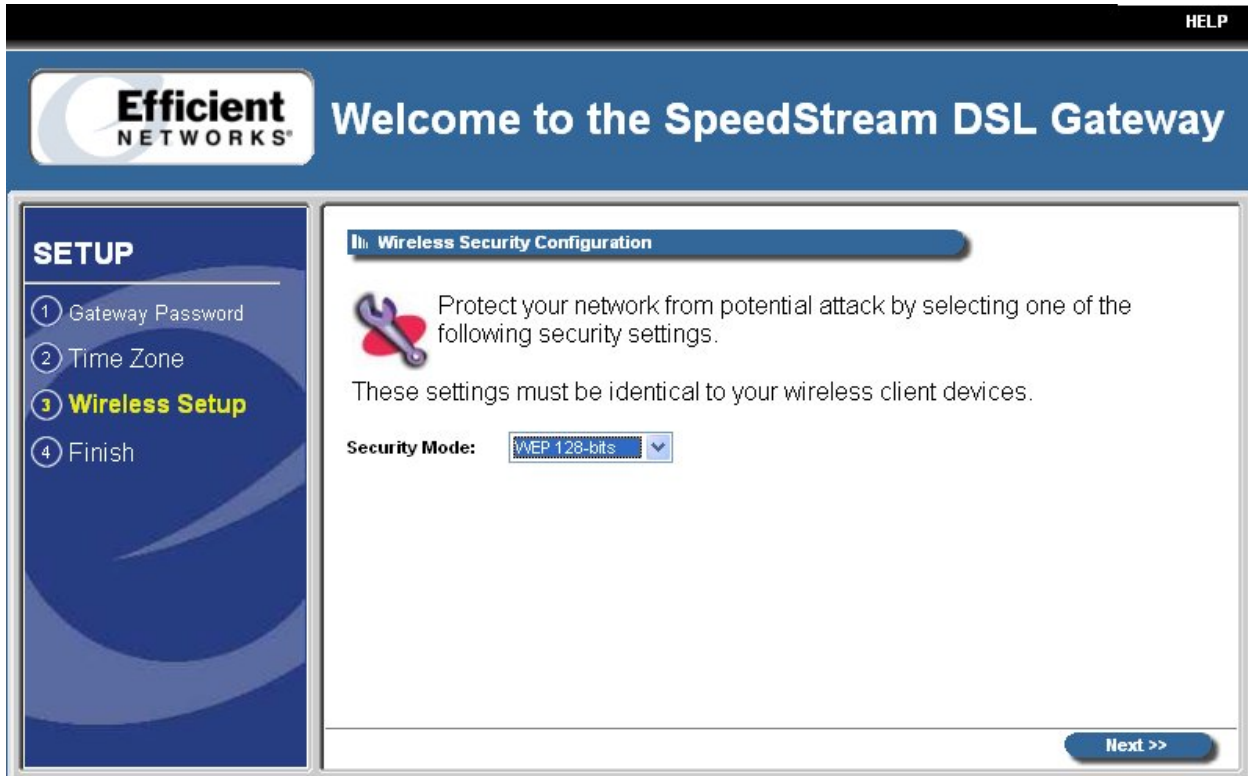
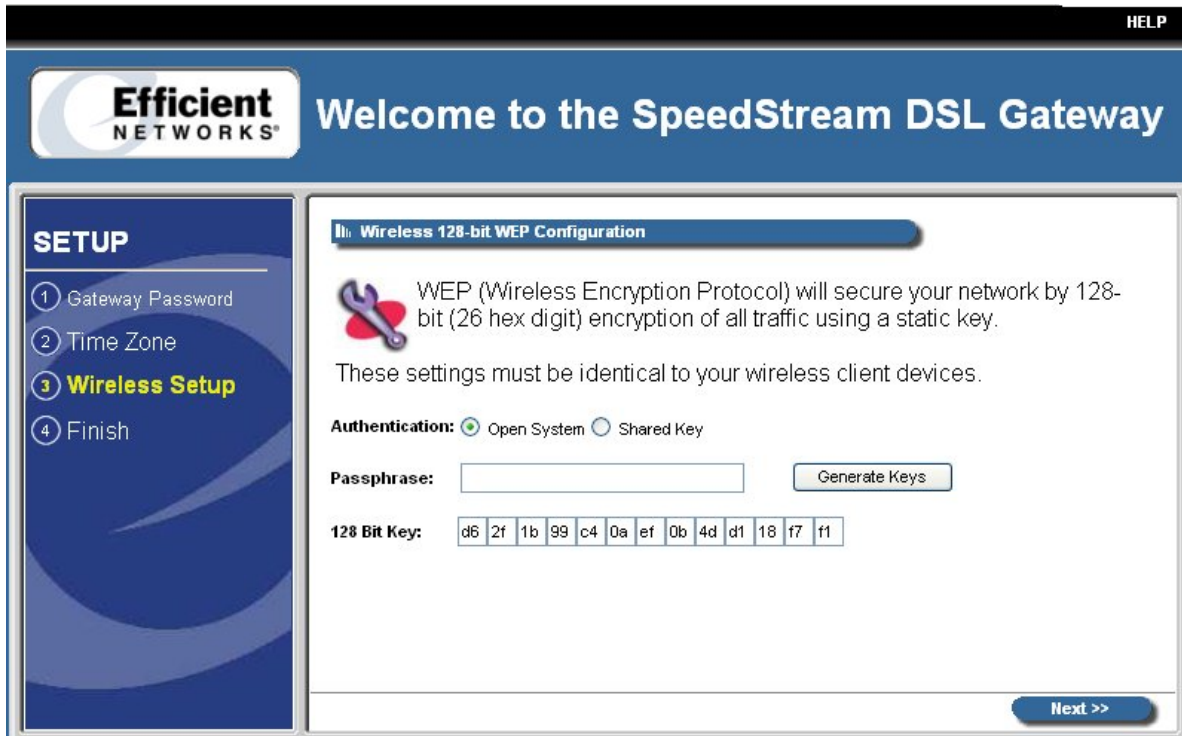


Figure 20. Wireless Security Configuration 128-Bit WEP

3. The “Wireless 128-bit WEP Configuration” window allows you to configure the security for the 128-bit WEP option. Select one of the following options:
 - **Open System:** Open system keys are always authenticated at the device level. After authentication, data is then encrypted between the gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
 - **Shared Key:** Shared keys accept a string of unencrypted data from a device. The gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
4. Type a phrase in the “Passphrase” box. The passphrase is used to generate the 64-bit key. The passphrase must at least be one character with a maximum of 32 characters.
5. Click **Generate Keys**. The system responds by generating keys that display in the boxes under the “Passphrase” box.

6. Click **Next**.



The screenshot shows the configuration interface for the SpeedStream DSL Gateway. At the top, there is a blue header with the Efficient Networks logo and the text "Welcome to the SpeedStream DSL Gateway". A "HELP" link is visible in the top right corner. On the left side, there is a "SETUP" menu with four steps: 1 Gateway Password, 2 Time Zone, 3 Wireless Setup (highlighted in yellow), and 4 Finish. The main content area is titled "Wireless 128-bit WEP Configuration". It contains a red wrench icon and text explaining that WEP will secure the network by 128-bit (26 hex digit) encryption. Below this, it states that these settings must be identical to wireless client devices. There are two radio buttons for "Authentication": "Open System" (selected) and "Shared Key". A "Passphrase:" field is followed by a "Generate Keys" button. Below that, the "128 Bit Key:" is displayed as a sequence of 13 hex digits: d6 2f 1b 99 c4 0a ef 0b 4d d1 18 f7 f1. A "Next >>" button is located at the bottom right of the configuration area.

Figure 21. Wireless 128-Bit WEP Configuration Window

7. On the “Congratulations” window, click **Finish**. The system responds with the “What do I do now?” window. From this window you may either:
- Click **Surf Now**. Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the Gateway’s configuration interface at anytime should you choose to further configure the Gateway.
 - Click **Continue**. The system responds with the Home window where you can create usage profiles/rules for different users, change the level or type of security used on the Gateway or define/configure your network to be managed by the Gateway. Please see the section in this document titled [Gateway Environment](#).

Wireless Setup WPA PSK Option

WPA security changes encryption keys after a specified amount of time. This is the **most secure option** for wireless networks. This section assumes you currently have the “Wireless Security Configuration” window displayed on your computer.

To use the WPA option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. Click **Next**.

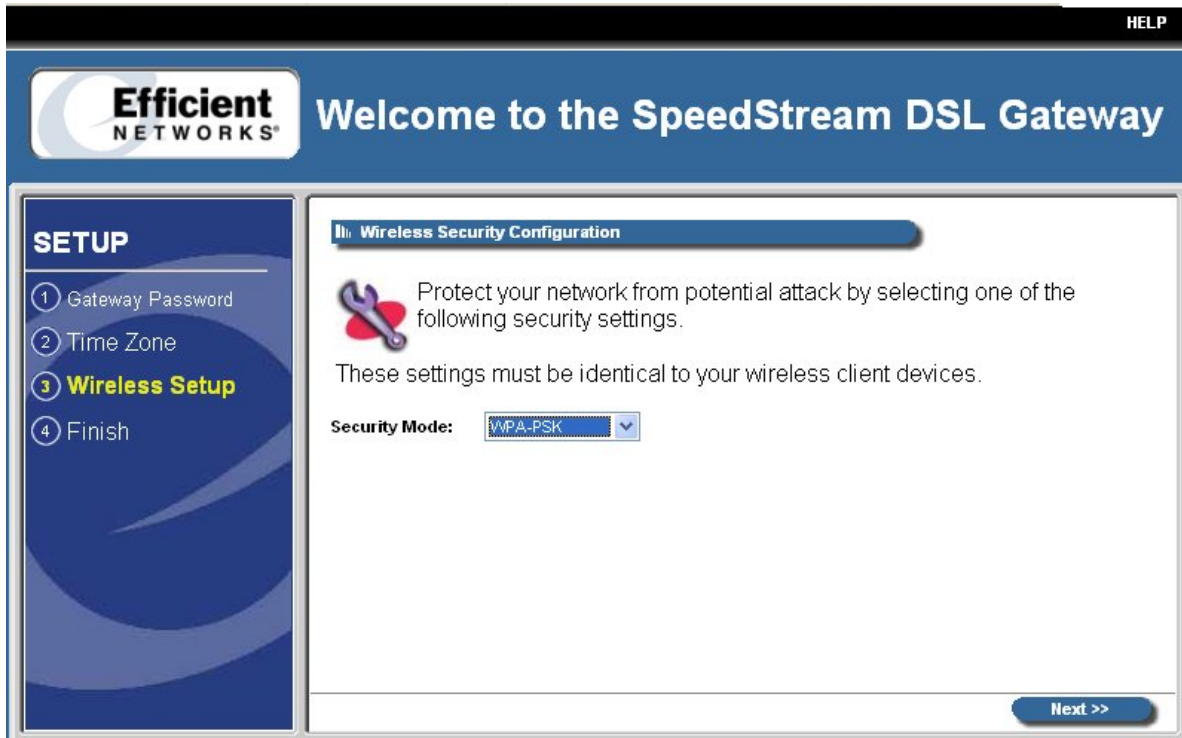


Figure 22. Wireless Security Configuration WPA-PSK

3. The “Wireless WPA Configuration” window is used to configure the algorithm, shared key, and key renewal options. Select one of the following options from the “Algorithms” drop-down:
 - **TKIP:** (Temporal Key Integrity Protocol) TKIP is a more powerful security protocol than WEP and supports: Verification of the security configuration after the encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and the determines a unique starting unicast encryption key for each pre-shared key authentication.
 - **AES:** (Advanced Encryption Standard) AES supports a private key algorithm that ranges from 128 to 256 bits.
4. Type a key in the “Shared Key” box. The shared key is used to generate a dynamic encryption key for gateway security.

5. Type a numeric value (in seconds) of the time lapse in changing the key in the “Group Key Renewal” box and click **Next**. **Note:** The minimum time value is 30.

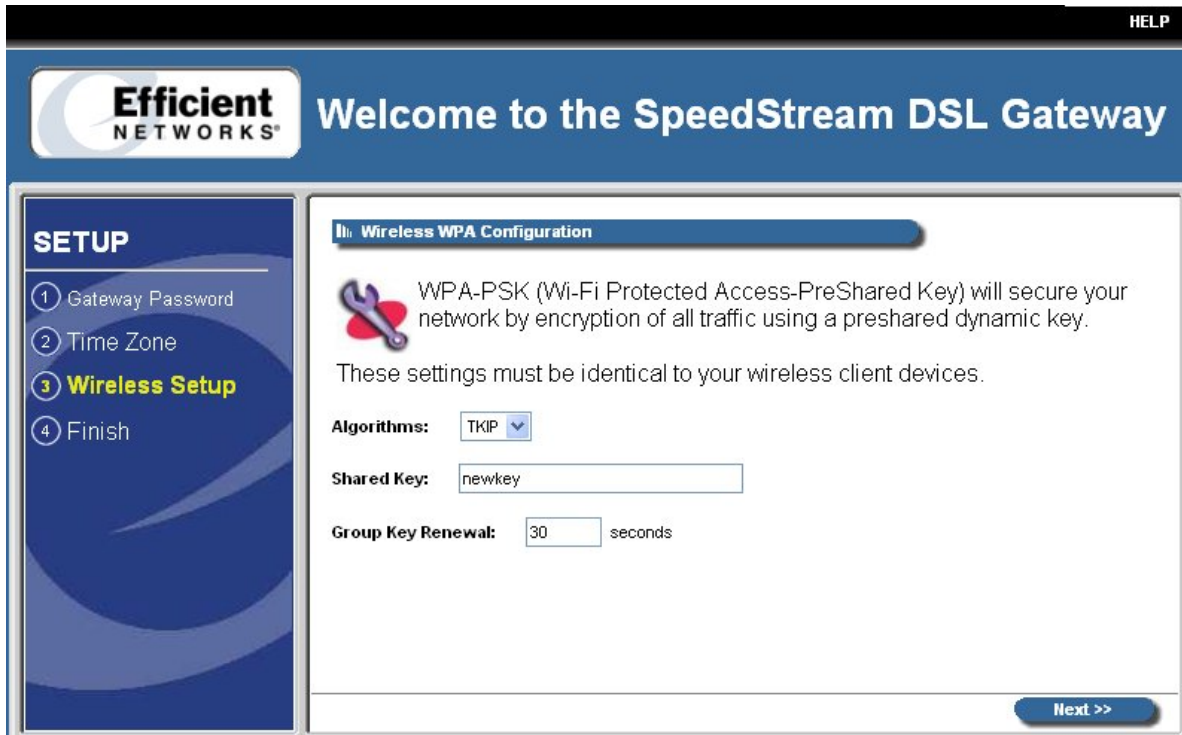


Figure 23. Wireless WPA Configuration Window

6. On the “Congratulations” window, click **Finish**. The system responds with the “What do I do now?” window. From this window you may either:
 - Click **Surf Now**. Your Web browser re-directs you to default home page of the Web browser you are using. You may return to the Gateway’s configuration interface at anytime should you choose to further configure the Gateway.
 - Click **Continue**. The system responds with the Home window where you can create usage profiles/rules for different users, change the level or type of security used on the Gateway or define/configure your network to be managed by the Gateway. . Please see the section in this document titled [Gateway Environment](#).

Gateway Environment

Home Window

After finishing the Setup Wizard and clicking Configure, the Home window appears. When connecting to the Gateway in the future, this screen appears. Pay special attention to the Login box in the top left-hand corner of the screen to ensure that you are logged in to access all available features. All configuration options display for the user defined as Administrator of the Gateway, whereas other users are not given as many options (depending upon the amount of control assigned in their User Profile).

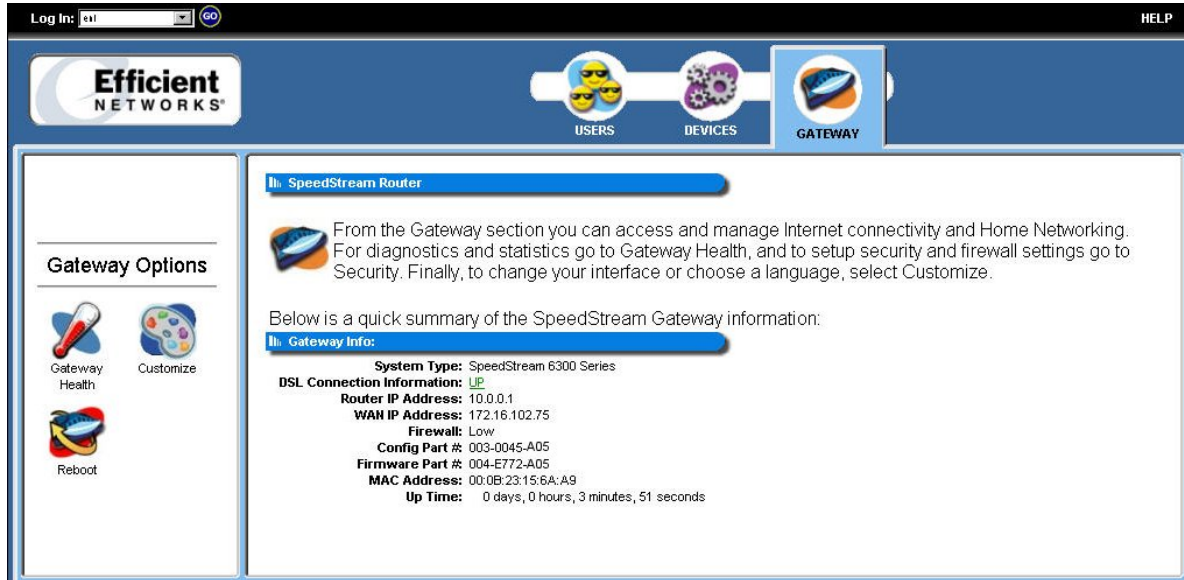





Figure 24: Home Window (Non-Administrative Log on)

Menu Bar

The only two items on the menu bar are the login drop-down and the Help menu option. The "Log In" drop-down is used to login a user or administrator. The Help option is used to display a Help system for the gateway.

Toolbar

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

Button	Function
	Users Button: This button provides access to user profiles and the User Profile Wizard. This wizard guides you through the steps required to set up and configure individual user profiles, allowing you to establish different permissions for different users. User profiles for particular users of the gateway can be viewed as well.
	Devices Button: This button provides access to display all network devices connected to the Gateway and allows you to view details about each of the devices. You can also view shared files and resources on other computers if they are shared via Windows File Sharing. (Consult your Windows systems documentation for more details on enabling file and printer sharing).
	Gateway Button: This button provides access to all Gateway configuration options, security settings, Gateway health monitoring, and Internet connection and network details. The settings available may differ depending upon your service provider.

Logging into the Gateway

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

To logon to the gateway:

1. Select a user from the “login” drop-down in the upper-left corner of the Home window and click **GO**. The system responds with the “Welcome to the SpeedStream Gateway” window. **Note:** If you setup users without passwords, the “Welcome to the SpeedStream Gateway” window does not appear.



Figure 25. Login Box

2. Select a user from the “Username” drop-down.
3. Type the user password in the “Password” box.
4. Click **Log In**. The system responds with the Home window. **Note:** Depending on if you logged in as a user or administrator, determines the modem options in the left-pane of the Home window.

Logging out of the Gateway

To log out of the gateway:

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



Figure 26. Logout

Gateway Options

In the left-pan of the Home window, there are configuration options for the gateway. These options differ depending on how a user is logged into the system. An administrator has full configuration rights, while a user has limited configuration rights. Please see [Chapter 5. Gateway Configuration Options](#) for more information on each option.

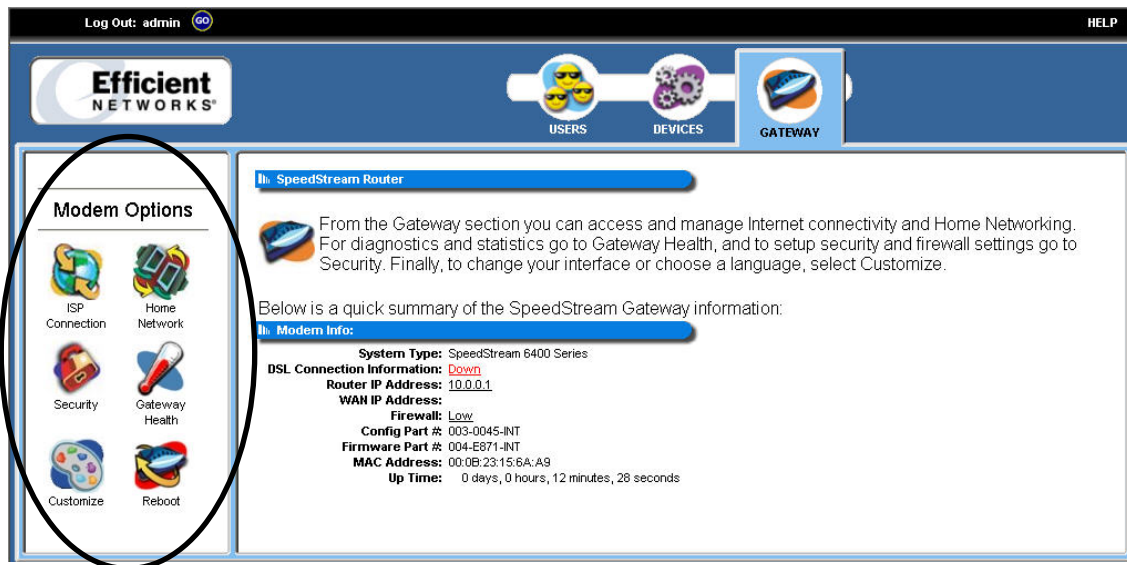


Figure 27. Gateway Options on the Home Window (with administrator log on)

Chapter 5

5

Gateway Configuration Options

This chapter explains when and how to use the Gateway's modem options.

Overview

Many advanced features, status, and diagnostic screens are provided for your convenience. This chapter contains details of the configuration and use of each of these features. This chapter is organized into three parts corresponding to the buttons in the toolbar:

- **Users**
- **Devices**
- **Gateway**

Note: Some of the features described below require at least a mid-level understanding of networking principles. These features are provided to allow configuration flexibility for advanced users.

Users

To use user profiling, simply click **Users** in the toolbar. The system responds with the “User Profiles” window. The “User Profiles” window provides details about all active user profiles. Select the “Enable User Profiling” checkbox option to activate user profiles. You must enable User Profiling to utilize the content filtering feature described in the next section. You must also be logged in as the administrator to see all user profiles and to add a user.

From this window, you can add, view, and delete user profiles. Please see the next section in this document titled Adding a User.

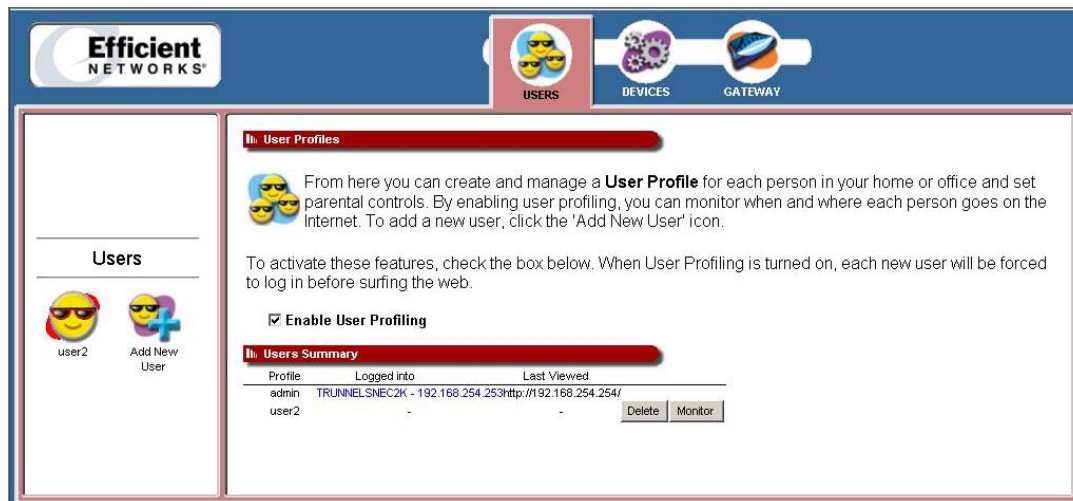


Figure 28: User Profile Window

Adding a User

You may add different users to the gateway to restrict their access to both gateway functions and to the Internet. You **MUST** be logged in as the administrator to add a user.

To add a user:

1. Click **Add New User** in the left-navigation-pane. The system responds with the “Profile User Information” window.

The screenshot shows the 'Profile User Information' window. At the top, there is a navigation bar with 'Log Out: admin' and a 'GO' button, and a 'HELP' button. Below this is the 'Efficient NETWORKS' logo and three main menu items: 'USERS', 'DEVICES', and 'GATEWAY'. The 'USERS' menu item is highlighted. On the left side, there is a 'User Setup:' sidebar with a list of steps: 1. Enter Username (highlighted), 2. Content Filtering, 3. Security Level, 4. Time Settings, 5. Computer, 6. Customize, and 7. Finished. The main content area is titled 'Profile User Information' and contains a form with the following fields: 'Enter Profile Username and Password:' followed by a smiley face icon. Below this are three input fields: 'Username: user1 (required)', 'Password: [masked]', and 'Confirm: [masked]'. At the bottom of the form are three buttons: 'Cancel', 'Next >>', and 'Finish'.

Figure 29. Profile User Information Window

2. Type a user name in the “Username” box.
3. Type a password in the “Password” box.
4. Re-type the password in the “Confirm” box.
5. Click **Next**. The system responds with the “Profile Content Filtering” window. **Note: Optionally**, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.
6. Please see the next section in this document titled *Content Filtering (Optional)*.

Content Filtering (Optional)

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

To use content filtering:

1. Select one of the following options from under the “These are three ways to set this up” heading:
 - **Disable:** All Internet content is allowed for this user.
 - **Allow access Only:** Allows access only to the specified Web addresses or to addresses containing specified word entries. You must specify words or Web addresses to add to the table.
 - **Deny all access:** Disables access to all Web addresses specified as well as addresses that contain any words specified in the filter entries. You must specify words or Web addresses to add to the table.

Note: Optionally, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.

2. If the “Allow access Only” or “Deny all access” option is selected from step 1, 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. **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.
3. Click **Next**.

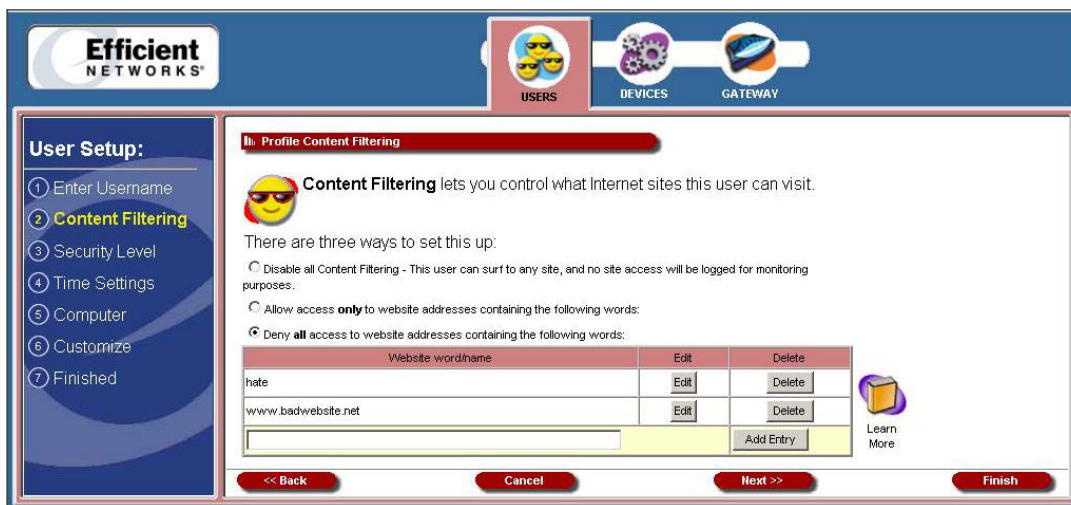


Figure 30: Profile Content Filtering Window

4. The system responds with the “Profile Configuration Access” window. Please see the next section in this document titled *Profile Configuration Access (Optional)*.

Profile Configuration Access (Optional)

Profile configuration allows the administrator to grant users certain permissions to access options on the gateway.

To use profile configuration access:

1. Select one of the following profiles and click **Next**. **Note: Optionally**, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.



Figure 31: Profile Configuration Access Window

2. The system responds with the “Profile Time Settings” window. **Note: Optionally**, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.
 - **Administrator**
Allows access to the Internet and all of the configuration tools on the gateway.
 - **Gamer**
Allows access to the Internet as well as the gateway’s commonly used tools for gamers, including Port Configuration and DMZ.
 - **Web Surfer**
Allows access only to the Internet, not to the gateway’s configuration.
3. Please see the next section in this document titled *Profile Time Settings (Optional)*.

Profile Time Settings (Optional)

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

To use profile time settings:

1. Select one of the following options:
 - **No time of day restrictions:** The user may have Internet privileges at any time.
 - **Only allowed from:** The user may only have Internet privileges at the time range set in the time drop-downs.

Note: Optionally, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.

2. Select one of the following options under the “Designate the number of minutes a user can sit idle before they are automatically logged out from the web” heading:
 - **Infinite Time:** The user is never automatically logged out of the Internet.
 - **Minutes:** Type a time interval in minutes in the “Minutes” box. This time represents how long a user may be idle before automatically being logged out of the Internet.
3. Click **Next**. The system responds with the “Associated Computer/Connected Device” window.

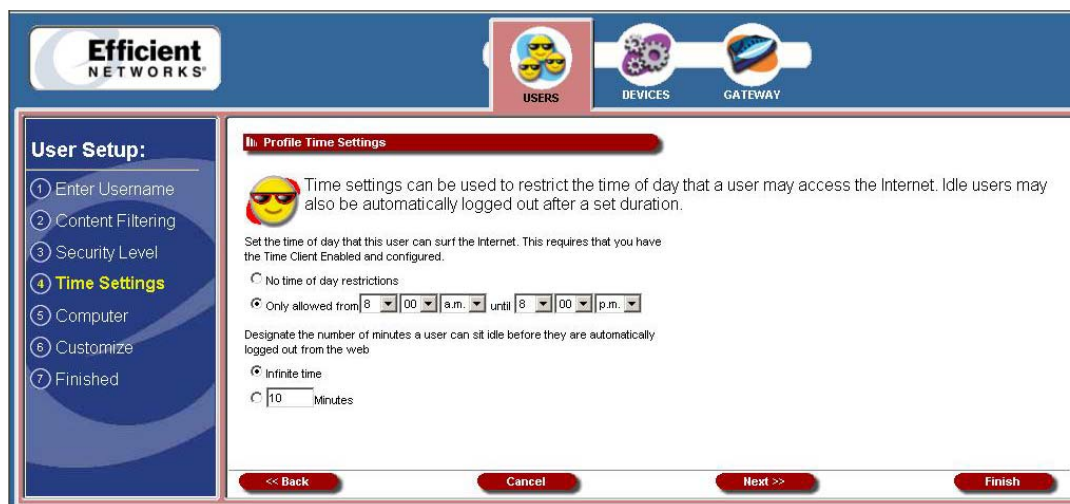


Figure 32: Profile Time Settings Window

4. Please see the next section in this document titled *Associated Computer/Connected Devices (Optional)*.

Associated Computer/Connected Device (Optional)

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

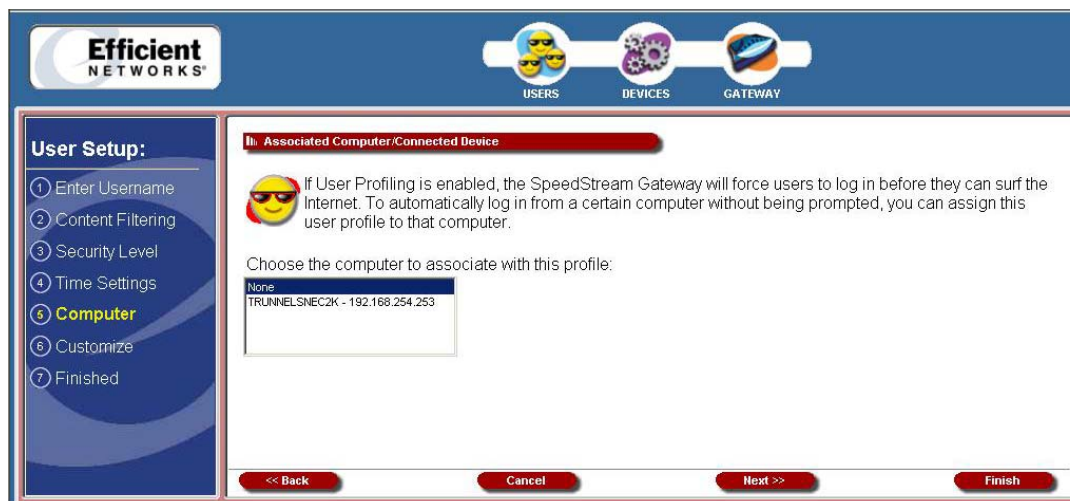


Figure 33: Associated Computer/Connected Device Window

All computers and devices currently on the network, powered on, and detected by the Gateway are displayed in the list. **Note: Optionally**, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.

To associate a connected computer:

1. Select a specific device to associate with the profile, or select **None** to require the user to log in from any device used.
2. Click **Next**. The system responds with the “Customized Profile” window.
3. Please see the next section in this document titled *Customized Profile Icon (Optional)*.

Customized Profile Icon (Optional)

All user profiles have an icon that displays in the left-navigation-pane of the “User Profiles” window. You may customize the color of this icon. **Note: Optionally**, you can click **Finish** to complete the user profile. The system accepts all of the defaults for a user.

To change the color of the user icon:

1. Select a color from the drop-down.
2. **Optionally**, type a numeric color value in the box next to the color drop-down. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. **Note:** If you are entering a numeric value for the color, ensure that the “#” is in front of your numeric value.
3. Click **Finish**. The system responds with the “User Profile” window. The icon of the user you just created is displayed in the left-navigation-pane.
4. Please see the next section in this document titled [Editing a User](#).

Editing a User

To edit a user:

1. Log on as the administrator.
2. Click the **Users** button in the toolbar. The system responds with the “User Profile” window.
3. Click a user icon in the left-navigation-pane. The system responds with the “Profile Monitor” window.
4. Click **Edit Profile**.

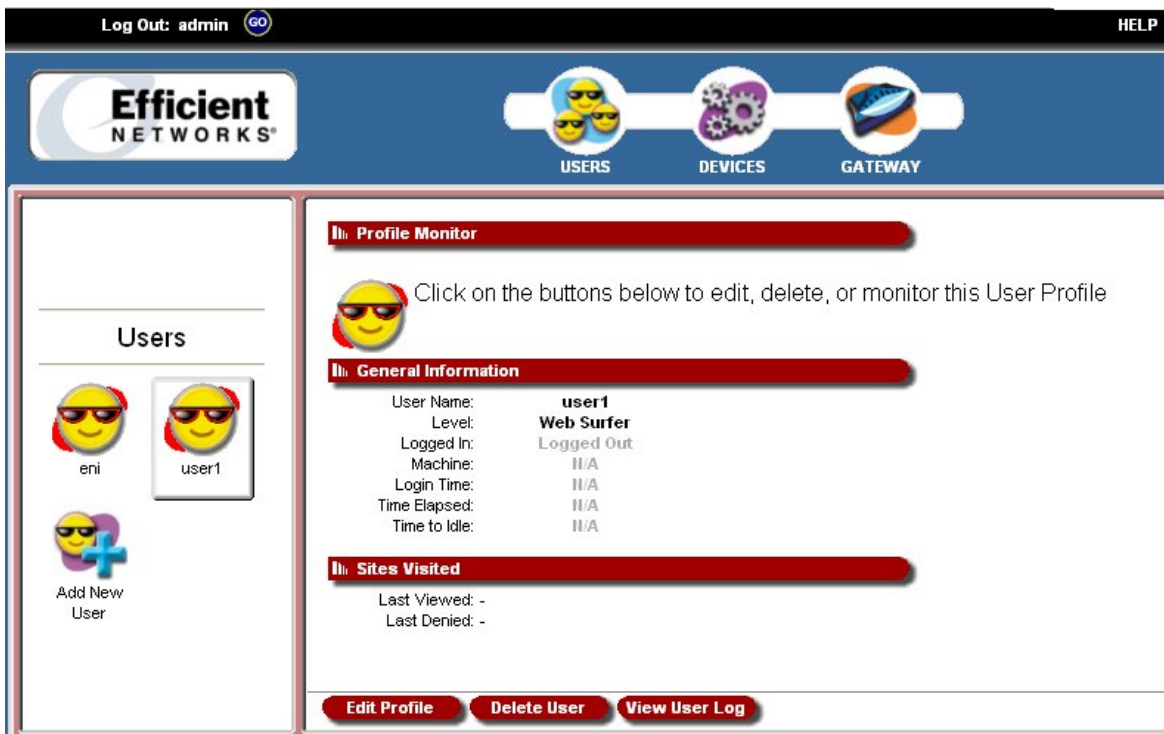


Figure 34. Profile Monitor Window (Editing a User Profile)

5. Make any changes and click **Finish**.

Deleting a User

To delete a user:

1. Log on as the administrator.
2. Click the **Users** button in the toolbar. The system responds with the “User Profile” window.
3. Click a user icon in the left-navigation-pane. The system responds with the “Profile Monitor” window.
4. Click **Delete User**. The system responds with by deleting the user from the system.

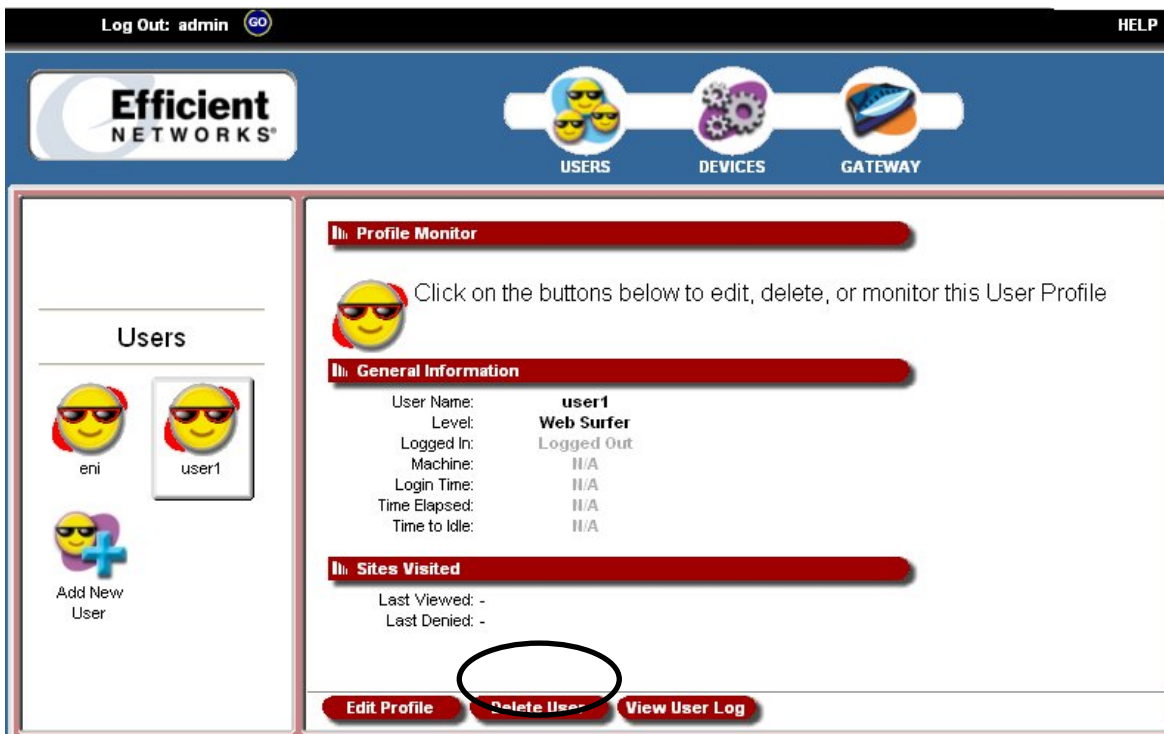


Figure 35. Profile Monitor Window (Deleting a User Profile)

Viewing User Logs

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

To use user logs:

1. Click the **Users** button in the toolbar. The system responds with the “User Profile” window.
2. Click a user icon in the left-navigation-pane. The system responds with the “Profile Monitor” window.
3. Click **View User Log**. The system responds with the “Current Log Entries” window displaying all of the log information about the user.

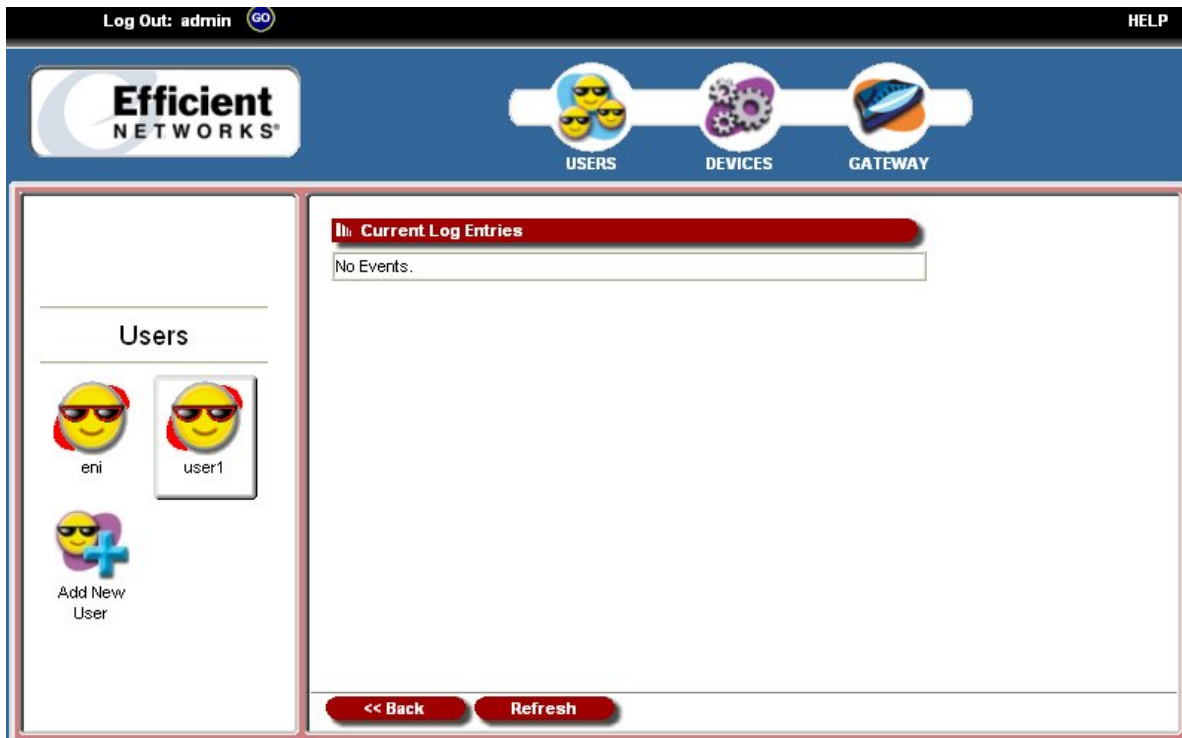


Figure 36. Profile Monitor Window (Viewing User Logs)

Devices

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

To use the Devices option:

1. Click **Devices** in the toolbar. The system responds with the “Connected Devices” window displaying general information about devices on your network.

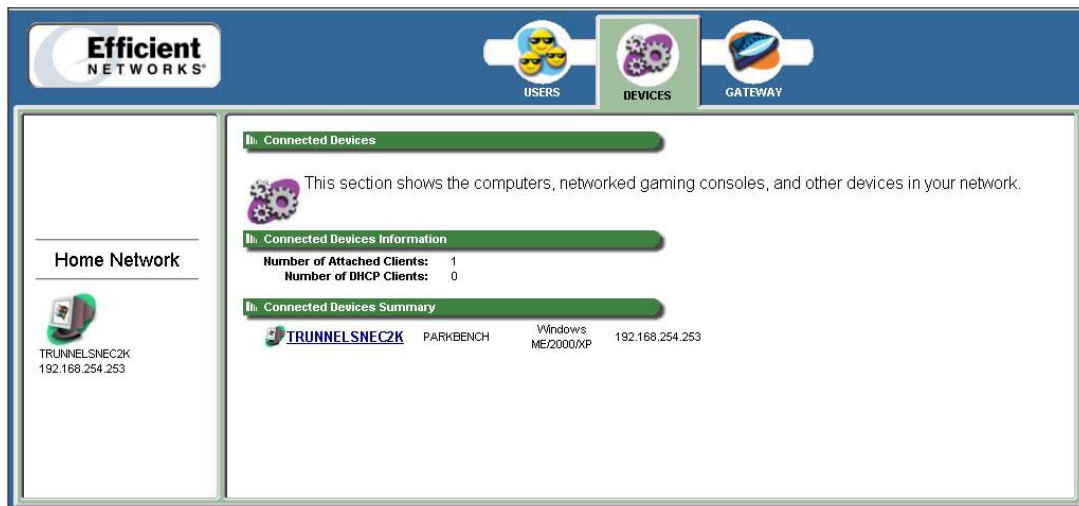


Figure 37: Devices Screen

2. Click the icon of a connected device in the left-navigation-pane, or click the device hyperlink under the “Connected Devices Summary” heading. The system responds with the “Connected Devices” window displaying both general and network information about the select device.

Gateway

The **Gateway** option provides access to all Gateway configuration options, security settings, Gateway health monitoring screens, and Internet connection and network details. The options that display under the Modem Options heading in the left-navigation-pane are based on how you logged into the system. If you logged in as the administrator, all options are turned on and enabled. If you logged in as a user, only the Gateway Health, Customize, and Reboot options are enabled.

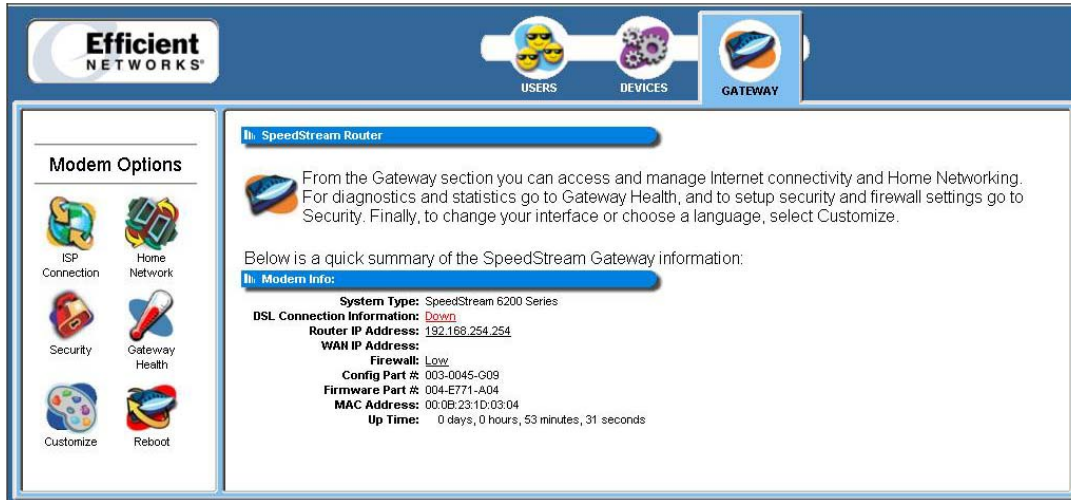


Figure 38: Gateway Window (with Administrator Log on)

ISP Connection

All active and available Internet connections are shown in this window. Many of the settings for this option are intended for use by advanced users. This option may not be available depending on your ISP.

Note: You must be logged in as an administrator to use this option.

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

To use the ISP connection function:

1. Log on as the administrator.
2. Click **Gateway** in the toolbar.
3. Click **ISP Connection** in the left-navigation-pane. The system responds with the “ISP Connection Information” window.

- Click one of the ISP connections (in red) to reconfigure that connection. Please check with your ISP for the information required to reconfigure a connection.

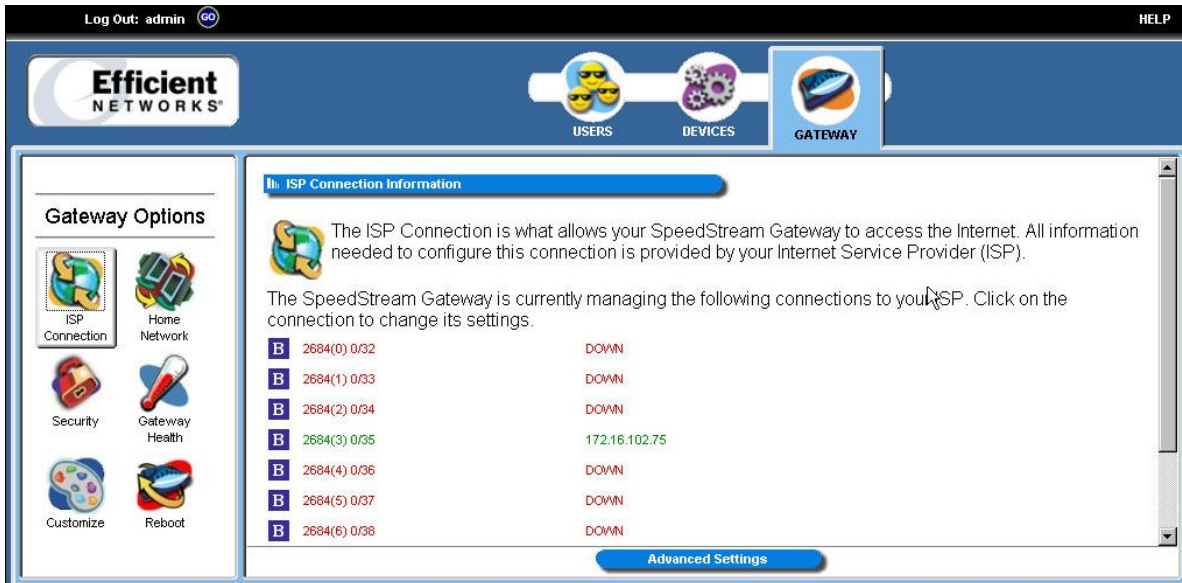


Figure 39: ISP Connection Information Window

- Click **Advanced Settings** to configure additional access options from your ISP. The system responds with the “Advanced Internet Options” window.

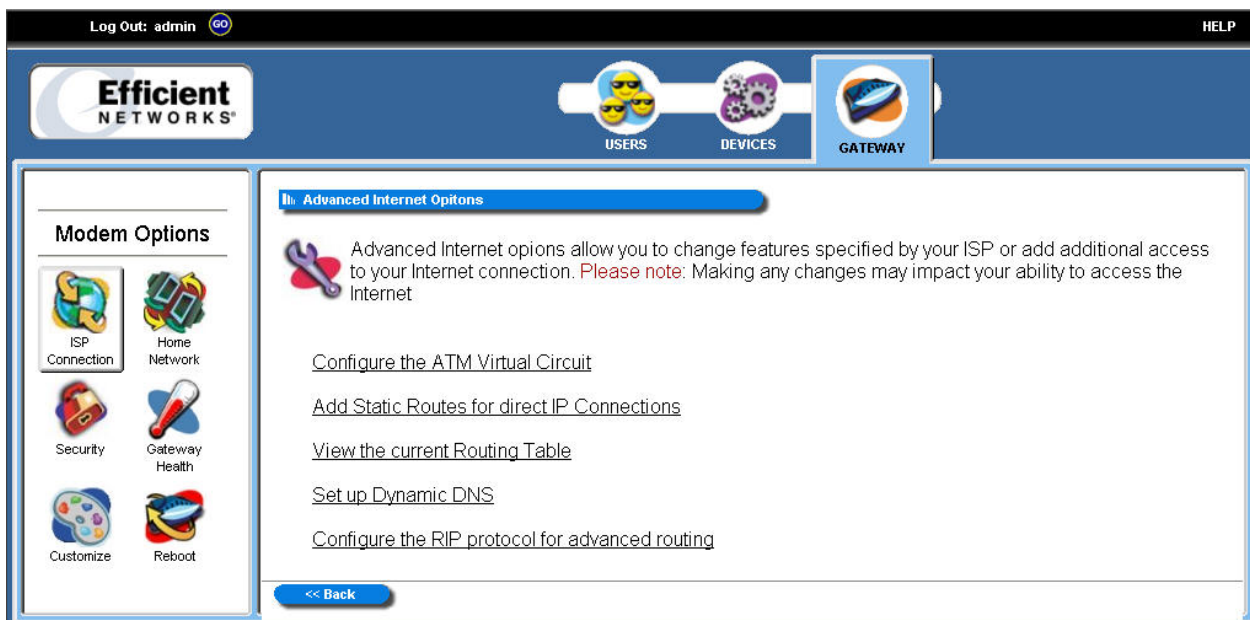


Figure 40: Advanced Internet Options Window

- Please see the next section in this document titled [Advanced Internet Options](#).

Advanced Internet Options

All of 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.

ATM Virtual Circuits

The ATM virtual circuit option provides access to settings that your Internet Service Provider may advise you to modify depending upon your service needs. This option allows the creation and configuration of a PVC (Permanent Virtual Circuit) across a network. A PVC is used to maintain a permanent connection between two points on a network. **Note: ATM Setting changes should not be made unless you are advised to do so by your Internet Service Provider.**

To access the ATM virtual circuit option:

1. Click **Advanced Settings**. The system responds with the “Advanced Internet Options” window.

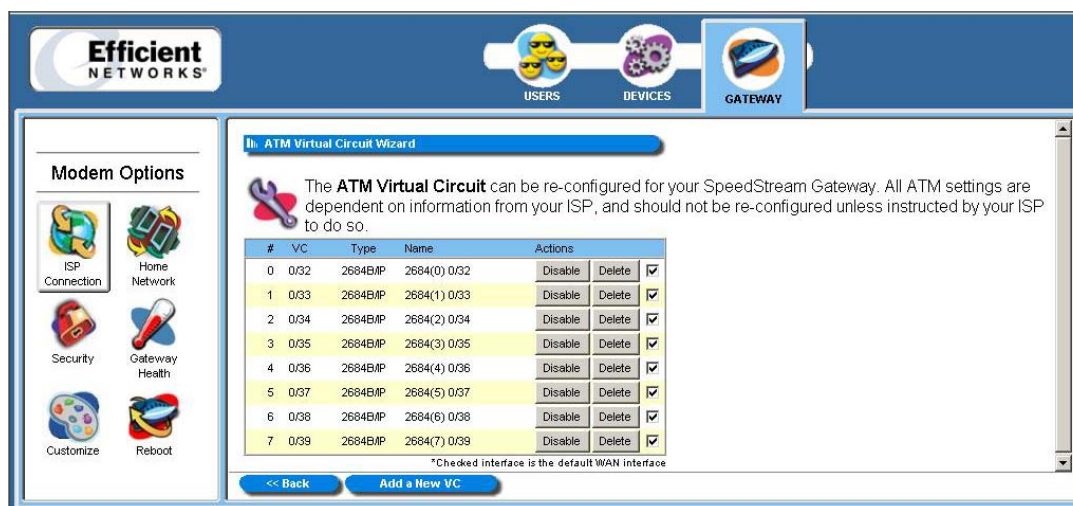


Figure 41: ATM Virtual Circuits Screen

2. Click the “Configure ATM Virtual Circuit” hyperlink. The system responds with the “ATM Virtual Circuit Wizard” window.

Static Routes

The static routes option allows you to configure static routes to remote equipment. These routes appear in the routing table. 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 use the static route option:

1. Click **Advanced Settings**. The system responds with the “Advanced Internet Options” window.
2. Click the “Add Static Routes for Direct IP Connections” hyperlink. The system responds with the “Static Routes” window.

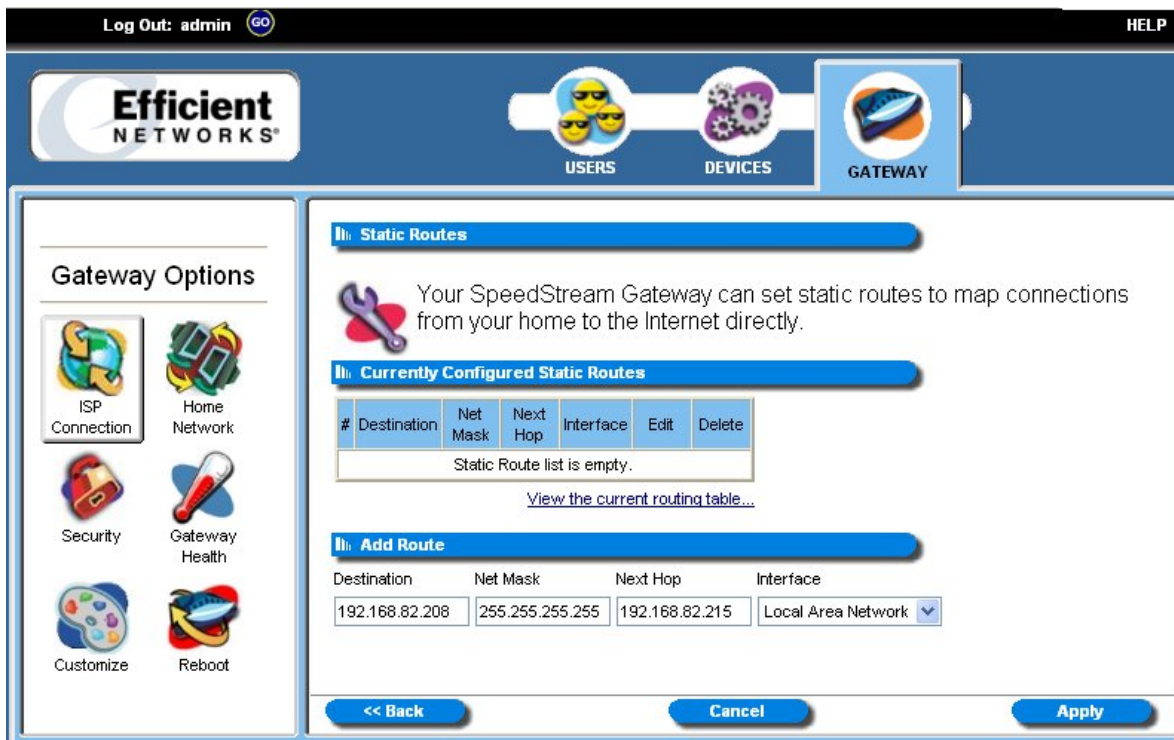


Figure 42: Static Routes Window

3. Type the IP address of the destination device in the “Destination” box.
4. **Optionally**, click the “View the current routing table” hyperlink to view the current routing table. Please see the section in this document titled [Routing Table](#) for more information.
5. Type the net mask of the destination device in the “Net Mask” box.
6. **Optionally**, type the IP address of a destination gateway in the “Next Hop” box.
7. Select a connection type from the “Interface” drop-down.
8. Click **Apply**. The system responds by adding your new route to the routing table.

Routing Table

This screen shows a table of routing information including Destination IP Address, Subnet Mask, Flags, Gateway, Metric and Interface of all static and dynamic routes for network devices.

To access the routing table:

1. Log on as the administrator.
2. Click **Gateway** in the toolbar.
3. Click **ISP Connection** in the left-navigation-pane.
4. Click **Advanced Settings**. The system responds with the “Advanced Internet Options” window.
5. Click the “View the Current Routing Table” hyperlink. The system responds with the “Current Routing Table” window.

Current Routing Table

This is a listing of all currently mapped routes in the SpeedStream Gateway. It shows both static and dynamically learned routes.

Destination	Netmask	Gateway	Flags	Metric	Interface
127.0.0.0	255.0.0.0	127.0.0.1		1	lo0
192.168.254.0	255.255.255.0	192.168.254.254		1	LAN

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

<< Back

Figure 43: Routing Table Window

Dynamic DNS

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

To use the DDNS service:

1. You must register for the service at <http://www.dyndns.org/services/dydns> there is no fee for this service.

- In the Address bar of your browser type www.dydns.org/services/dydns and press the **ENTER** key. The system responds by displaying the “DynDNS.org” Web page.

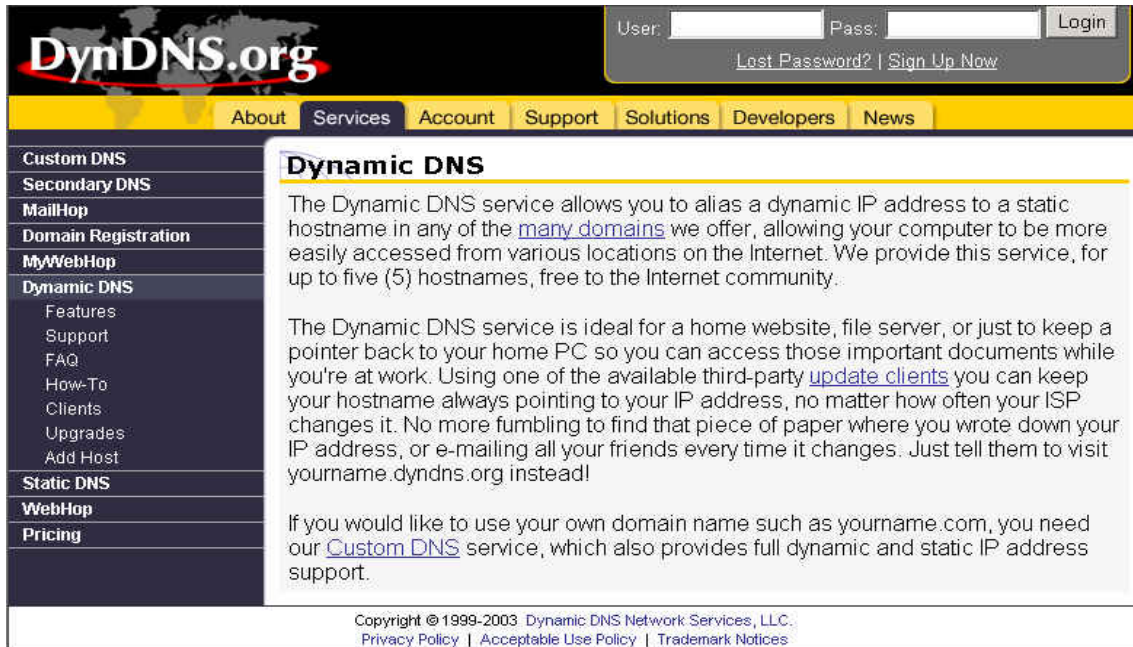


Figure 44. DynDNS Main Web Page

- Click the “Sign Up Now” hyperlink in the upper-right corner of the “DynDNS” Web page. The system responds with the “Create Account” Web page.
- Read the license agreement and click the “I have read and agree to the Acceptable Use Policy above” checkbox.
- Type a user name in the “Username” box.
- Type an email address in the “Email Address” box.
- Re-type the email address in the “Confirm Email Address” box.
- Type a password in the “Password” box.
- Re-type the password in the “Confirm Password” box.
- Click **Create Account**. The system responds by sending an email to the email address you typed in step 6. You must click the hyperlink specified in the email in 48 hours for your account to be active.

11. Re-type www.dyndns.org/services/dyndns in the Address bar of your browser. In the upper-right corner of the DynDNS Web page, type your user ID in the “User” box.
12. Type your password in the “Pass” box.
13. Click **Login**.

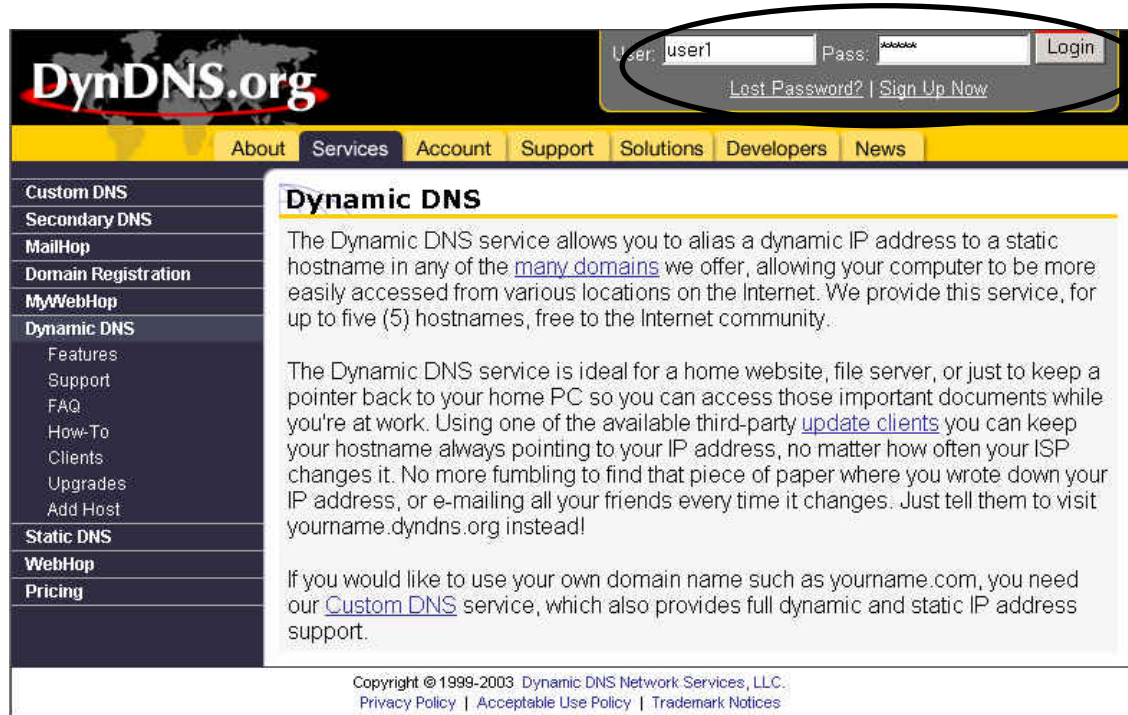


Figure 45. DyDNS Login

14. At the bottom of the “DynDNS” Web page, click the “Add a Host” hyperlink.

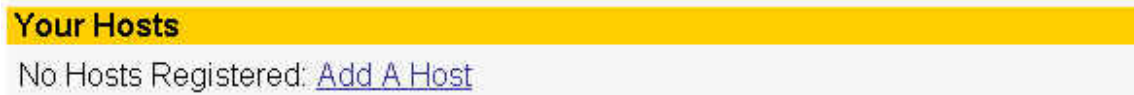


Figure 46. Your Hosts

15. In the “New Dynamic DNS Host” Web page, type a hostname in the “Hostname” box. The hostname can be something like “mypage.athome.”

16. Select the second part of the hostname in the drop-down next to the “Hostname” box.
17. The system automatically displays the IP address of the device you are using. Type the gateway IP in the “IP Address” box.
18. **Optionally**, select the “Enable Wildcard” checkbox if using custom DNS options.
19. **Optionally**, type the hostname of a mail exchanger in the “Mail Exchanger (optional)” box. A mail exchanger allows you to specify that you want mail to a specific machine to be handled by another machine.
20. **Optionally**, select the Backup MX checkbox if you wish for your mail to be stored in a backup location on the mail exchanger. This is used in case a server fails, and the mail is stored and can be accessed once a specified server is operational.
21. Click **Add Host**. The system responds with the “Hostname Created” window displaying a confirmation that the new hostname is now active.
22. Enter your data from www.dyndns.org in the Gateway's DDNS screen. The gateway automatically ensures that your current IP address is recorded at <http://www.dyndns.org>. From the Internet, users can connect to your servers (or DMZ computer) using your Domain name. Please see the section in this document titled [DMZ](#) for more information on DMZs.

To set up Dynamic DNS:

1. Click the “Set up Dynamic DNS” hyperlink. The system responds with the “Set Up Dynamic DNS” window.

The screenshot shows the 'Set Up Dynamic DNS' window in the Efficient Networks gateway interface. The interface has a top navigation bar with 'Log Out: admin' and 'HELP' on the left, and 'USERS', 'DEVICES', and 'GATEWAY' icons on the right. The main content area is titled 'Set Up Dynamic DNS' and contains the following elements:

- Dynamic DNS Client:** Two radio buttons, 'Disable' (unselected) and 'Enable' (selected).
- Service Username:** A text input field containing 'user1'.
- Service Password:** A text input field containing seven dots.
- Host Name 1:** A text input field containing 'http://myusername.dydns.org'.
- Host Name 2:** An empty text input field with '(Optional)' to its right.

At the bottom of the window are three buttons: '<< Back', 'Cancel', and 'Apply'.

Figure 47: Dynamic DNS Window

2. Select the “Enable” option.
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.

RIP (Routing Information Protocol)

RIP (Routing Information Protocol) is based on distance algorithms that calculate the shortest distance between two points on the network based on the addresses of the originating devices. The shortest path is determined by the number of hops between these two points. RIP also allows for the receiving of routing updates from the devices connected to the gateway.

1. Click the “Configure the RIP protocol for advanced routing” hyperlink. The system responds with the “RIP Configuration” window.

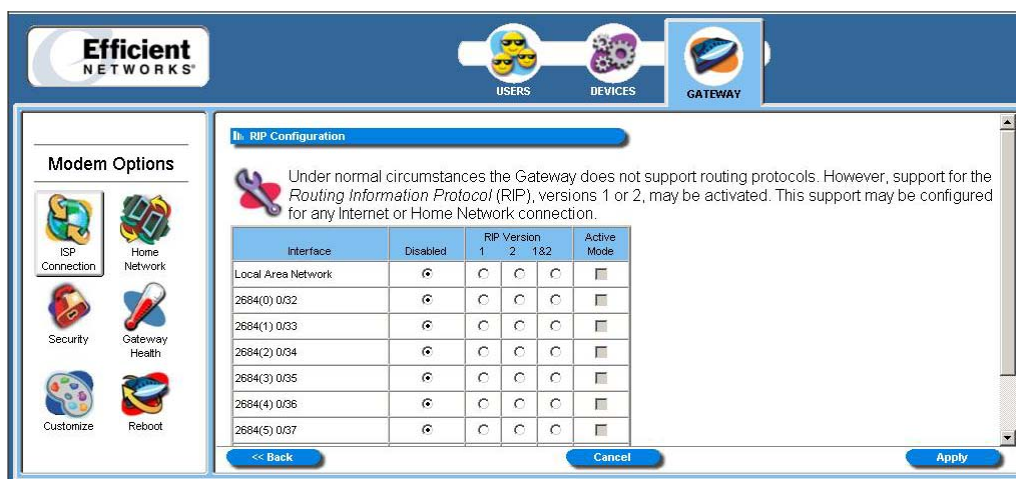


Figure 48: RIP Window

2. Select one of the following options from under the “RIP Version” heading and 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:** Specifies an IP address for the routing entry.
 - **Subnet Mask:** Specifies a mask for the routing entry.
 - **Next Hop:** IP address of the next hop where the packets should be forwarded.
 - **Metric:** Shows how many routers the routing packet has crossed to its destination.
 - **1&2:** A combination of both types of RIP packets.
3. Select an “Active Mode” checkbox next to a corresponding connection to enable it.
4. Click **Apply**. The system responds with the “Your Settings Have Been Saved” window.
5. **Optionally**, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your gateway.

Home Network

The home network option displays all network-related information. **Note:** You must be logged in as the administrator to access this option.

To use the Home Network option:

1. Log on as the administrator.
2. Click **Gateway** in the toolbar.
3. Click **Home Network** in the left-navigation-pane. The system responds with the “Home Network” window.

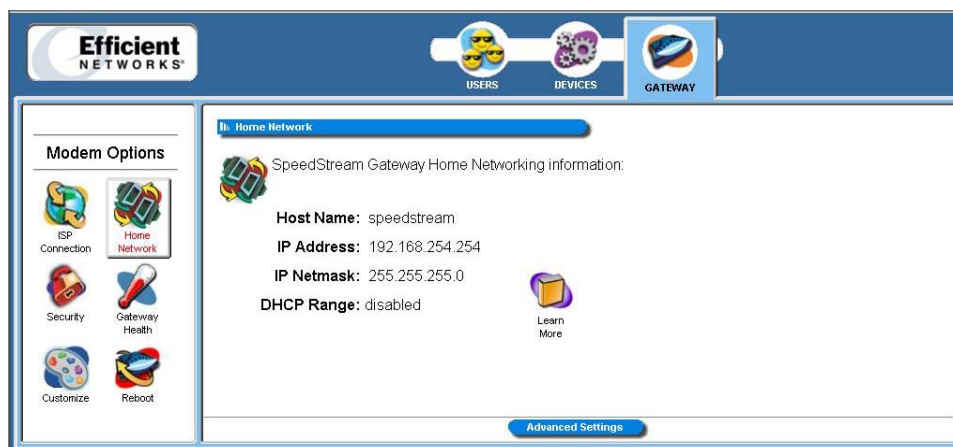


Figure 49: Home Network Window

4. **Optionally**, click Advanced Settings. The system responds with the “Advanced Home Networking” window.

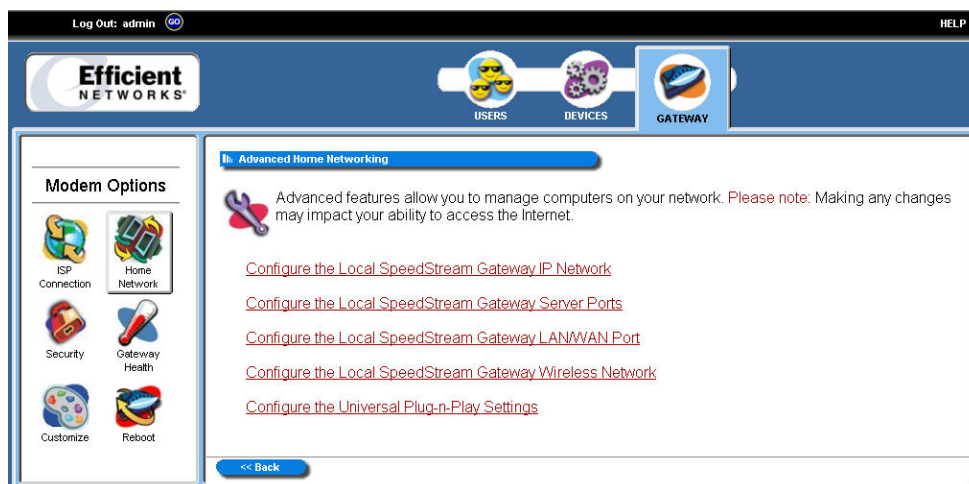


Figure 50. Advanced Home Networking Window

IP Network

The Gateway provides the flexibility to use different ranges of IP addresses to be assigned by the DHCP Server housed in the Gateway. DHCP (Dynamic Host Configuration Protocol) allows computers to obtain either permanently or temporarily, IP addresses from a central server. Ensure that you select an IP address range that is not in conflict with any existing devices. A custom configuration option is provided for advanced users.

To use the IP network option:

1. Click the “Configure the local SpeedStream Gateway IP Network” hyperlink. The system responds with the “SpeedStream Gateway IP Network” window.

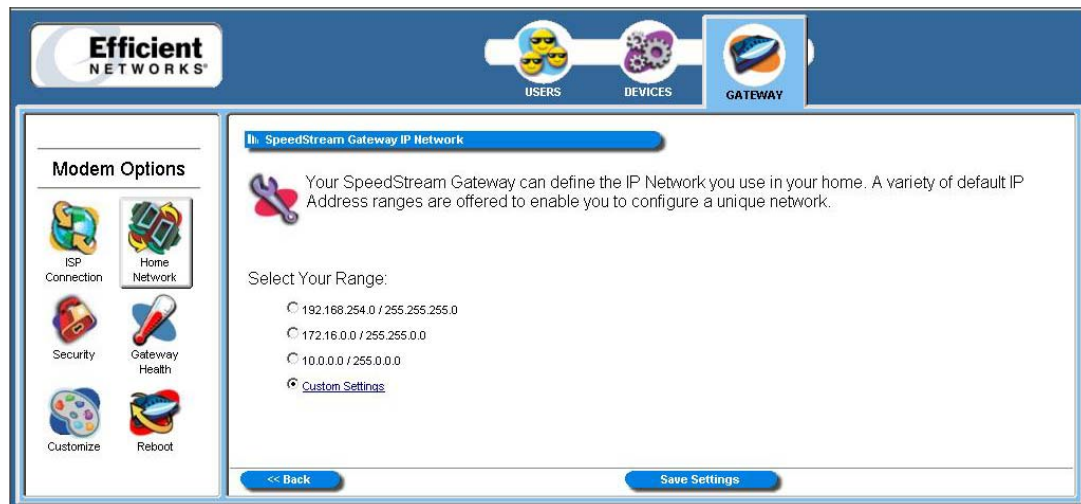


Figure 51. Speedstream Gateway IP Network Window

2. Select a range from the displayed options and click **Save Settings**.
3. **Optionally**, click the “Custom Settings” hyperlink for advanced configuration. Please contact your ISP for more information on configuring the options for custom settings.

Server Ports

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

To use the server port option:

1. Click the “Configure the Local SpeedStream Gateway Server Ports” hyperlink. The system responds with the “SpeedStream Gateway Server Ports” window.

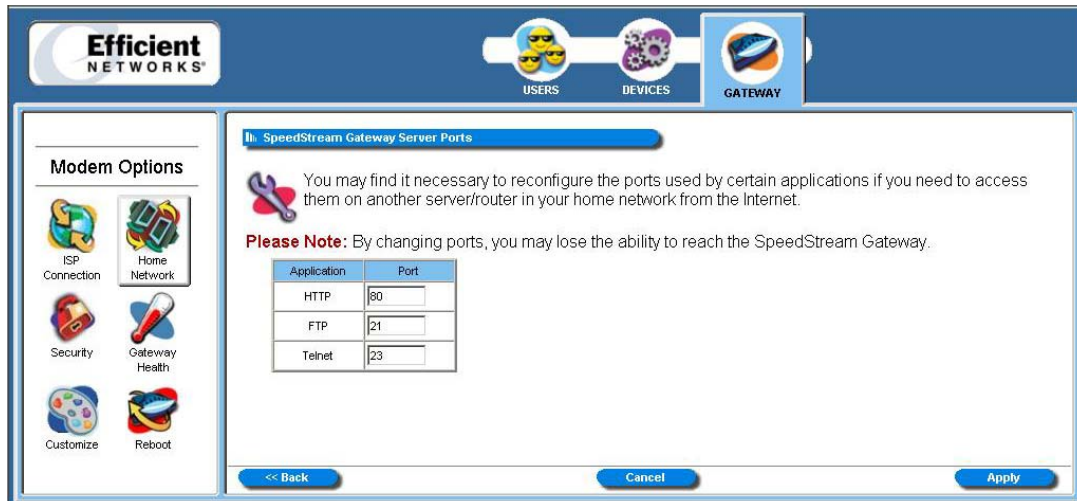


Figure 52: Server Ports Screen

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**. The system responds with the “Your settings have been saved” window.
6. **Optionally**, click **Reboot** if you wish for the settings to immediately be implemented. The system responds by restarting your gateway.

LAN/WAN Port

Ethernet port #5 can be used as either a LAN (network) port or as a WAN (Internet connection) port. Select the appropriate option to define whether the port is used as a fifth local network port or as a connection for another broadband device.

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

To configure the LAN/WAN port:

1. Click the “Configure the Local SpeedStream Gateway LAN/WAN Port” hyperlink. The system responds with the “SpeedStream Gateway LAN/WAN Port” window.

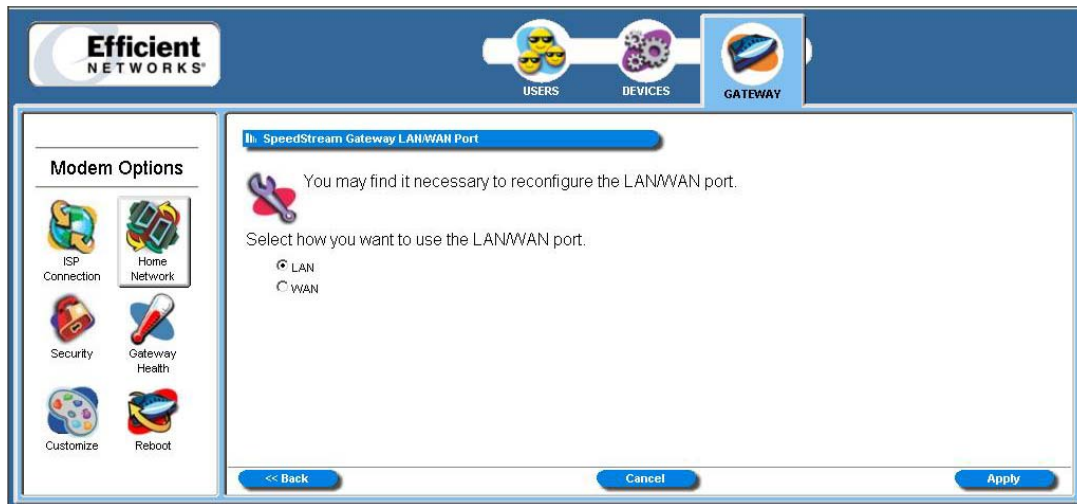


Figure 53: LAN/WAN Port Window

2. Select one of the following options under the “Select how you want to use the LAN/WAN port” heading:
 - **LAN** (Local Area Network): The connected network located in your home or premises.
 - **WAN** (Wide Area Network): A large connected network such as the Internet that is spread over a large geographic area. Note: If you select the WAN option, please contact your ISP for instructions on how to configure this option.
3. Click **Apply**.

Wireless Network (Optional)

This option allows you to either setup or configure a pre-existing setup of the wireless equipment in your gateway. **Note:** This option is only shown when a SpeedStream wireless expansion card is installed in the SpeedStream 6200 Gateway, or with the SpeedStream 6300 model with built-in wireless interface.

The wireless settings on the Gateway must match those of any wireless clients on your network.

To use the wireless network option:

1. Click the “Configure the Local SpeedStream Gateway Wireless Network” hyperlink. The system responds with the “Wireless Setup Configuration” window.

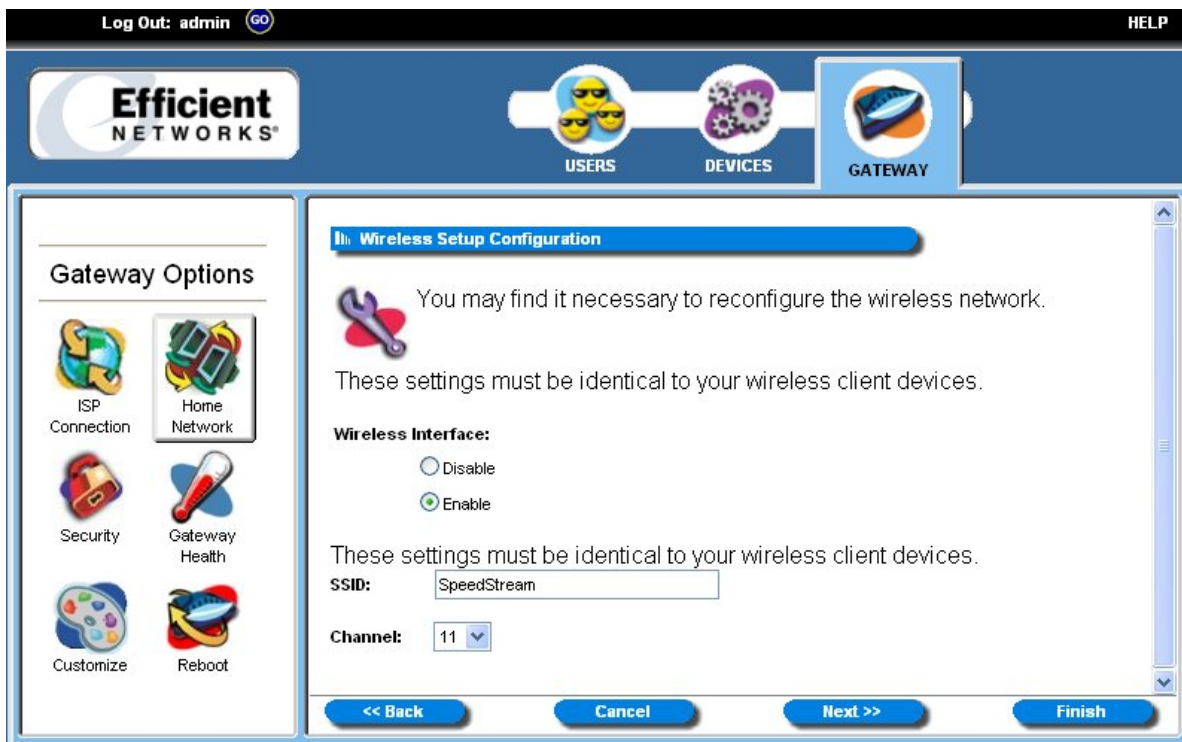


Figure 54: Wireless Setup Configuration Window

2. Select the “Enable” option.
3. Type your wireless network ID in the “SSID” (Service Set Identifier) box.
4. **Optionally**, change the “Channel ID” drop-down from 11 if you experience any interference with your wireless gateway.

5. Click Next.

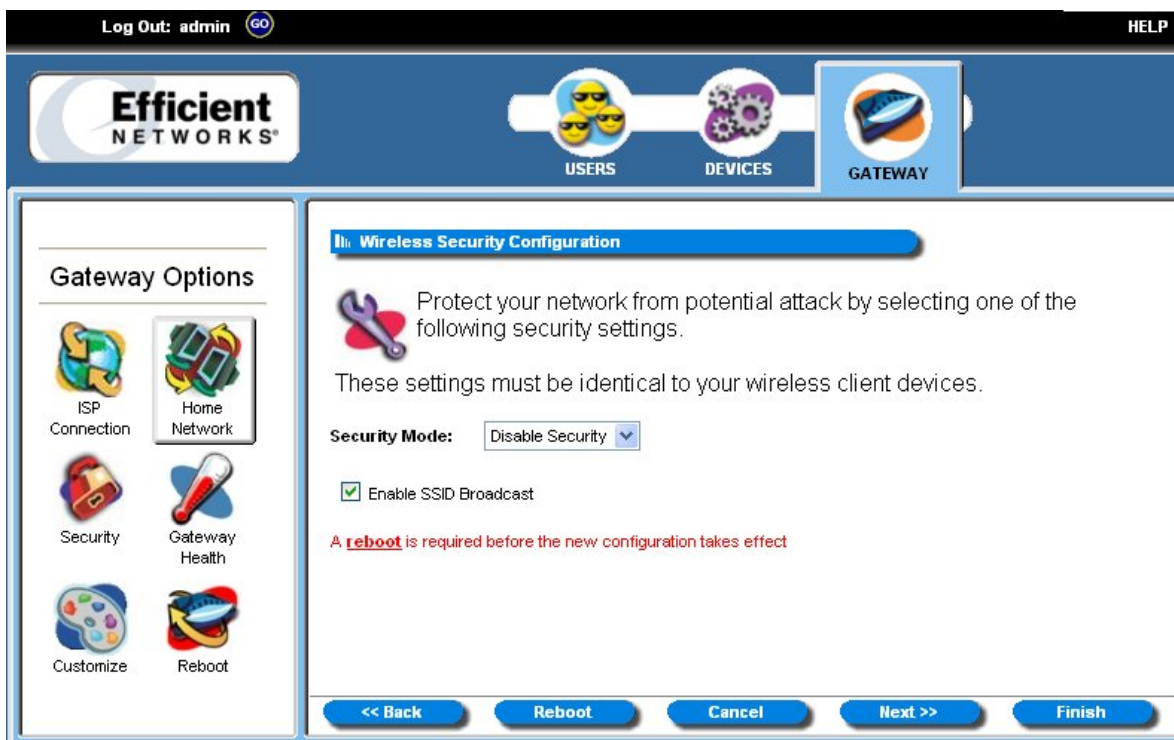


Figure 55. Wireless Configuration Window (Default)

6. The “Wireless Security Configuration” window allows you to set the wireless security level you wish to use. All wireless devices attached to the gateway **MUST** have the same wireless security settings for your network to have proper communications and security. If you own the 6200 series gateway, the “Wireless Security Configuration” window does not appear. From the “Security Mode” drop-down, select one of the following options:

- **WEP 64-bits:** (Wireless Equivalency Privacy): WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. Please see the section in this document titled [Wireless Setup WEP 64-Bit Option \(Advanced Home Networking\)](#) for more information.
- **WEP 128-bits:** (Wireless Equivalency Privacy): WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is a most secure WEP option. Please see the section in this document titled [Wireless Setup WEP 128-Bit Option \(Advanced Home Networking\)](#) for more information.
- **WPA PSK:** (Wi-Fi Protected Access) WPA security changes encryption keys after a specified amount of time. This is the most secure option for wireless networks. Please see the section in this document titled [Wireless Setup WPA PSK Option \(Advanced Home Networking\)](#) for more information.

Wireless Setup WEP 64-Bit Option (Advanced Home Networking)

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 64-bit encryption, which is the least secure WEP option. This section assumes you currently have the “Wireless Security Configuration” window displayed.

To use the WEP 64-bit option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. **Optionally**, select the “Enable SSID Broadcast” option if you wish if you wish for wireless users to see the existence of your wireless router with the associated SSID. This could cause a security problem if outside users can determine your channel and encryption. Disabling the SSID broadcast prevents outside users from seeing the existence of your wireless router.
3. Click **Next**.

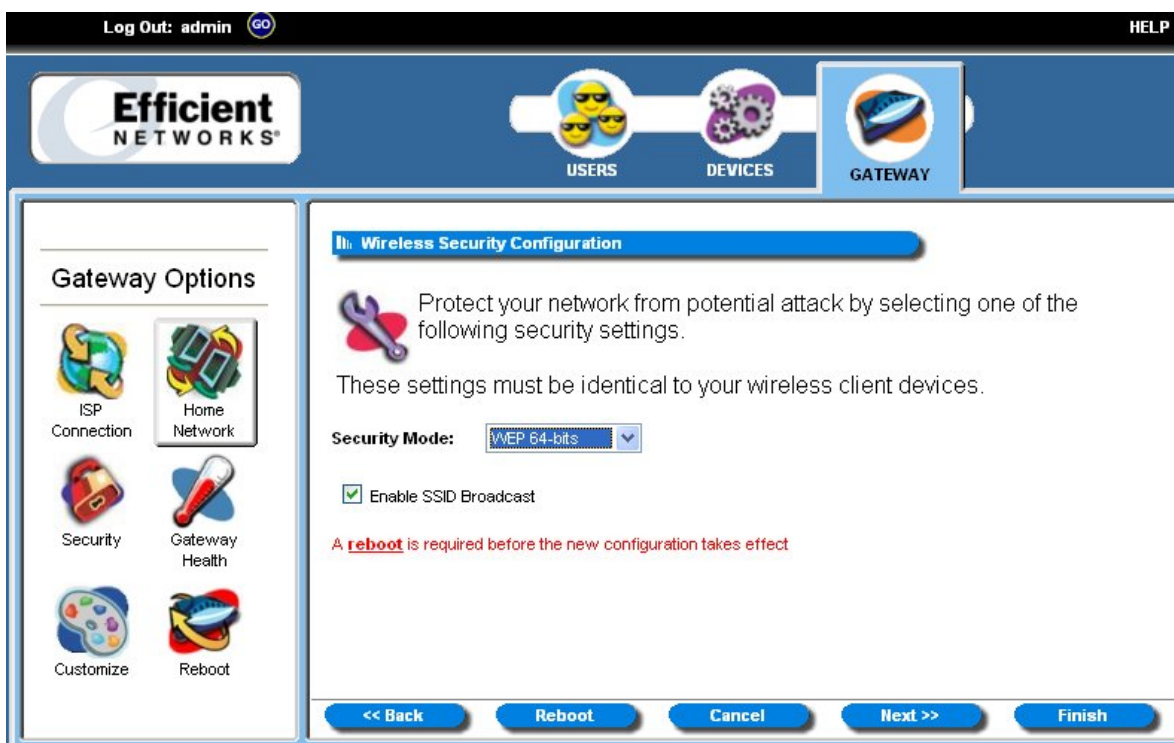


Figure 56. WEP 64-Bit Encryption (Advanced Home Networking)

4. The “Wireless 64-bit WEP Configuration” window allows you to configure the security for the 64-bit WEP option. Select one of the following options:
 - **Open System:** Open system keys are always authenticated at the device level. After authentication, data is then encrypted between the gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
 - **Shared Key:** Shared keys accept a string of unencrypted data from a device. The gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
8. Type a phrase in the “Passphrase” box. The passphrase is used to generate the 64-bit key. The passphrase must at least be one character with a maximum of 32 characters.

9. Click **Generate Keys**. The system responds by generating keys that display in the boxes under the “Passphrase” box.
10. Click **Next**.



Figure 57. Wireless 64-Bit WEP Configuration Window

11. Please see the section in this document titled [Wireless Filter and Options Configuration](#).

Wireless Setup WEP 128-Bit Option (Advanced Home Networking)

WEP security offers the same security offered by a wired LAN with encrypted packets. This option offers 128-bit encryption, which is the most secure WEP option. This section assumes you currently have the “Wireless Security Configuration” window displayed.

To use the WEP 64-bit option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. **Optionally**, select the “Enable SSID Broadcast” option if you wish if you wish for wireless users to see the existence of your wireless router with the associated SSID. This could cause a security problem if outside users can determine your channel and encryption. Disabling the SSID broadcast prevents outside users from seeing the existence of your wireless router.
3. Click **Next**.

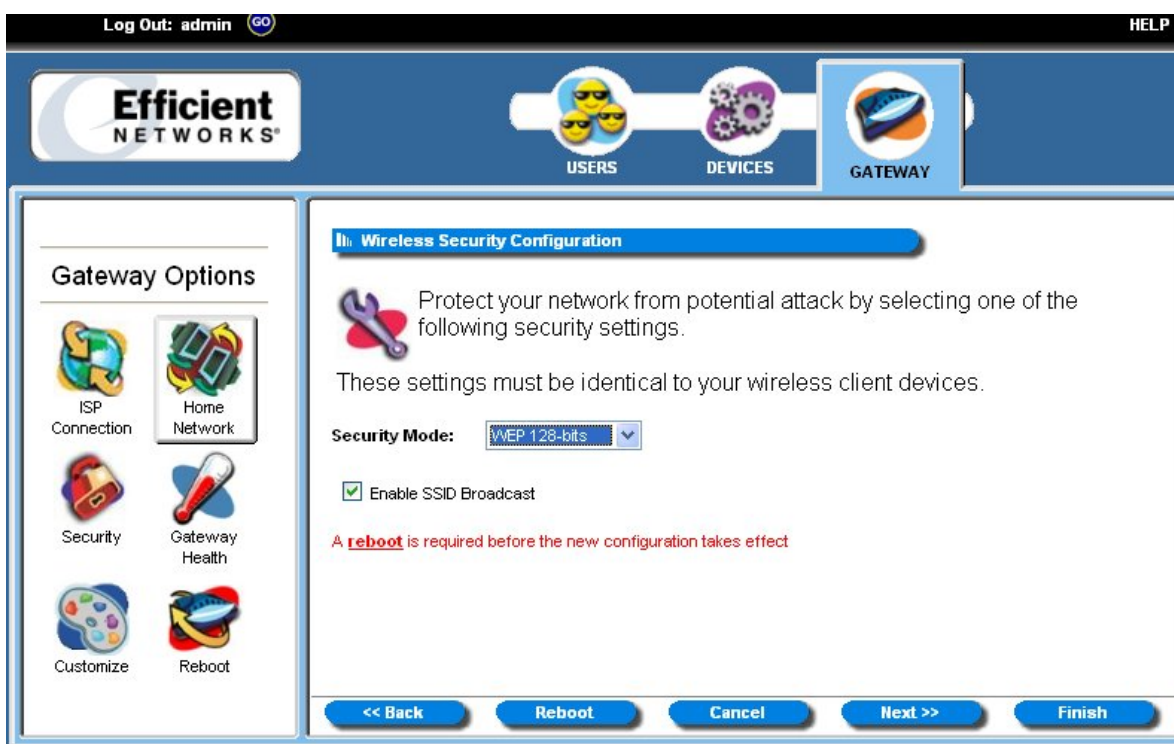


Figure 58. Wireless Security Configuration 128-Bit WEP

4. The “Wireless 128-bit WEP Configuration” window allows you to configure the security for the 128-bit WEP option. Select one of the following options:
 - **Open System:** Open system keys are always authenticated at the device level. After authentication, data is then encrypted between the gateway and the connected device. This is the weakest form of security and should not be used for sensitive data.
 - **Shared Key:** Shared keys accept a string of unencrypted data from a device. The gateway encrypts with a WEP key and sends back the encrypted data to the attached device.
5. Type a phrase in the “Passphrase” box. The passphrase is used to generate the 64-bit key. The passphrase must at least be one character with a maximum of 32 characters.

6. Click **Generate Keys**. The system responds by generating keys that display in the boxes under the “Passphrase” box.
7. Click **Next**.

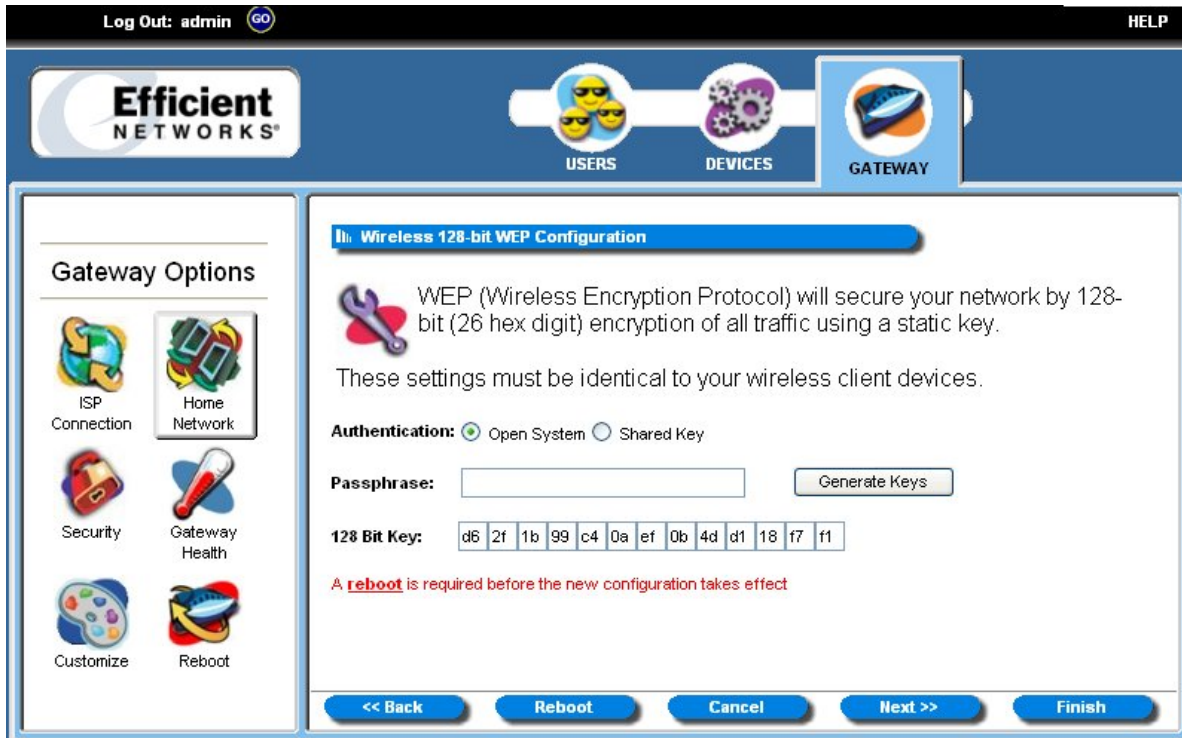


Figure 59. Wireless 64-Bit WEP Configuration Window

7. Please see the section in this document titled [Wireless Filter and Options Configuration](#).

Wireless Setup WPA PSK Option (Advanced Home Networking)

WPA security changes encryption keys after a specified amount of time. This is the **most secure option** for wireless networks. This section assumes you currently have the “Wireless Security Configuration” window displayed on your computer.

To use the WPA option:

1. Select the WEP 64-bits option from the “Security Mode” drop-down.
2. **Optionally**, select the “Enable SSID Broadcast” option if you wish if you wish for wireless users to see the existence of your wireless router with the associated SSID. This could cause a security problem if outside users can determine your channel and encryption. Disabling the SSID broadcast prevents outside users from seeing the existence of your wireless router.
3. Click **Next**.

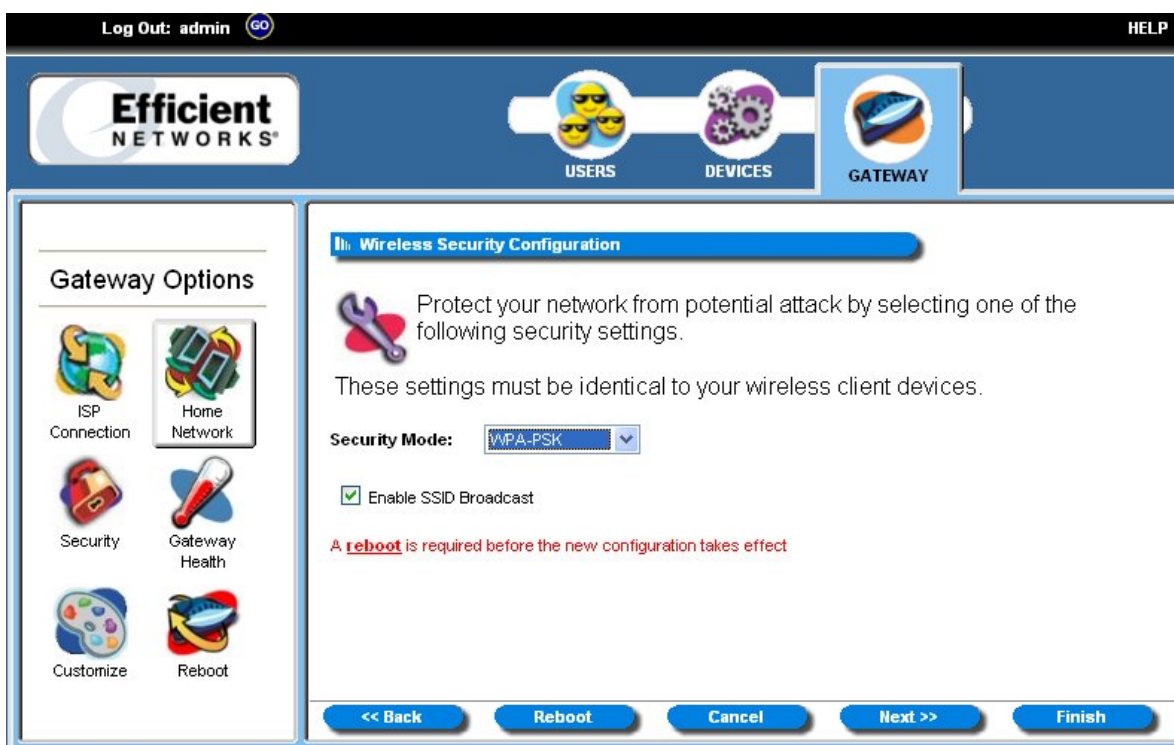


Figure 60. Wireless Security Configuration WPA-PSK

4. The “Wireless WPA Configuration” window is used to configure the algorithm, shared key, and key renewal options. Select one of the following options from the “Algorithms” drop-down:
 - **TKIP:** (Temporal Key Integrity Protocol) TKIP is a more powerful security protocol than WEP and supports: Verification of the security configuration after the encryption keys are determined, synchronizes changing of the unicast encryption key for each frame, and the determines a unique starting unicast encryption key for each pre-shared key authentication.
 - **AES:** (Advanced Encryption Standard) AES supports a private key algorithm that ranges from 128 to 256 bits.

5. Type a key in the “Shared Key” box. The shared key is used to generate a dynamic encryption key for gateway security.
6. Type a numeric value (in seconds) of the time lapse in changing the key in the “Group Key Renewal” box and click **Next**. **Note:** The minimum time value is 30.



Figure 61. Wireless WPA Configuration Window

7. Please see the section in this document titled *Wireless Filter and Options Configuration*.

Wireless Filter and Options Configuration

The “Wireless Filter Configuration” window allows you to either permit or deny access to the gateway of wireless devices based on the MAC address of the device. A MAC (Media Access Control) address refers to a hardware address that uniquely identifies each device of a network. **Note:** Please see the user documentation for each device you wish to deny or allow access for a particular MAC address.

Log Out: admin [GO](#) HELP

Efficient NETWORKS

USERS DEVICES GATEWAY

Gateway Options

- ISP Connection
- Home Network
- Security
- Gateway Health
- Customize
- Reboot

Wireless Filter Configuration

A **reboot** is required before the new configuration takes effect

This feature allows you to control which wireless devices may or may not have access to the gateway.

When the Filter is **Enable** and the mode is **Allow**, only these devices will be allowed to access the Gateway.
If the Filter is **Enable** and the mode is **Deny**, only these devices will be denied access to the Gateway.

Wireless Filter: Enable Disable Filter Mode: Allow Deny

User	MAC Address	User	MAC Address
Device 1	00:20:ea:62:57:81	Device 11	
Device 2		Device 12	

<< Back Reboot Cancel Next >> Finish

Figure 62. Wireless Filter Configuration Window

To use the wireless filter configuration:

1. Select the “Enable” option to either allow or deny access to the gateway. **Note:** If you select the “Disable” option, all devices have access to the gateway.
2. If the “Enable” option was selected in step 1, click the “Allow” or “Deny” option next to the “Filter Mode” heading. The “Allow” option allows all of the MAC addresses entered in the table below access to the gateway. The “Deny” option denies all of the MAC addresses entered in the table below access to the gateway.
3. Type the MAC address in the “MAC Address” column of each device in which you either want to allow or restrict access.

4. Click **Next**. The system responds with the “Wireless Options Configuration” window.

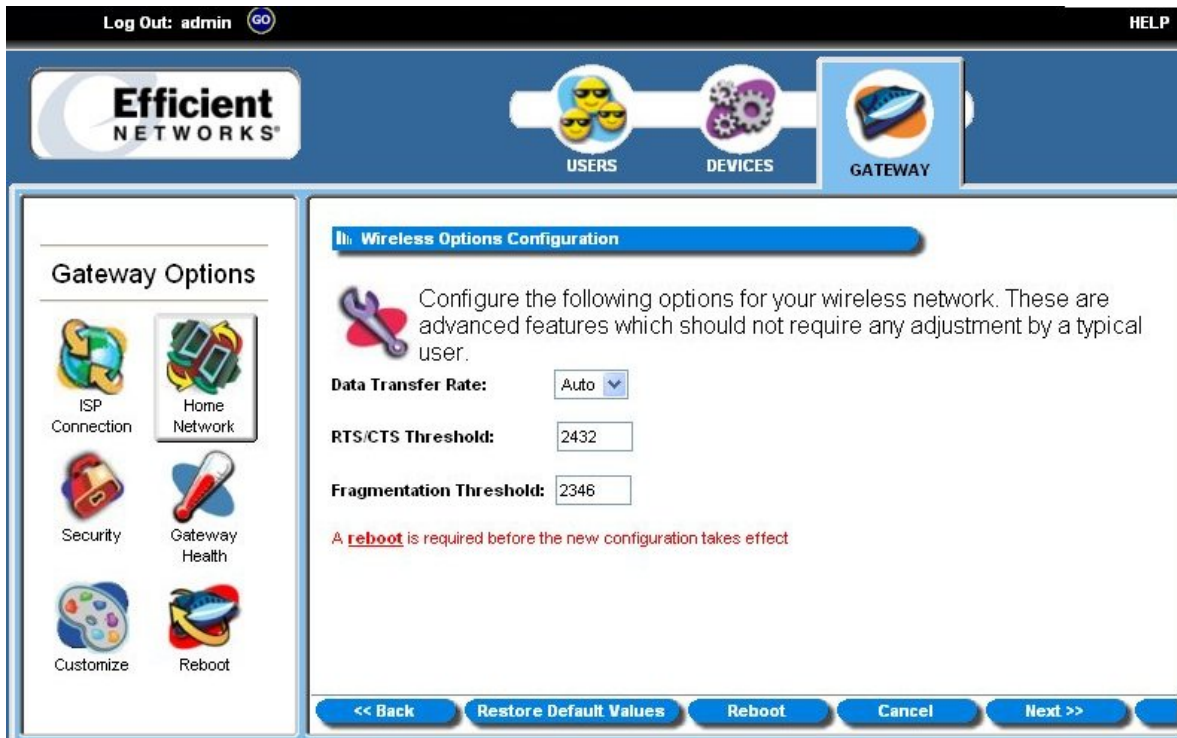


Figure 63. Wireless Options Configuration Window

5. Optionally, configure the following items:

- **Data Transfer Rate**
If a particular wireless client is unable to auto-negotiate a connection to the Gateway, the data transfer rate may be set to a specific data rate such as 11 Mbps for 802.11b wireless clients.
- **RTS/CTS Threshold**
A combination of wireless clients may experience difficulty allowing each other to communicate with the Gateway without interrupting each other’s communications. If this occurs, the RTS/CTS threshold may be set to a higher number to allow them each a longer period in which to communicate with the Gateway before the priority is switched to another wireless client wishing to transmit data.
- **Fragmentation Threshold**
The fragmentation threshold may be lowered to improve reliability in an excessively “noisy” wireless environment where changing channels does not provide significant enough improvement.

Note: If you wish to reset the options in the “Wireless Options Configuration” window, click Restore Default Values. The system responds by restoring all of the advanced features on this page.

- Click **Next**. The system responds with the “Wireless Wizard” window.

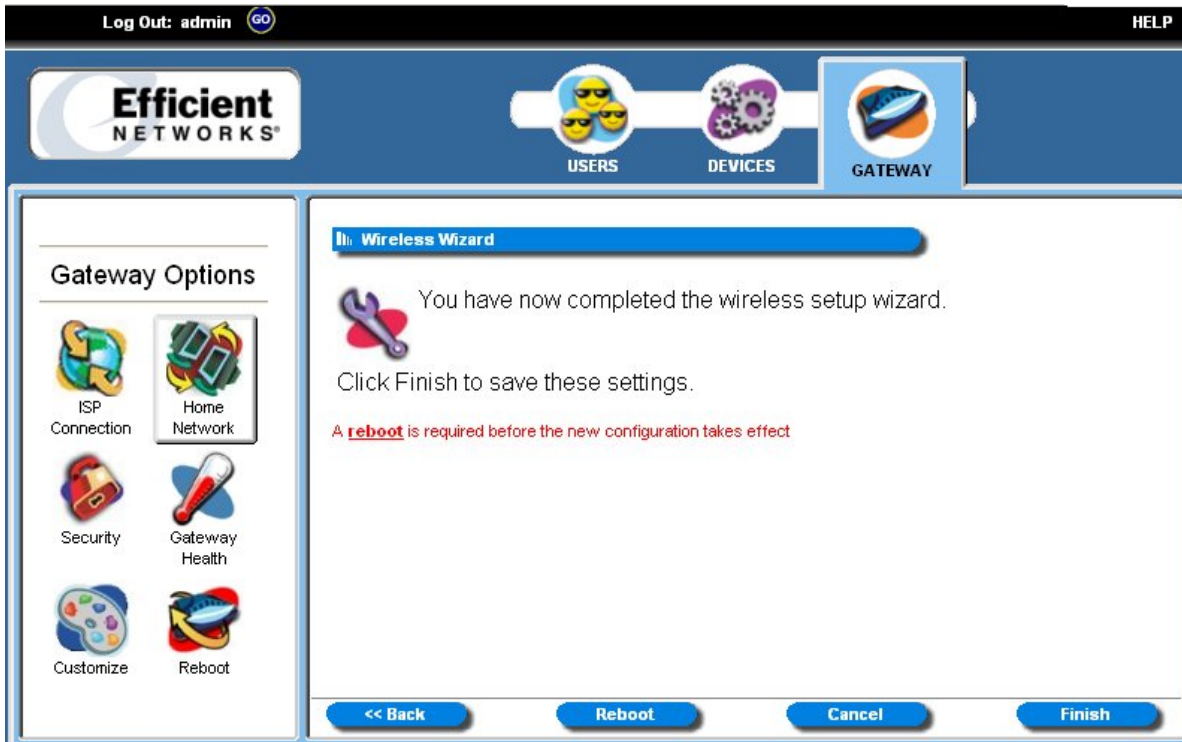


Figure 64. Wireless Wizard Window

- Click **Finish**.
- Click **Reboot** for your wireless configuration to take effect.

UPnP (Universal Plug and Play)

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

Click **Configure the Universal Plug and Play Settings** link to display the following window:

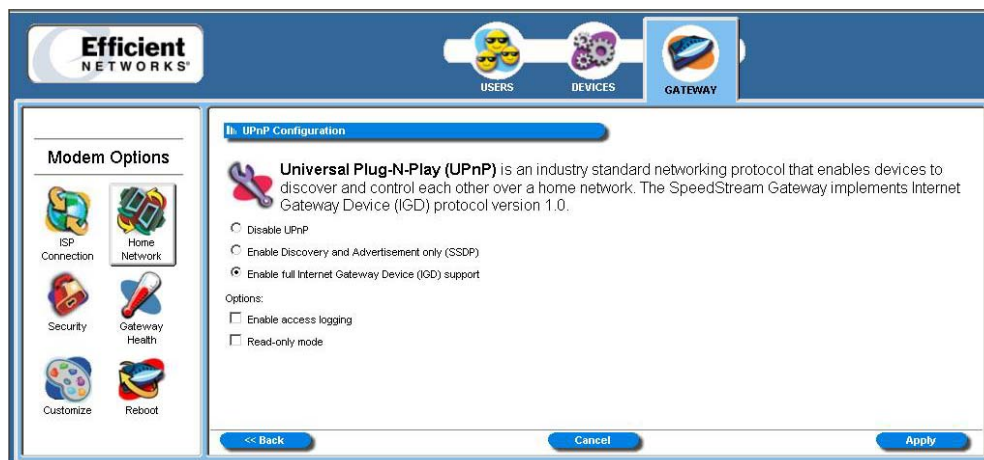


Figure 65: UPnP Configuration Screen

Three options are provided for UPnP:

- **Disable UPnP**
Prevents the Gateway from using the UPnP feature to communicate with other devices or your operating system. Also may be disabled if your operating system does not support UPnP.
- **Enable Discovery and advertisement only (SSDP)**
Only allows the Gateway to send information about new devices (hardware) detected. No information concerning software applications or services is transmitted. Note that UPnP must be enabled in your supported operating system to use this feature. See *About UPnP* below for more information on supported operating systems and enabling UPnP functionality.
- **Enable full Internet Gateway Device (IGD) support**
Allows the Gateway to communicate freely with computers on the network about new devices, software applications, and services as needed to ensure they are working with minimal manual configuration required. Note that UPnP must be enabled in your supported operating system to use this feature. See *About UPnP* below for more information on supported operating systems and enabling UPnP functionality.

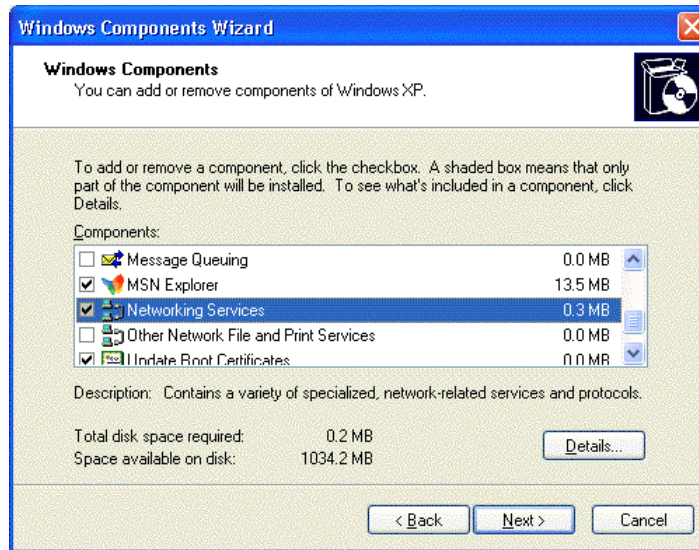
About UPnP

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.

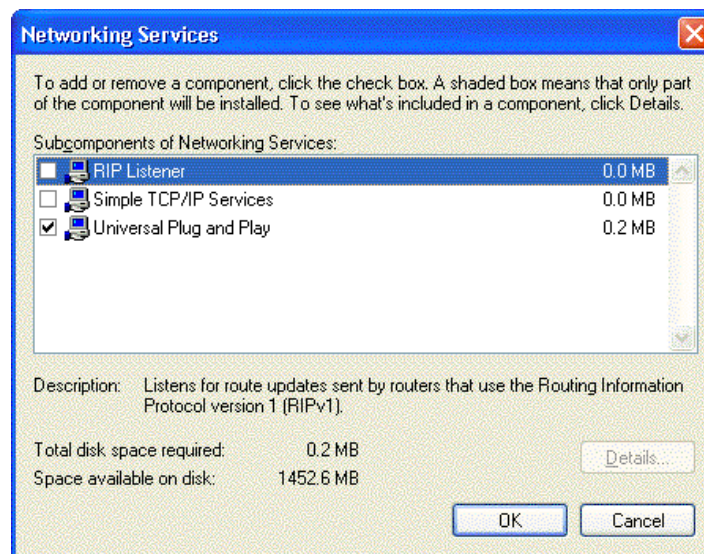
Follow the steps below for installing UPnP components.

1. Click on the **Start** menu, point to Control Panel, and click the **Control Panel** icon.

2. Select **Add or Remove Programs > Add/Remove Windows Components** to open the **Windows Components Wizard** dialog box.

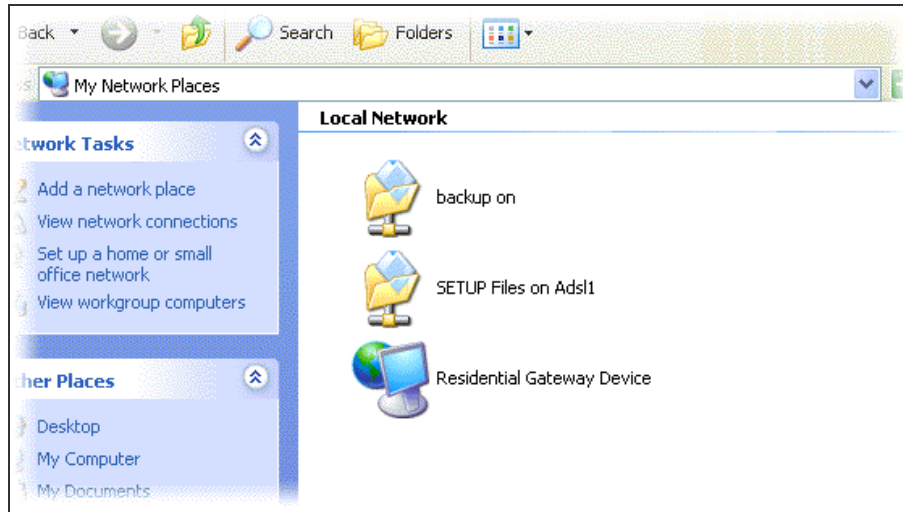


3. Select **Network Services** and click **Details**. Check the **Universal Plug and Play** check box.



4. Click **OK**. The system installs the UPnP components automatically.

5. After finishing the installation, go to My Network Places. You will find an icon (ex: Residential Gateway Device) for the UPnP function.



6. Double-click the icon. The Gateway will open another Web page for UPnP functions. Now, the NAT traversal function of UPnP will be available. The Gateway will create virtual servers automatically when it detects the computer running some Internet applications that require this configuration.

Consult your Windows operating system documentation for more information on UPnP, installation, and usage.

Security

Your gateway provides broad security measures against unwanted users. Security also allows for the configuration of the gateway firewall, administrator password, (NAT) Network Address Translation, and DMZ (Demilitarized Zone) configuration. A firewall is a system designed to prevent unauthorized access to or from a private network. The administrator password allows you to configure all of the gateway options. NAT is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. The hiding of internal addresses allows greater security for your network. DMZ allows a device on your gateway through your firewall. This feature is primarily used for gaming. The administrator logon allows you access to all of the security options while the gamer user allows access to the firewall options and address translation. The user logon does not allow you access to any of the security options.

To access security options,

1. Logon as the administrator.
2. Click **Gateway** in the toolbar.
3. Click **Security** in the left-navigation pane.
4. Please see the next section in this document titled *Firewall*.

Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. The firewall screen provides a listing of options to be enabled or disabled as well as links to configure the more complex details of each feature. **Note:** Clicking the “Configure” hyperlink next to an option for the firewall allows you to customize a particular setting.

1. From the “Security Settings” window, click **Firewall Settings**. The system responds with the "Firewall Settings" window.

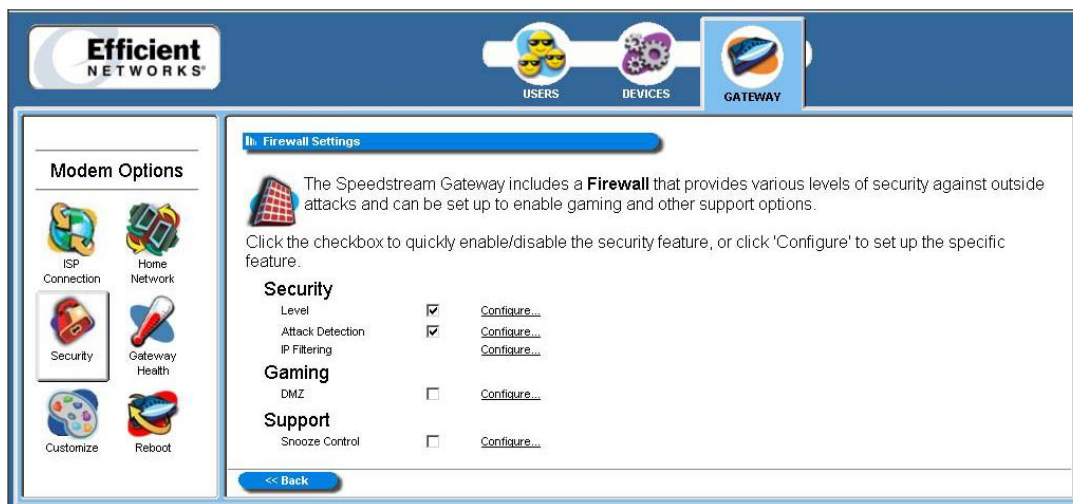


Figure 66: Firewall Settings Window

2. Select the checkboxes for all options you wish to use. For each option, click the link to verify or change configuration settings.
3. **Optionally**, click **Configure** next to any of the security, gaming, and support options for further configuration of the firewall.
4. Please see the next section in this document titled *Security Level*.

Security Level

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

To use the security level feature:

1. Select the "Level" checkbox.
2. Click the "Configure" hyperlink next to the "Level" heading.
3. Select one of the following options from the "Select Firewall Level" drop-down.
4. Select the firewall security level appropriate for your needs and click **Apply**. Available options are:
 - **Off:** No firewall protection. Data can move freely both in and out of the gateway.
 - **Low:** Provides basic firewall protection. Attack detection is enabled and only ports well known to the gateway can allow the flow of data.

- **High:** Provides maximum firewall protection. Only certain applications are allowed through the firewall or traffic that is already "in conversation" with an application from the host PC and host application. ICSA 3.0a Compliant.
- **Custom:** Set your own rules for firewall protection (For Advanced Users). This option is used with IP filtering to set customized rules for both inbound and outbound traffic.

5. Click **Apply**.

6. Please see the next section in this document titled *Attack Detection*.

Attack Detection

The SpeedStream Gateway provides protection against the most common hacker attacks that attempt to access your computer/network from the Internet. Enable this feature and select **Filter All** to provide maximum protection against this type of malicious intrusion. Intrusion attempts can also be logged to provide a record of attempts and their source (when available). Click **Apply** to save your settings.

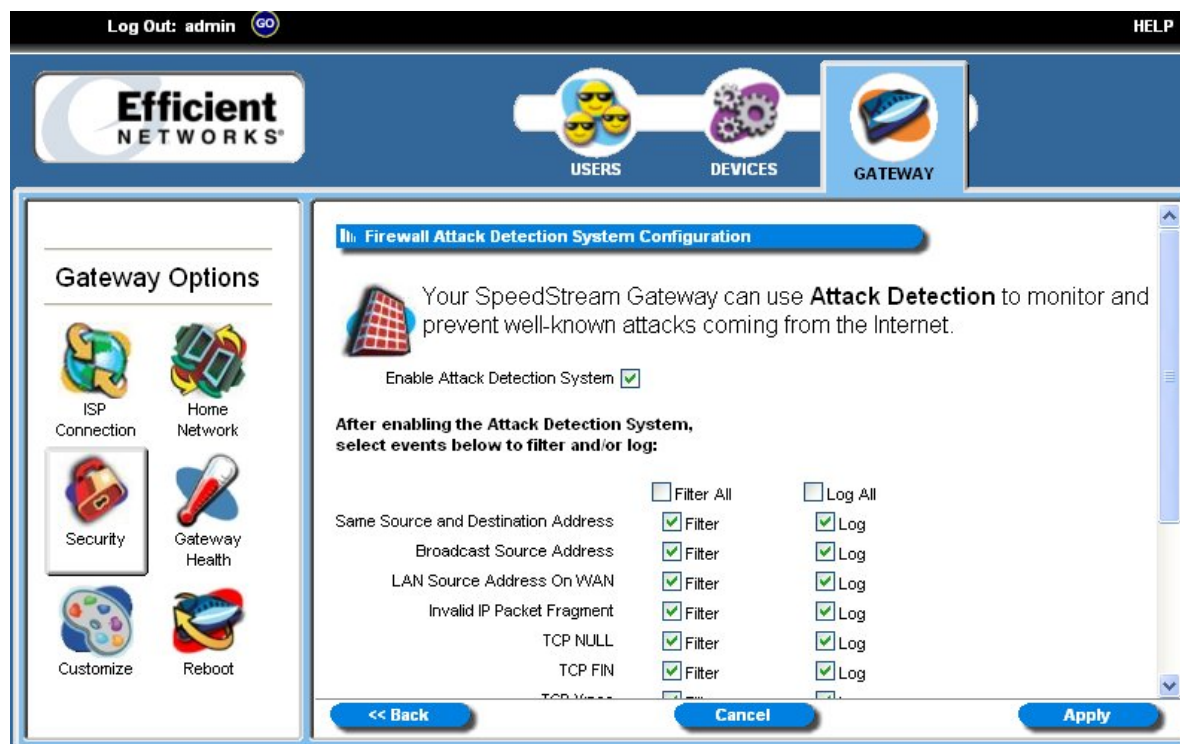


Figure 67. Firewall Attack Detection System Configuration

Intrusion/attack types to block and/or log may be selected individually for a custom configuration (for advanced users).

To use the attack detection feature:

1. Select the "Attack Detection" checkbox.
2. Click the "Configure" hyperlink next to the "Attack Detection" heading.

3. Select the checkboxes next to the corresponding option under the "After enabling the Attack Detection System, select events below to filter and/or log:" heading. **Note:** You can select the "Filter all" and "Log all" checkboxes to both select and log all options. Please see the descriptions below for all of the available options:
 - **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.
 - **Broadcast Source Address:** An outside device can send a ping to your gateway 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.
 - **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 gateway 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 of 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 gateway 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.
4. Click **Apply**.

IP Filtering

IP filtering options are only available if your Firewall Level setting is **Custom**. This method of firewall protection is recommended for advanced users only. Click the **Configuration** button to step through the IP Filter Configuration Wizard for Inbound and Outbound IP Filter Rules.

To use the IP filtering option:

1. Click the "Configure" hyperlink next to the "IP Filtering" heading.
2. Click **Add New IP Filter Rule**.
3. Type up to a five digit numeric value in the "Rule No" box.
4. Select either "Permit" or "Deny" from the "Access" drop-down. Select "Permit" to allow the rule and "Deny" to not allow the rule.
5. Select either "Inbound" or "Outbound" from the "Direction" drop-down. Inbound refers to data coming into the gateway, while outbound refers to data transmitted from the gateway.
6. **Optionally**, select the "Disable stateful inspection for packets matching this rule" option.
7. **Optionally**, select the "Create a log entry for packets matching this rule" option places an entry in the log file when packets match this rule.
8. Click **Next**.
9. Under the "Source" heading, select a network connection from the "Network Interface" drop-down.
10. 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 specified IP address of the source. Type the IP address and netmask in the boxes below this option.
11. Under the "Destination" heading, select a network connection from the "Network Interface" drop-down.
12. Select one of the following options:
13. Any IP address: Select this option if this rule applies to any IP address from the destination.
14. This IP address: Select this option if a rule applies to a specified IP address of the destination. Type the IP address and netmask in the boxes below this option.
15. Optionally, select the "or Host" checkbox to use your gateway netmask as the destination netmask.
16. Select one of the following options from the "Select by Name" drop-down:
17. TCP (Transmission Control Protocol): Provides reliable, sequenced, and unduplicated delivery of bytes to remote or local users.
18. UDP (User Datagram Protocol): Provides for the exchange of datagrams without acknowledgement or guaranteed delivery.
19. ICMP (Internet Control Message Protocol): A mechanism that provides for peer communication. The most commonly used application for this protocol is the PING command.

20. GRE (Generic Routing Encapsulation): A tunneling protocol that is used primarily for VPN (Virtual Private Networks).
21. Optionally, you can type a protocol number in the "Select by Number" box.
22. Click Next.
23. Select one of the following options from the "Source Port Operator" drop-down:
 - **any**: Any port is accepted.
 - **less than or equal to**: Less than or equal to a numeric value in the "Port 1" box.
 - **equal to**: Equal to the value in the "Port 1" box.
 - **greater than or equal to**: Greater than or equal to the value in the "Port 1" box.
 - **range**: A range of ports between the value of the entry in the "Port 1" box and the value in the "Port 2" box.
24. Select one of the following options from the "Destination Port Operator" drop-down:
 - **any**: Any port is accepted.
 - **less than or equal to**: Less than or equal to a numeric value in the "Port 1" box.
 - **equal to**: Equal to the value in the "Port 1" box.
 - **greater than or equal to**: Greater than or equal to the value in the "Port 1" box.
 - **range**: A range of ports between the value of the entry in the "Port 1" box and the value in the "Port2" box.
25. **Optionally**, select the "Check TCP syn packets" option if you wish this rule to prevent the blocking of synchronization packets for pre-existing sessions.
26. Click Next.
27. Click Finish.

To clone rules:

1. Click Clone IP Filter Level.
2. Select either "Low" or "High" from the "Select preconfigured firewall level for cloning" drop-down.
3. Click Apply. The system respond by copying either the high or low level hard-coded firewall options and copying or "cloning" them for additions or modifications.

DMZ

The gateway allows you to configure a DMZ (Demilitarized Zone) to allow for either a temporary or permanent bypassing of the firewall for network or Internet gaming. If the DMZ feature is enabled, you must select the computer to be used as the DMZ computer/host.

To configure the DMZ:

1. Log on as the administrator or gamer.

2. Click Gateway in the toolbar.
3. Click Security in the left-navigation pane.
4. Click **Firewall Settings**. The system responds with the “Firewall Settings” window.

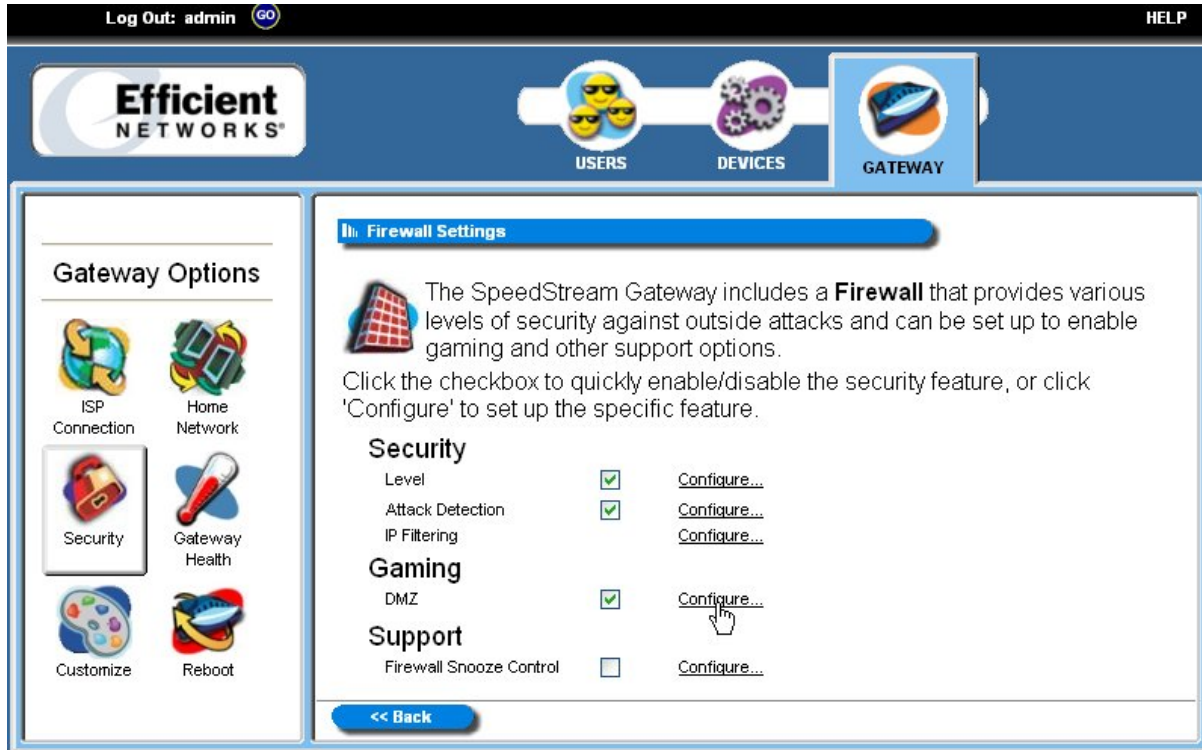


Figure 68. Firewall Settings Window with the DMZ Option Selected

5. Under the "Gaming" heading, select the "DMZ" checkbox.
6. Click the "Configure" hyperlink next to the "DMZ" checkbox.
7. Select one of the following 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 drop-down next to this field.
8. Select one of the following options:
 - **Make Settings Permanent:** The settings in step 3 are permanent unless changed by the administrator.
 - **Make Settings Last for:** The settings in step 3 are only enabled for the time (in minutes) entered in the box next to this option.
9. Click Apply.

Snooze Control

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

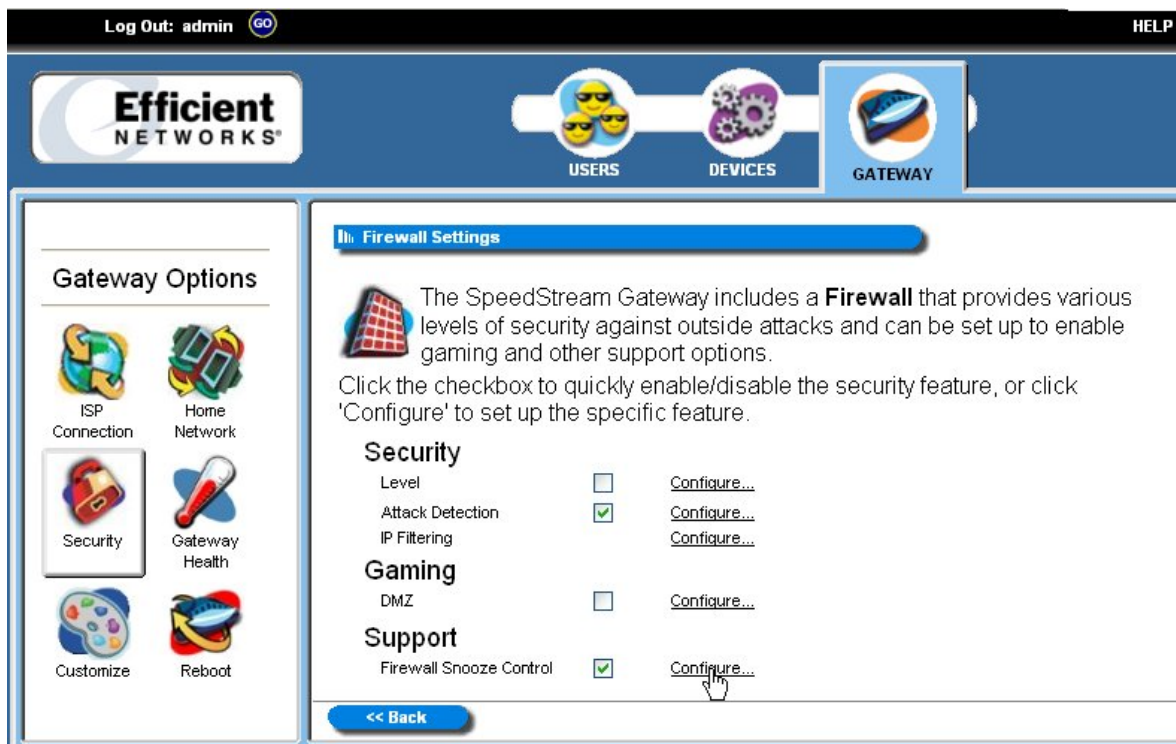


Figure 69. Firewall Settings Window with the Firewall Snooze Control Option Selected

To use the snooze control feature:

1. Under the "Support" heading, select the "Firewall Snooze Control " checkbox.
2. Click the "Configure" hyperlink next to the "Firewall Snooze Control" checkbox.
3. Select one of the following options:
 - **Disable Snooze:** This option disables all snooze control. In this mode, the firewall is not bypassed.
 - **Enable Snooze, and set the Snooze time interval to:** This option enables snooze and allows you to type a value in the box next to this option.
 - **Reset the Snooze time interval to:** This option allows you to enter a value to reset the time if you need a time extension for an open snooze session. For example, if a service technician is in your system and needs 5 more minutes, type 5 in the "Reset the Snooze time interval to" box.
5. Click **Apply**.

Administrator Password

You may change the admin password at any time if you have administrative rights to the gateway.

To change the admin password:

1. Log on as the administrator.
2. Click **Gateway** in the toolbar.
3. Click **Security** in the left-navigation pane.
4. Click **Admin Password**.
5. Type your admin username and password and click **OK**.
6. Make any changes to the admin username and password then click **Save Settings**.

Address Translation

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

To use the address translation feature:

1. Log on as the administrator.
2. Click Gateway in the toolbar.
3. Click Security in the left-navigation pane.
4. Click Address Translation.
5. Select an interface from the "Select Interface" drop-down.
6. Select one of the following options:
 - **Use no address translation:** Address translation is disabled.
 - **Address Translation (NAT):** Internet standard that allows a LAN to use one set of IP addresses for internal traffic and a second set for external traffic.
 - **Port By-Pass (NAPT):** Only TCP, UDP, and ICMP protocols support NAPT. NAPT allows many devices connected to the gateway access to the Internet while masking the identification of the internal IP addresses.

To use address translation with NAT:

1. Click the "Configure" hyperlink next to the "Address Translation (NAT)" option.
2. Type the IP address of the one computer in your network that you wish to have access to the Internet.
Note: NAT features only support one machine on the Internet.
3. Click **Apply**.

To use address translation with NATP:

1. Click the "Configure" hyperlink next to the "Port-Bypass (NAPT)" option.
2. Click the option(s) of your choice from the list under the "Available Applications" heading. Once clicked, these applications appear under the "Enabled Applications" heading indicating they are now active. NATP is used to allow multiple users access to Internet applications while masking their IP addresses from outside users.
3. Optionally, click the "Add a custom bypass entry" hyperlink. This option allows you to configure special port access to the Internet.
4. Under the "Add/Edit Entry" heading, select one of the following options from the "Select service by name" drop-down:
 - **Telnet:** Telnet is a program that allows you to connect to other computers over the Internet. This option uses port 23.
 - **FTP (File Transfer Protocol):** FTP is used to transfer files in both ASCII and Binary format between local and remote devices. This option uses port 21.
 - **HTTP (Hyper Text Transfer Protocol):** HTTP is the standard method of transferring all types of information over the Internet. This option uses port 80.
 - **SNMP (Signaling Network Management Protocol):** SNMP is a protocol used by network management applications to help manage a network. This option uses port 161.
 - **SMTP: (Simple Mail Transfer Protocol):** SMTP is used for sending email between servers. This port uses port 25.
 - **PPTP (Point-to-Point Tunneling Protocol):** PPTP is a protocol that allows VPN (Virtual Private Network) applications. This option uses port 1723.
 - **Domain:** Domain is used for DNS options. This option uses port 53.
5. Optionally, instead of selecting a service in step 4, you can select a protocol and specify port numbers. Select one of the following options from the "Select protocol" drop-down:
 - **TCP: (Transmission Control Protocol)** Provides reliable, sequenced, and unduplicated delivery of bytes to a remote or local user.
 - **UDP: (User Datagram Protocol)** A connectionless mode protocol that provides the delivery of packets to a remote or local user.
 - **ICMP: (Internet Control Message Protocol)** A method by which IP software on a host or gateway can communicate to pass information to other machines.
 - **GRE: (Generic Routing Encapsulation)** This protocol is used to provide tunneling for a VPN connection.
 - If you are using the protocol option in step 5, type the range of UDP or TCP ports in the boxes next to the "and TCP/UDP port(s)" heading.
6. Select one of the following options:
 - **Redirect selected protocol/service to this router:** The protocol or service that you select is directed to your gateway.

- **Redirect selected protocol/service to IP Address:** The protocol or service that you select is directed to an IP address on your LAN that you type in the box next to this field.

7. Click **Apply**.

Gateway Health

The gateway health options are used to gauge the various measures of gateway's health. These options include: statistics, update firmware, diagnostics, and reboot. The statistics option is used to measure the Internet stats, home networking stats, security stats, and the different gateway log files. The update firmware option is used to update the firmware of your gateway through the Internet or from a device connected to your gateway. The diagnostics option runs a diagnostic program against a selected connection on your gateway. The reboot option is used to reboot the system and to reset all gateway factory defaults. The administrator logon allows you access to all of the gateway health options, while a user logon allows only access to the statistics and reboot options.

To use the gateway options features:

1. Logon as the administrator or user depending on which options you wish to use.
2. Click **Gateway** in the toolbar.
3. Click **Gateway Health** in the left-navigation pane. The system responds with the "Gateway Health Options" window.
4. Please see the next section in this document titled *Statistics*.

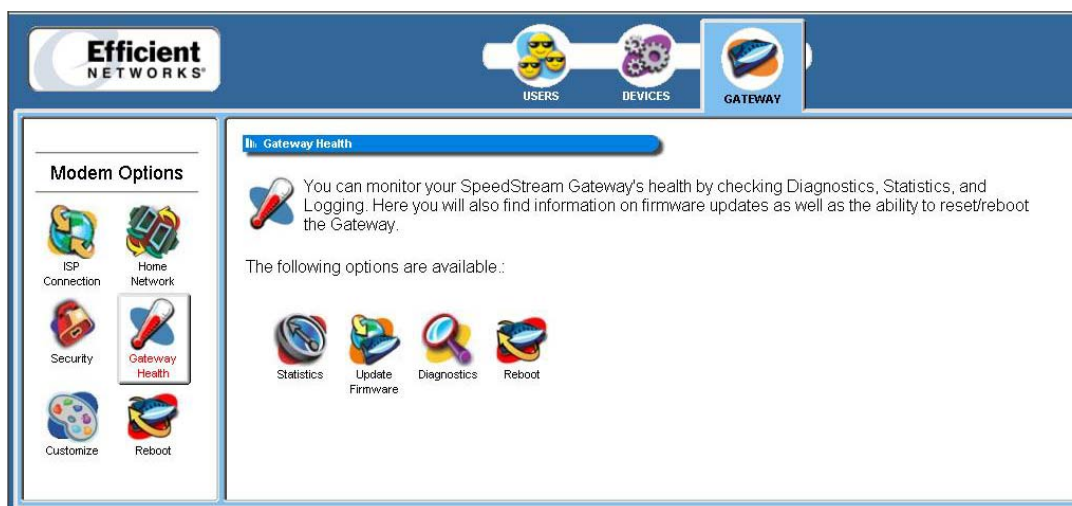


Figure 70: Gateway Health Window

Statistics

Statistics are displayed for your Internet connection, Network status, Security, and the Gateway system log. Click the hyperlink of your choice for the type of statistics you wish to view.

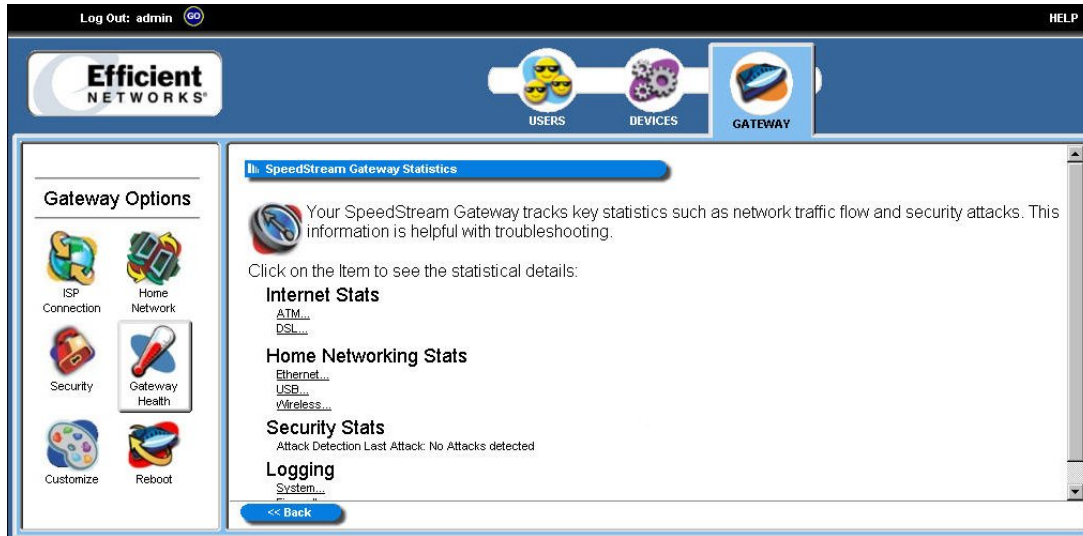


Figure 71: Statistics Window

Internet Stats

These statistics are commonly used by your Internet Service provider to diagnose service-related issues. The following statistics related to you Internet connection are displayed:

Click the “ATM” hyperlink under the “Internet Stats” heading to display the ATM connection status, uptime, and transmit/receive data, VPI/VCI and related data for each circuit.

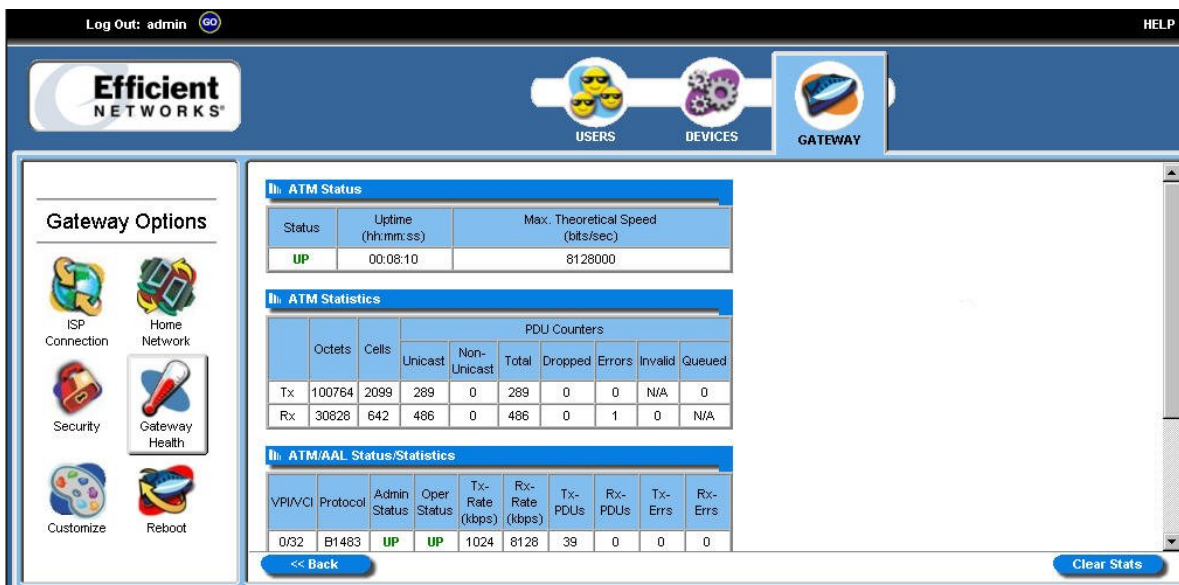


Figure 72. ATM Statistics

Click the “DSL” hyperlink under the “Internet Stats” heading to display information about your DSL connection.

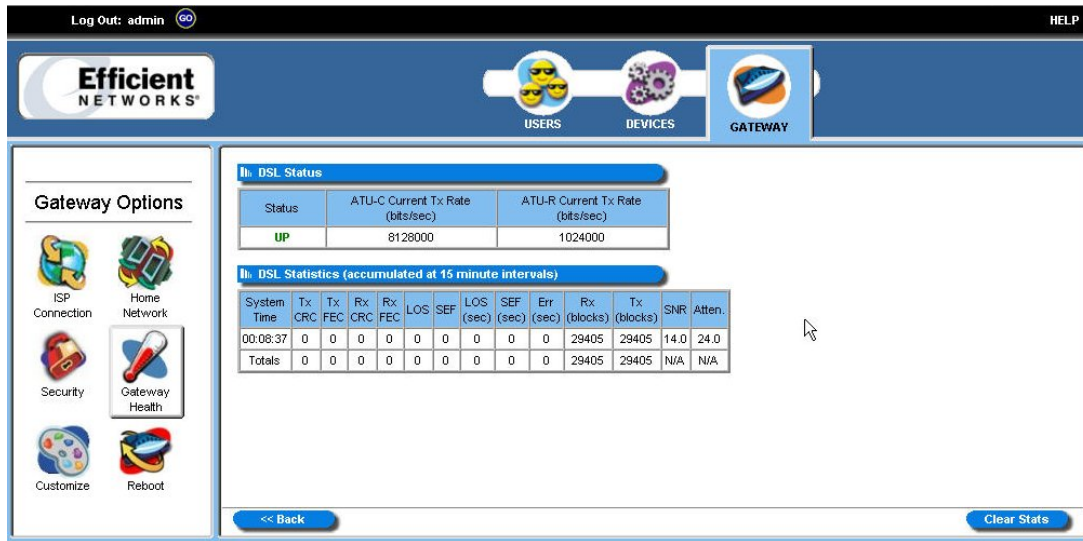


Figure 73. DSL Statistics

Home Networking Stats

These statistics are helpful when used to troubleshoot issues on your home network. These statistics are displayed for each physical interface connected to the Gateway. They are separated into Ethernet and USB statistics. Select the link for the interface you are interested in viewing. Pay special attention to the status (up or down) reported for each Ethernet port or the USB port (when used) to verify that each cable is connected properly and detected by the Gateway.

Security Stats

Security breach attempts are shown for any firewall rules or attack detection services you have defined on the Firewall customization window.

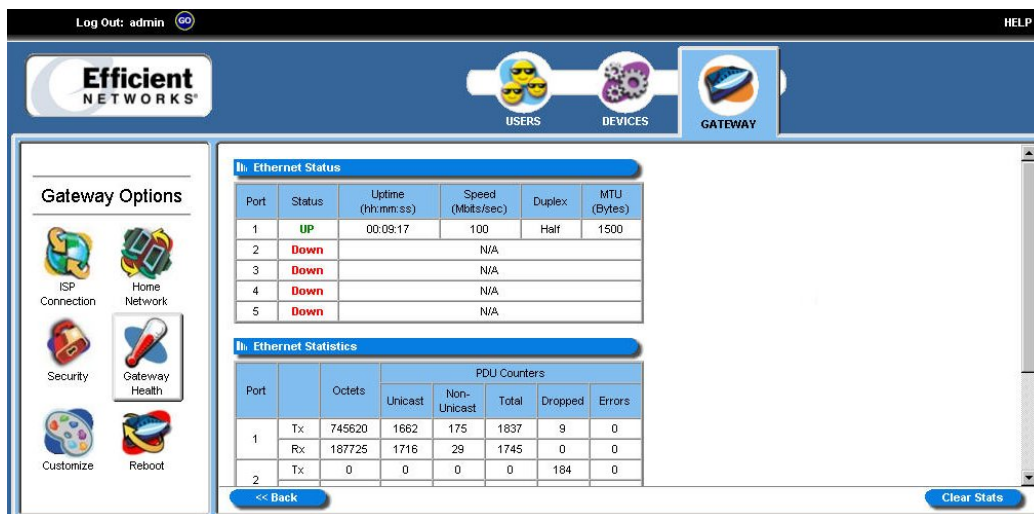


Figure 74. Security Statistics

Logging

Extensive activity logs are provided for advanced troubleshooting and administrative use. The following types of logs are available:

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

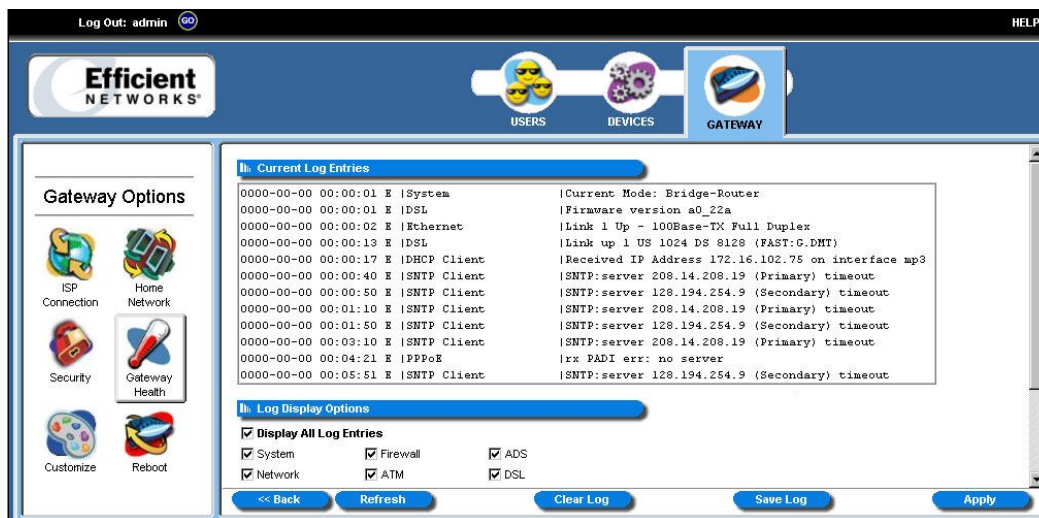


Figure 75. System Log(s)

- Firewall**
 Displays attempts (both failures and successes) to access data through the firewall. Firewall log entries are defined on the **Firewall Settings Configuration** screen found under the **Security** menu.
- User Access**
 Displays activity related to users logging in or out of the Gateway. Records both successful and unsuccessful attempts by username.

Update Firmware

Note: This option may not be available on your Gateway. If available, you must be logged in as the Gateway Administrator to access the utility.

The firmware (software) on the Gateway can be upgraded using your Web browser. Click in the table cell of one of the following options:

- Recommended:** Select **Remote** to allow the gateway to search the Internet for the appropriate upgrade file.
- Alternate:** Select **Local** to browse to a location on your network and select the upgrade file. You must first download the upgrade file to your computer then select the file from the file-browsing window to begin the upgrade process.

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

Diagnostics

The Gateway provides diagnostic tests and data for each interface. This data is commonly requested by technical support to assist in troubleshooting.

To use the diagnostic option:

1. Select a connection to test from the “Connection to Test” drop-down.
2. Click **Run Diagnostics**. The system responds by displaying the results in the different tables. **Note:** Pay special attention to any tests that report a failing condition and check the connections for these interfaces before running the diagnostics again.

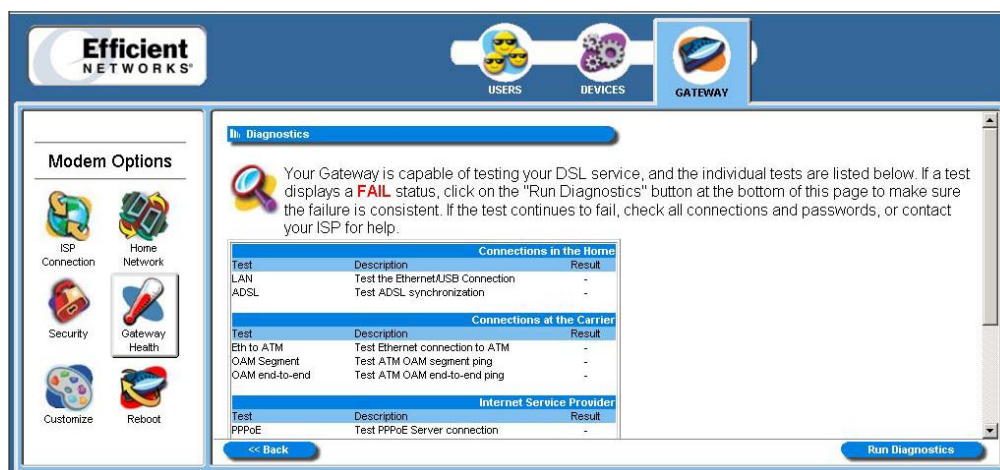


Figure 76: Diagnostics Window

The example below illustrates a successful diagnostic process:

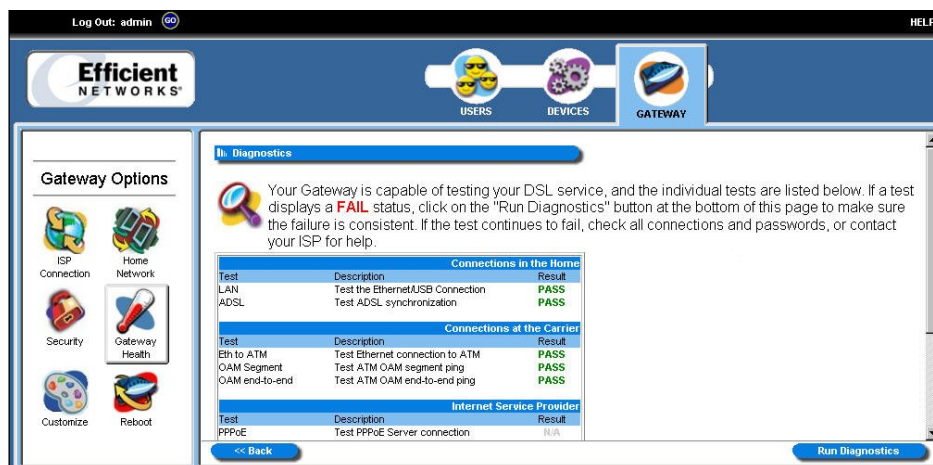


Figure 77. Successful Diagnostic Process

The example below displays a diagnostic result with failures detected:

The screenshot shows the 'Diagnostics' page in the Efficient Networks Gateway interface. The page title is 'Diagnostics'. Below the title, there is a paragraph explaining that the gateway can test DSL service and that a 'FAIL' status indicates a problem. A 'Run Diagnostics' button is located at the bottom right. The main content area contains three tables of test results:

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

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

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

Navigation buttons include '<< Back' and 'Run Diagnostics'.

Figure 78. Diagnostic Process with Failures

Customize

Several options are available for you to customize the Gateway's display. Select the icon for the option you wish to configure. The customization options are explained below:

The screenshot shows the 'Customized Settings' page in the Efficient Networks Gateway interface. The page title is 'Customized Settings'. Below the title, there is a paragraph explaining that the gateway allows users to choose a background color, change the language, and modify time zone settings. A 'Please choose which area you would like to customize:' prompt is followed by three icons representing 'Color Palette', 'Language', and 'Time Zone'.

Figure 79: Customized Settings Screen (Administrator Log on)

Color Palette

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

To use the color palette option:

1. From the “Customized Settings” window, click **Color Palette**. The system responds with the “Customized Colors” window.



Figure 80. Customized Color Window

2. Using the color drop-downs from the different display options, select the colors you wish to use in the system.
3. **Optionally**, type a numeric color value in the box next to the particular color drop-down. The number is based on RGB (Red Green Blue) values. For example, the color red is represented by a value of ff0000, green is represented by a value of 00ff00, and blue is represented by a value of 0000ff. **Note:** If you are entering a numeric value for the color, ensure that the “#” is in front of your numeric value.
4. **Optionally**, click Reset System Default Colors if you want to reset all system color schemes to the factory settings.
5. Click **Apply**.

Language

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

- Select your desired language and click **Apply**.

Time Zone

Configure the Time Client parameters to automatically synchronize the Gateway's internal date and time settings with those of your selected time zone. This time will be used to control time restrictions you may set for users as well as in entries in the system log.

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

To use the time zone option:

1. From the "Customized Settings" window, click **Time Zone**. The system responds with the "Configure Time Zone" window.

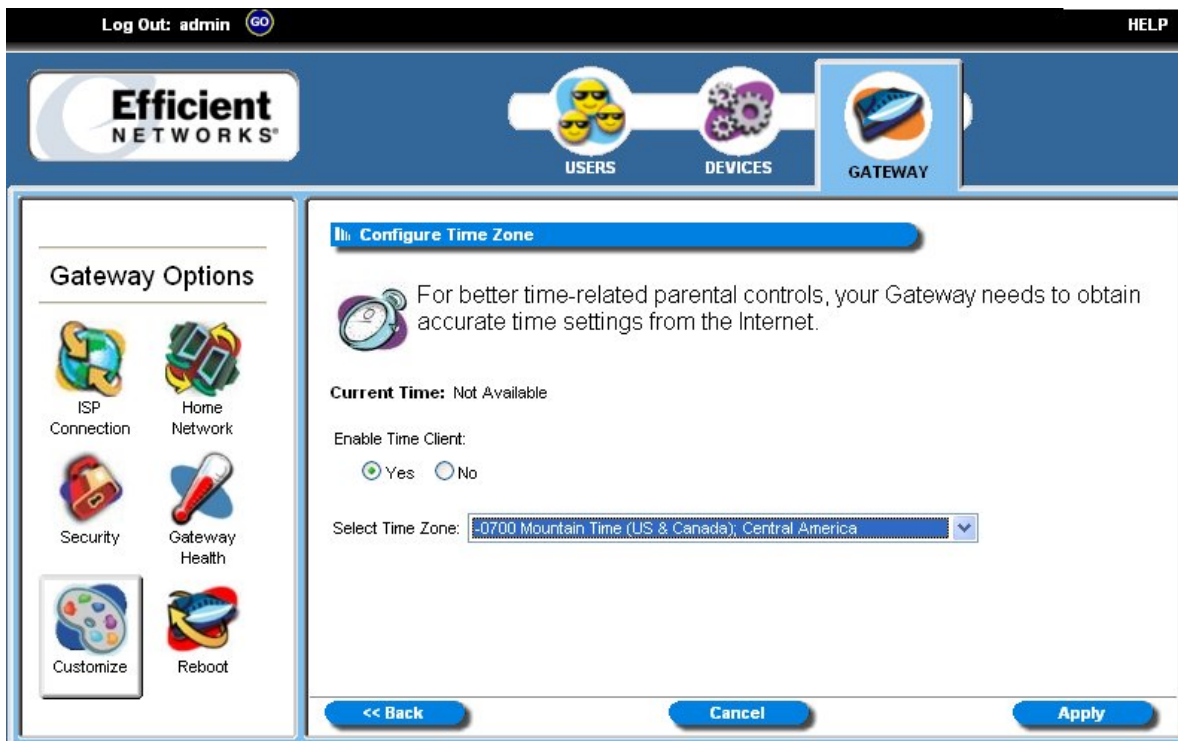


Figure 81. Configure Time Zone Window (Customize Option)

2. Select the "Yes" option from under the "Enable Time Client" heading.
3. Click a time zone from the "Select Time Zone" drop-down.
4. Click **Apply**.

Reboot / Reset

The **Reboot** screen offers two options: reboot and reset. Please see the section below for more information.

Reboot

Reboot should be used when the Gateway needs to be restarted. The Gateway can also be rebooted using the power switch on the rear panel of the Gateway. Note: This option can be used at either the user or administrator level.

To use the reboot option:

1. Click the **Reboot** icon. The system responds with the “System Reboot” window. Note: If you log on as the administrator, leave the “Reset to Factory Defaults” option de-selected for this operation to be successful.

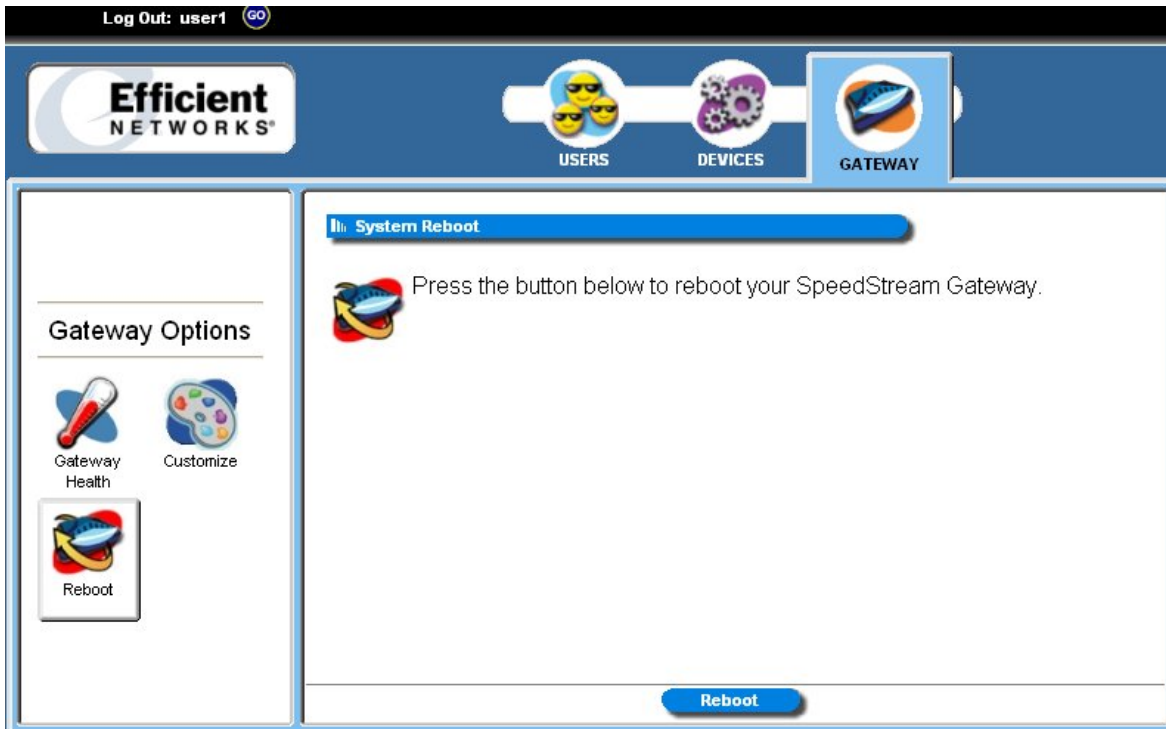


Figure 82. System Reboot Window (User Log on)

2. Click **Reboot**.

Reset

Reset should be used when you find it necessary to recover the factory default settings. This may be necessary when a custom configuration did not go as planned, when a new configuration is desired, or when the Gateway does not appear to be working properly. **Important:** This option resets all custom settings, users, and passwords on your gateway. **Note:** You must be logged on as the administrator to use this option.

To use the reset option:

1. Click the **Reboot** icon. The system responds with the “System Reboot” window.

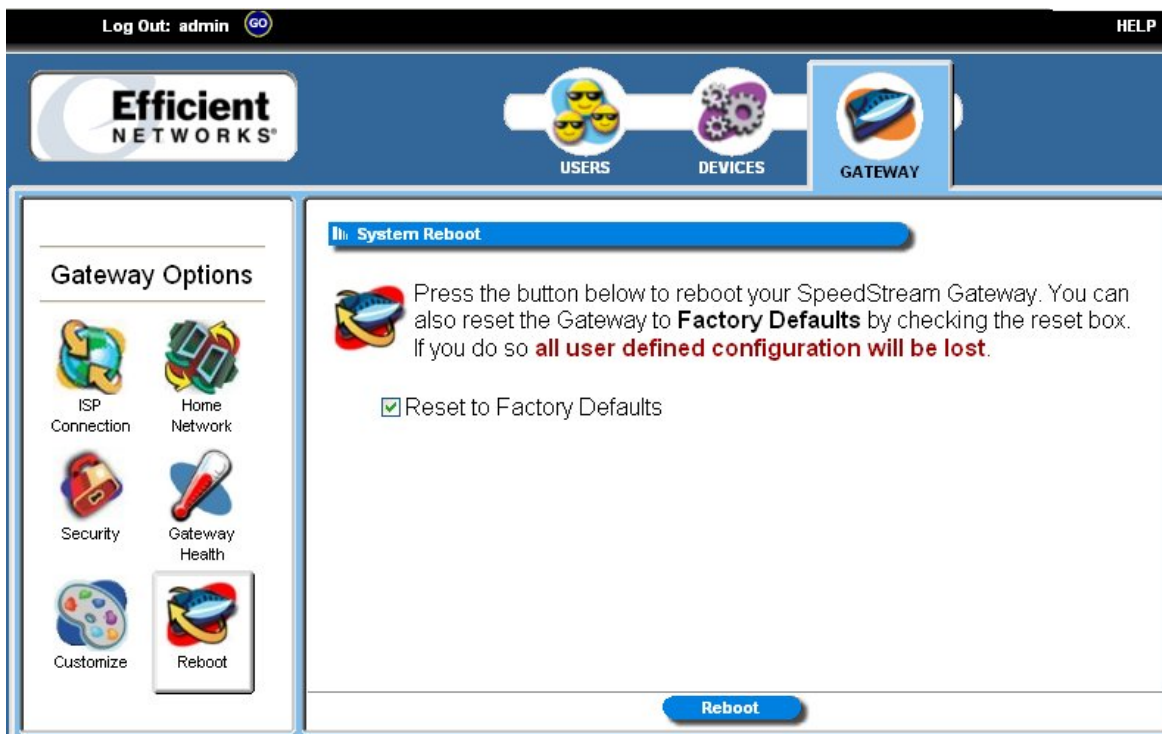


Figure 83. System Reboot Window (Reset)

2. Click **Reset to Factory Options**.
3. Type your administrator user ID and password.
4. Click **OK**.
5. The gateway begins a 45 second countdown to reset.

Appendix A

Troubleshooting



Overview

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

General Issues

Problem 1: Can't connect to the Gateway to configure it.

Solution: Check the following:

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

Internet Access

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

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

- Verify that other computers work. If they do, ensure that your computer's IP settings are correct. *Refer to Chapter 3- Operating System Configuration.* If using a fixed (static) IP address, check the network mask, default Gateway and DNS settings as well as the IP address.
- If the computers are configured correctly, but still not working, check the Gateway. Ensure that it is connected and on. Connect to it and check its settings. (If you cannot connect to it, check the Ethernet and power connections.)

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

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

- If you are running a supported Windows operating system, ensure that the UPnP feature is enabled. Refer to *UPnP (Universal Plug and Play)* in Chapter 5 for more information on this feature.
- If this does not solve the problem or your operating system does not support UPnP you can use the *DMZ* function. This should work with almost every application, but:
 - It is a security risk, since the firewall is disabled for the *DMZ* computer.
 - Only one (1) computer can use this feature.
- A third option is to use the “Firewall Snooze Control” feature to temporarily disable the firewall to allow the application to function unimpeded. See “*Snooze Control*” in Chapter 5 for more information on this feature.

Contacting Technical Support

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

- Internet Service Provider and service type (DSL, cable)
- Product model number (SpeedStream SS6000 Series)
- Date of purchase or installation
- Description of problem

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

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

Appendix B

Specifications



Media Interface:	<p>RJ-11 DSL WAN connection</p> <p>(5) 10/100Base-T RJ-45 Ethernet LAN connections (Auto-MDI/MDI-X)</p> <p>USB Type B connection</p> <p>DB-9 RS-232 Serial console port</p>
Diagnostic LEDs:	Power, Status, Link and Activity for DSL, Ethernet, USB, and Wireless
Management:	<p>Intuitive, Web-based management</p> <p>Comprehensive hardware diagnostics</p> <p>SNMPv1 support</p> <p>UPnP IGD-NAT traversal support</p> <p>XML Management Scheme, DSL Forum 2002-281</p>
Security:	<p>PAP (RFC 1334), CHAP (RFC 1994)</p> <p>Password Authentication</p> <p>Access Control list</p> <p>Stateful Inspection Firewall with Denial of Service (DoS) protection</p> <p>Pre-configured firewall levels for ease of use with “Custom” level for advanced users</p> <p>Filter on source and/or destination IP address</p> <p>Filter on transport protocol and/or port number</p> <p>Firewall logging with Network Time Protocol support and Syslog support</p> <p>DMZ support and Firewall “Snooze” feature</p> <p>Content filtering</p> <p>ICSA compliancy mode</p>
Standards Compliance:	<p>IEEE 802.1d, 802.11g, 802.3, and 802.3u</p> <p>USB 1.1</p> <p>T1.413 issue 2</p> <p>G.992.1 (G.DMT)</p> <p>G.992.2 (G.Lite)</p>

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

Efficient Networks

4849 Alpha Road

Dallas, TX 75244 USA

+1 (972) 852-1000 Tel

+1 (972) 852-1001 Fax

support@efficient.com

<http://www.support.efficient.com>