

Efficient Networks Business Class

5800 Series

Business Class Router
User Reference Guide



Efficient
NETWORKS®

222-00974-01

Efficient Networks and SpeedStream are registered trademarks, and the Efficient Networks logo is a trademark of Efficient Networks, Inc. All other names may be trademarks, service marks or registered trademarks held by their respective companies. This document is for information purposes only. Efficient Networks is not responsible for errors or omissions herein. Efficient reserves the right to make changes to product specifications without notice.

Efficient Networks, Inc. – End User Software License and 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 AND SOFTWARE IN ITS ORIGINAL PACKAGING TO THE 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 premise equipment ("Hardware") and the limited warranty that EFFICIENT provides on its Software and Hardware. EFFICIENT reserves any right not expressly granted to the End User.

Software License

The Software is protected by copyright laws and international copyright treaties. The Software is licensed and not sold to you. The definition of Software includes, but is not limited to, system and operating software marketed by Efficient, including firmware, embedded software, software provided on media, downloadable software, software for configurable or programmable logic elements, and all Efficient maintenance and diagnostic tools associated with the above-mentioned software. Accordingly, while you own the media (such as CD ROM or floppy disk) on which the Software is recorded, EFFICIENT or its licensors retains ownership of the Software itself.

1. **Grant of License.** You may install and use one (and only one) copy of the Software in conjunction with the EFFICIENT provided Hardware. You may make backup copies of the system configuration as required. 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 Assurances.** 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 or its licensors.
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 return the Software and all copies thereof.
8. **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 or its licensors.

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 three years 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 (90) 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 network. 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 systems or network.
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, whichever is longer.
4. **Warranty Procedures.** If a problem develops during the limited warranty period, the end user shall follow the procedure outlined below:
 - A. Prior to returning a product under this warranty, the end user must first call 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 or defective component, 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 phone 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 not consider the warranty voided, if: (1) the seal or serial number on the Product have been tampered with or (2) 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 at a fixed fee. Please contact EFFICIENT at the numbers provided above to determine the current out of warranty repair rates. 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 OTHER DAMAGES.** TO THE FULL EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EFFICIENT OR ITS LICENSORS 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 OR IT'S LICENSOR'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 insure 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 a 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

Installation	1-1
Introduction	1-1
Installation Requirements	1-1
PC Requirements	1-1
Network Service Provider Requirements.....	1-1
Package Contents	1-2
Connecting Your Router	1-3
Configuring Your Computer	1-4
Administration Login	1-5
Easy Setup.....	2-1
Router Information Screen.....	2-1
Easy Setup	2-2
Wide Area Network Configuration	2-2
Point-to-Point Protocol over ATM	2-4
Point-to-Point Protocol over Ethernet over PPPoA.....	2-6
Point-to-Point over Ethernet over RFC 1483	2-8
RFC 1483 Networking	2-10
RFC 1483 MAC Encapsulated Routing	2-12
Dynamic Host Configuration Protocol.....	2-14
Local Area Network Configuration	2-16
Additional Features.....	3-1
Access Control.....	3-2
Feature Activation	3-4
Setting The Date and Time	3-6
Set DHCP	3-8
NAT Settings.....	3-10
Set Firewall	3-12
Dial Backup.....	3-14
IKE/IPSec Configuration	3-16
IKE/IPSec Setup	3-18
Advanced IKE/IPSec Setup	3-20
IKE Peer Definition	3-22
IKE Proposal Definition.....	3-24
IKE IPSec Proposal Definition	3-26
IKE IPSec Policy Definition	3-28
Command Line Interface.....	3-30
Frequently Asked Questions	4-1
Product Specifications	5-1
Front Panel	5-1
5800 Series Back Panel	5-3
Hardware Specifications	5-4
Modem Specifications.....	5-5
Software Specifications.....	5-6
Safety and Certifications	A-1

Support B-1

Chapter 1

Installation

Introduction

This User Reference Guide covers basic installation and setup of the 5800 Series Business Class Routers including:

- 5851 Symmetric Digital Subscriber Line router (SDSL)
- 5861 Asymmetric DSL / Discrete Multi Tone router (DMT)
- 5865 Asymmetric DSL / DMT (international) router
- 5871 Integrated Services Digital Network DSL router (IDSL)

Installation Requirements

PC Requirements

- CD-ROM Drive
- Ethernet network interface card
- TCP/IP network protocol installed
- Web browser
- Terminal emulation software if you want to configure your router via your computer's serial port before placing it into service on a network.

Network Service Provider Requirements

Your Network Service Provider should provide the following:

- DNS address

- One or more LAN IP addresses and a subnet mask
- Protocol to use, from one of the following:
 - PPP (Point-to-Point Protocol), with a user name and password
 - PPPoE (PPP over Ethernet)
 - RFC 1483 (SNAP Encapsulation)
 - RFC 1483 MER (MAC Encapsulated Routing, requiring a WAN gateway address)
 - VCI (PVC) numbers
- Network options:
 - Bridging
 - IP Routing (requires a WAN IP address and subnet mask)

Package Contents

Your package should contain the items listed below. If you determine anything to be damaged or missing, please contact the dealer from whom the equipment was purchased.

- One Efficient Networks 5800 Series Business Class Router
- One Efficient Networks Documentation Kit
- One AC power supply
- One Ethernet 10Base-T cable, RJ-45, red label (straight through)
- One Ethernet 10Base-T cable, RJ-45, yellow label (crossover)
- One RJ-45 to DB-9 serial port adapter (console)
- Customer Release Notes with the latest information

Connecting Your Router

1. Place your router in a location where it will be well ventilated. Do not stack it with other devices or place it on carpet.
2. Connect your PC directly to any of the router's four Ethernet ports, using one of the red straight-through cables. You may also connect one to seven additional Ethernet devices to the router's built-in Ethernet hub.
3. Connect your router to the DSL jack using the remaining Ethernet 10Base-T, RJ-45 cable.
4. Connect the router to an AC power outlet using the power cord.

The following diagram shows an Efficient Networks 5800 Series Business Class Router when fully connected:

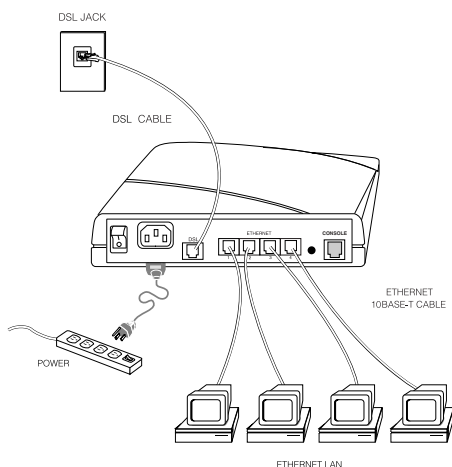


Figure 1-1: 5800 Series Router Fully Connected



CAUTION:

To reduce the risk of fire, use only no. 26 AWG or smaller guage telecommunication cord to connect the DSL port on your router a DSL telephone jack.

Configuring Your Computer

1. Configure the TCP/IP protocol stack on your computer to obtain an address automatically from the router. To do so with a PC running Windows 9x or NT, select **Start > Settings > Control Panel >** and click on **Network**.
2. Select the **Configuration** tab at the top of the dialog. Users with Windows NT select the **Protocols** tab.
3. From the list of network components, select **TCP/IP**.
4. Click on the **Properties** button.
5. Select the **IP Address** tab.
6. Ensure that “Obtain an IP Address Automatically” is selected. Users of Windows NT should select “Obtain an IP Address from a DHCP server”.
7. Click **OK** as needed to confirm your settings, and reboot your computer.

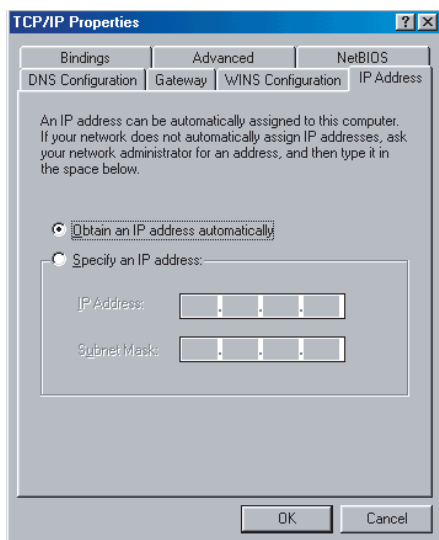


Figure 1-2: MS Windows TCP/IP Properties Dialog

Administration Login

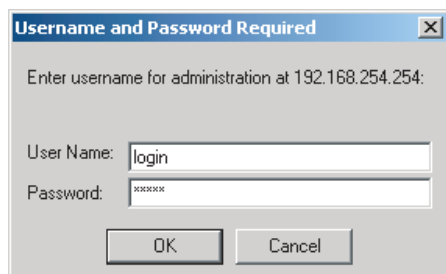
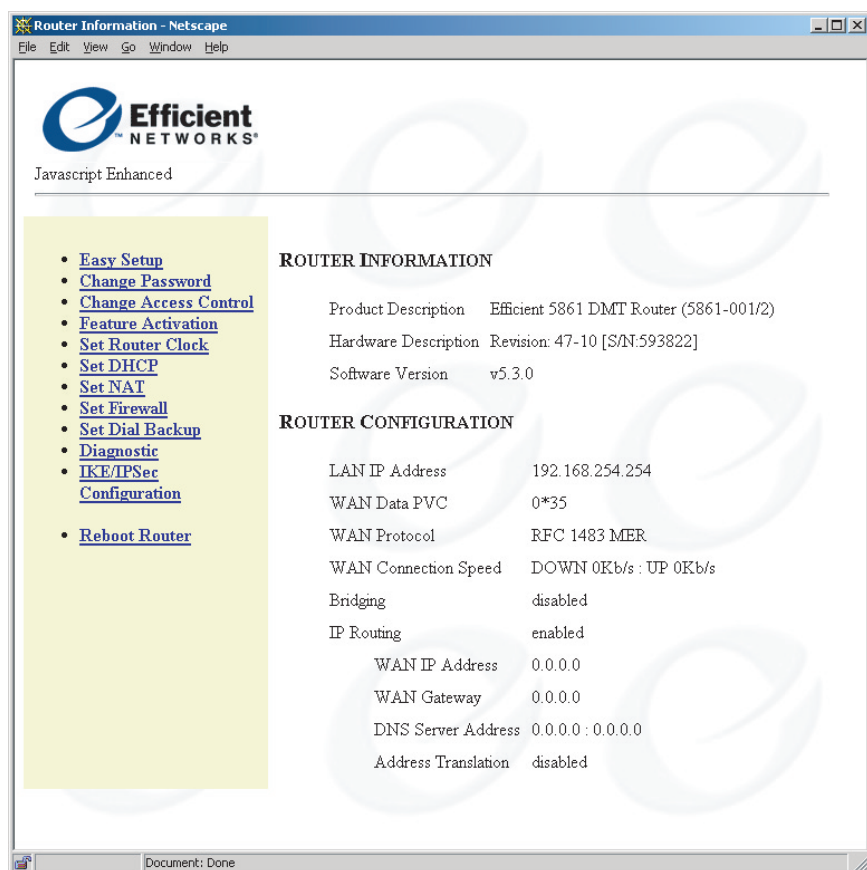


Figure 1-3: Administration Login Dialog

1. Using your web browser, enter the following default router address into the address field of your browser: `http://192.168.254.254/`
2. At the login prompt, make the following entries:
User Name: `login`
Password: `admin`
3. After you have logged into your router, a dialog will appear, prompting you to change your password. It is a security risk to leave the password set to the factory default. Therefore, changing the password is strongly recommended. To change the password, click on OK at the prompt.



Figure 1-4: Change Password Prompt

**Figure 1-5: Router Information Screen**

Chapter 2

Easy Setup

Router Information Screen

The first screen in the Web User Interface is the Router Configuration screen. This screen displays basic router information and router configuration settings. It also provides links to other router setup and control forms. On the Router Configuration screen, the following information is presented:

- **Router Information** - Including the model number, software version number and options that have been enabled.
- **Router Configuration** - Displays router configuration details such as LAN IP address, WAN data and voice PVC (ATM) or DLCI (frame relay), WAN protocol and WAN network settings.

A menu of links is on the left side of the Router Configuration screen. This menu links to forms that provide settings for your router. Easy Setup is the first set of forms on the menu.

Click on the **Easy Setup** link to begin a basic configuration of your router.

Easy Setup

Wide Area Network Configuration

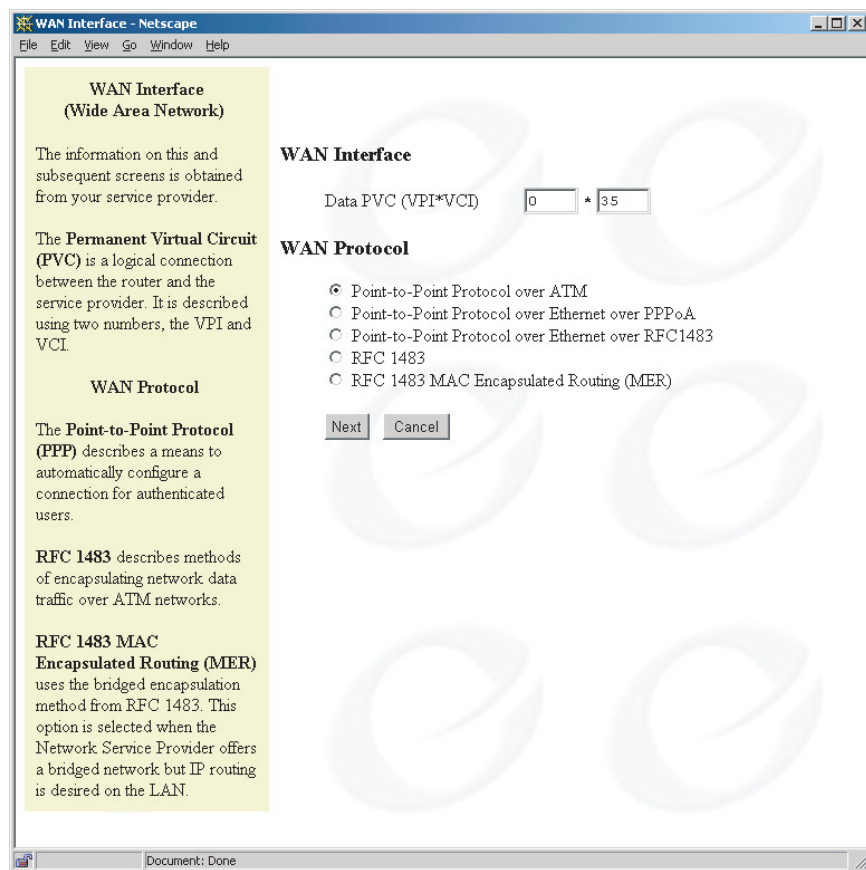


Figure 2-1: WAN Interface Screen

The first Easy Setup screen is for entering and reviewing information about Wide Area Network (WAN) settings. Your Network Service Provider (NSP) can provide you with the information needed to correctly make these WAN settings. Your Network Service Provider should specify a WAN protocol, and VPI/VCI settings for you to use.

1. Enter the WAN interface VPI/VCI numbers in the fields provided.
2. Your router supports any one of five available WAN protocols: PPP, RFC 1483, RFC 1483 MER (for ATM), and RFC 1490 or RFC 1490 MER for frame relay. To make your selection, click on the button shown next to the appropriate protocol.
3. Click on the **Next** button to continue Easy Setup.

Point-to-Point Protocol over ATM

Point-to-Point Protocol (PPP)

PPP usually requires a username and password.

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring excess charges in fee-for-service agreements.

Point-to-Point Protocol (PPP)

PPP username:

PPP password:

PPP Networking

☐ Bridging enabled
☐ Only bridge PPPOE traffic

☐ IP routing enabled
☐ NAT enabled
☐ Block NetBIOS traffic

Document: Done

Figure 2-2: Point-to-Point Protocol Screen

1. If you have selected PPP as your WAN protocol, you will see a screen requesting a PPP User Name and a PPP Password. Enter this information in the fields provided.
2. Select one of the following PPP Networking options:
 - **Bridging** will forward all traffic for remote hosts that is not routed (non-IP) to the WAN.
 - **IP Routing** will route all IP packets for remote hosts to the WAN.
 - **Network Address Translation** (NAT) allows multiple workstations on your LAN to share a single, public IP address. All outgoing traffic appears to originate from the router's IP address.
 - **NetBIOS** is a PC networking protocol that can keep network connections open inadvertently. To avoid excess connection charges, such traffic should be blocked on any metered network service.

Click on the **Next** button to continue Easy Setup.

Point-to-Point Protocol over Ethernet over PPPoA

The screenshot shows a Netscape browser window titled "PPPoE Configuration - Netscape". The main content area is titled "Point-to-Point Protocol over Ethernet over PPPoA". On the left, a yellow box contains explanatory text: "PPPoE requires a username and password.", "PPPoE Service Name requires a name. Default is * for any.", "PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.", "PPPoE only Filter is used to specify that only PPPoE traffic will be bridged.", and "PPPoA Setting is used for PPPoE over PPPoA." The main form area is titled "Point-to-Point Protocol over Ethernet over PPPoA" and "PPPoE Setting". It includes fields for "Username:", "Password:", "Service Name", and "PPPoE Timer" (set to "permanent"). There is an unchecked checkbox for "PPPoE only Filter". Below these is the "PPPoA Setting" section with "Username:" and "Password:" fields. At the bottom are "Previous", "Next", and "Cancel" buttons. The status bar at the bottom says "Document: Done".

Point-to-Point Protocol over Ethernet over PPPoA

PPPoE requires a username and password.

PPPoE Service Name requires a name. Default is * for any.

PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.

PPPoE only Filter is used to specify that only PPPoE traffic will be bridged.

PPPoA Setting is used for PPPoE over PPPoA.

Point-to-Point Protocol over Ethernet over PPPoA

PPPoE Setting

Username:

Password:

Service Name:

PPPoE Timer:

☐ PPPoE only Filter

PPPoA Setting

Username:

Password:

Document: Done

Figure 2-3: Point-to-Point Protocol over Ethernet over PPPoA Screen

If you have selected PPPoEoA as your WAN protocol, you will see a screen requesting a PPP user name and a PPP password. You should have received this information from your service provider.

1. Enter your user name and password in the fields indicated.
2. PPPoE Service Name requires the domain name of your network service provider. Use as a default * (for all services). Enter the domain name of your network service provider in the Service Name field.
3. PPPoE Timer will set a timeout interval for periods of inactivity. After the number of seconds elapses, the PPP connection closes to limit timed connection charges from your service provider. Enter the timeout interval (measured in seconds) into the PPPoE Timer field. The default entry of “permanent” will keep the PPP connection open constantly, with no timeout interval.
4. PPPoE Only Filter will filter all traffic on the bridge to allow PPPoE only. Check this box if you will only connect to your network service using PPPoE.
5. Click on the **Next** button to continue Easy Setup.

Point-to-Point over Ethernet over RFC 1483

The screenshot shows a Netscape browser window titled "PPPoE Configuration - Netscape". The main content area is titled "Point-to-Point Protocol over Ethernet over RFC1483". On the left, a yellow box contains explanatory text: "PPPoE requires a username and password.", "PPPoE Service Name requires a name. Default is * for any.", "PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.", and "PPPoE only Filter is used to specify that only PPPoE traffic will be bridged." The main form area is titled "Point-to-Point Protocol over Ethernet over RFC1483" and "PPPoE Setting". It includes fields for "Username:", "Password:", "Service Name", and "PPPoE Timer" (set to "permanent"). There is an unchecked checkbox for "PPPoE only Filter". At the bottom are "Previous", "Next", and "Cancel" buttons. The status bar at the bottom of the browser window says "Document: Done".

Point-to-Point Protocol over Ethernet over RFC1483

PPPoE requires a username and password.

PPPoE Service Name requires a name. Default is * for any.

PPPoE Timer requires a specific duration (in seconds) or the default permanent setting.

PPPoE only Filter is used to specify that only PPPoE traffic will be bridged.

Point-to-Point Protocol over Ethernet over RFC1483

PPPoE Setting

Username:

Password:

Service Name:

PPPoE Timer:

☐ PPPoE only Filter

Document: Done

Figure 2-4: Point-to-Point Protocol over Ethernet over RFC 1483 Screen

-
1. If you have selected PPPoE over RFC 1483 as your WAN protocol, you will see a screen requesting a PPP user name and a PPP password. You should have received this information from your service provider. Enter your user name and password in the fields indicated.
 2. PPPoE Service Name requires the domain name of your network service provider. The default entry is * (all services). Enter the domain name of your network service provider in the Service Name field.
 3. PPPoE Timer will set a timeout interval for periods of inactivity. After the number of seconds elapses, the PPP connection closes to limit timed connection charges from your service provider. The default value is “permanent” for unmetered service. To activate the timer, enter the timeout interval (measured in seconds) into the PPPoE Timer field.
 4. PPPoE Only Filter will filter all traffic on the bridge to allow PPPoE only. Check this box if you will only connect to your network service using PPPoE.
 5. Click on the **Next** button to continue Easy Setup.

RFC 1483 Networking

RFC 1483 Networking

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

The **IP address and Subnet Mask** define the IP address and network of the interface. This information is required in order to use NAT.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring excess charges in fee-for-service agreements.

RFC 1483 Networking

☐ Bridging enabled
☐ Only bridge PPPOE traffic

☐ IP routing enabled
☒ Obtain configuration automatically from WAN using DHCP
☐ Configure IP Routing manually

IP Address

Subnet Mask

☐ NAT enabled
☐ Block NetBIOS traffic

Document: Done

Figure 2-5: RFC 1483 Networking Screen

-
1. If you have selected RFC 1483 as your WAN protocol, you will see a screen for selecting networking options, and for setting your IP routing configurations.
 2. Choose either Bridging enabled or IP routing enabled. If you choose bridging, all traffic to remote computers that is not routed will be bridged. You also have the option to only bridge PPPoE (PPP over Ethernet) traffic.
 3. If you have chosen to have IP routing enabled, you must now choose to obtain your IP configuration automatically from a DHCP server on the WAN, or to configure your IP routing manually. To configure IP routing manually, you must enter a unique IP address and subnet mask for your router.
 4. As options, you can choose NAT enabled to activate NAT (Network Address Translation) and Block NetBIOS traffic.
 5. If your Network Service Provider has not provided specifics for use in making these settings, choose IP Routing, Obtain configuration automatically from WAN, and NAT enabled.
 6. Click on the **Next** button to continue Easy Setup.

RFC 1483 MAC Encapsulated Routing

RFC 1483 MER Networking

Bridging designates that all traffic to remote hosts that is not routed will be forwarded.

IP Routing routes IP traffic to remote hosts.

The **IP address and Subnet Mask** define the IP address and network of the interface. This information is required in order to use NAT.

The **Default Gateway** is the IP address of the next-hop router.

Network Address Translation (NAT) makes all connections appear to originate from the IP address of this interface.

NetBIOS is a PC networking protocol that may keep connections open inadvertently, thus incurring excess charges in fee-for-service agreements.

RFC 1483 MER Networking

☐ Bridging enabled
☐ Only bridge PPPOE traffic

☐ IP routing enabled
☒ Obtain configuration automatically from WAN using DHCP
☐ Configure IP Routing manually

IP Address

Subnet Mask

Default Gateway

☐ NAT enabled
☐ Block NetBIOS traffic

Document: Done

Figure 2-6: RFC 1483 MER Networking Screen

-
1. If you have selected RFC 1483 MER (MAC Encapsulated Routing) as your WAN protocol, you will see a screen for selecting networking options, and for setting IP routing configurations.
 2. Choose either Bridging enabled or IP routing enabled. If you choose bridging, all traffic to remote computers that is not routed will be bridged. You also have the option to only bridge PPPoE (PPP over Ethernet) traffic.
 3. If you have chosen to have IP routing enabled, you must now choose to obtain your IP configuration automatically from a DHCP server on the WAN, or to configure your IP routing manually. To configure IP routing manually, you must enter a unique IP address and subnet mask for your router.
 4. As options, you can choose NAT enabled to activate NAT (Network Address Translation) and Block NetBIOS traffic.
 5. If your Network Service Provider has not provided specifics for use in making these settings, choose IP Routing, Obtain configuration automatically from WAN, and NAT enabled.
 6. Click on the **Next** button to continue Easy Setup.

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP)

DHCP assigns IP configuration information to hosts on the LAN thus avoiding the need for manual setup.

Domain Name Service (DNS) maps names to addresses.

The **Domain Name** identifies the default network name.

Domain Name Servers map host names to IP addresses.

Windows Internet Naming Service (WINS) maps NetBIOS names to IP addresses.

Dynamic Host Configuration Protocol (DHCP)

☒ DHCP server enabled on LAN

☒ Obtain DNS information automatically
☐ Configure DNS manually

Domain Name

Primary DNS Server

Secondary DNS Server

Primary WINS Server

Secondary WINS Server

Document: Done

Figure 2-7: Dynamic Host Configuration Protocol Screen

1. DHCP dynamically assigns IP configuration information to PCs on the LAN, thus avoiding the need to set IP configurations for each PC manually. You can enable DHCP by clicking on the indicated checkbox.
2. Domain Name Service (DNS) maps host names to IP addresses. DNS is performed by Domain Name Servers. The domain name identifies the default name for the network. You can set your router to obtain DNS information automatically. You can also choose to configure DNS manually by making the required entries in the form. If you are configuring DNS manually, you must enter at least one DNS IP address.
3. The Windows Internet Naming Service (WINS) maps NetBIOS names to IP addresses.
4. Click on the **Next** button to continue Easy Setup.

Local Area Network Configuration

LAN IP Configuration

The IP Address is the network address of the router. This address must be globally unique unless NAT is enabled.

Subnet Mask is used along with the IP address to determine whether or not the local IP traffic should be forwarded.

LAN IP Configuration

IP Address: 192.168.254.254

Subnet Mask: 255.255.255.0

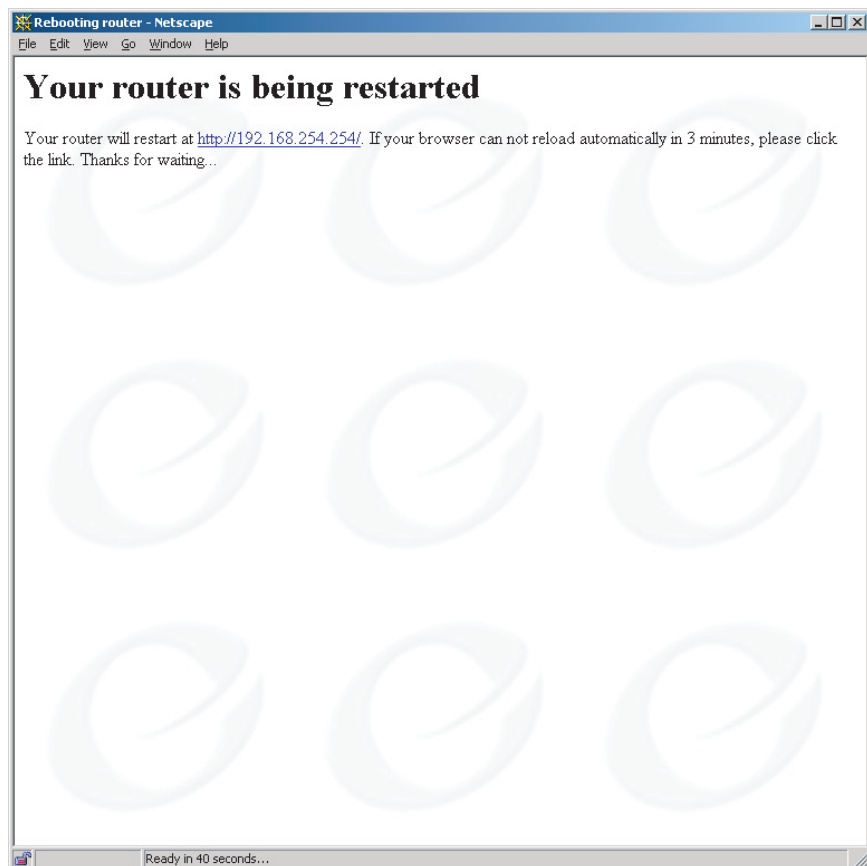
Previous Save and Reboot Cancel

Document: Done

Figure 2-8:

The final screen in Easy Setup is for Local Area Network (LAN) configuration.

1. Enter the IP address into the field provided. The IP address is the network address of your router. This address must be globally unique, unless NAT has been enabled.
2. Enter the subnet mask into the field provided. The subnet mask is used along with the IP address to determine if specific LAN IP traffic should be forwarded to the WAN.
3. Click **Save and Reboot** to save your settings in Easy Setup. Your router will reboot with the new configuration settings.

**Figure 2-9: Router Restart Screen**

Chapter 3

Additional Features

Beyond Easy Setup, your router is equipped with additional features that add services and value to your DSL connection. These features can be implemented using the Web interface links found on the Router Information Screen. These features, along with brief descriptions of each, are listed below:

- **Access Control** - The Access Control feature restricts administrative access and control of your router to a select group of hosts.
- **Feature Activation** - This feature supports the installation of feature activation keys that are used to enable additional features on your router.
- **Current Date and Time** - This feature enables you to set the date and time on your router.
- **Set DHCP** - The DHCP feature enables or disables DHCP, and manages your IP address pool.
- **Set NAT** - This feature enables or disables Network Address Translation between the Local and Wide Area Networks.
- **Set Firewall** - A simple yet powerful network security feature for the creation and development of firewalls.
- **Dial Backup** - The Dial Backup feature provides a backup connection to the Internet through an external modem, connected to the console port of your router.
- **IKE/IPSec Configuration** - This is an optional feature for your router. IKE/IPsec (Internet Key Exchange/Internet Protocol Security) configuration screens enable optional authentication and encryption of IP traffic for the authenticity, integrity and privacy of your communications.
- **Command Line Interface** - The Command Line Interface (CLI) is used for advanced router configuration.

Access Control

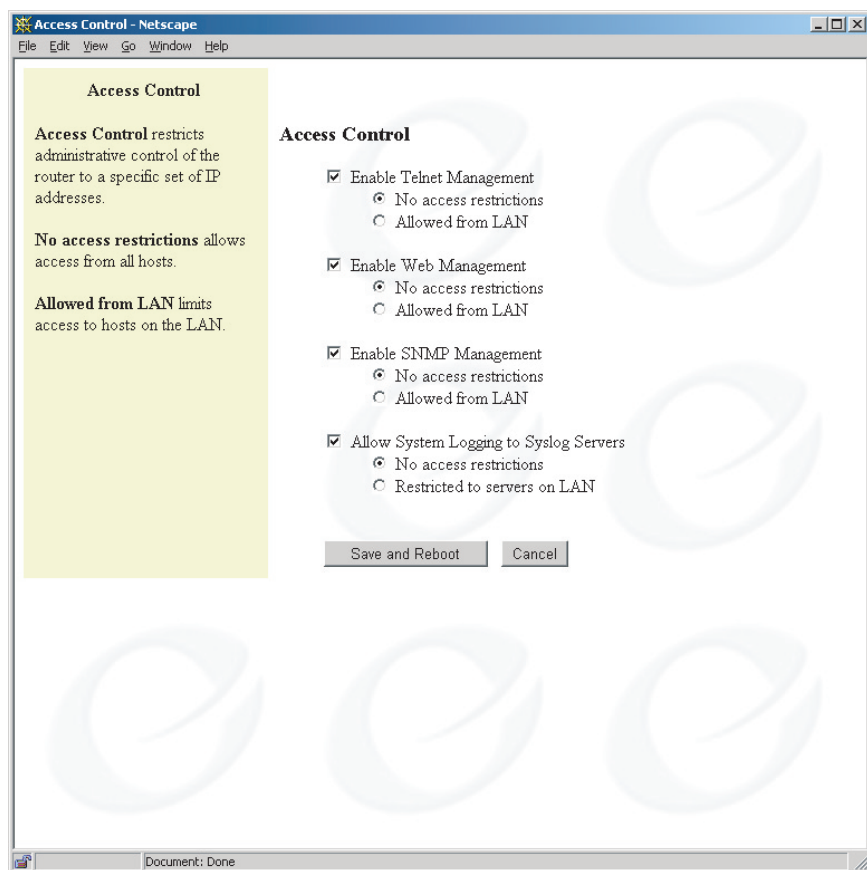


Figure 3-1: Access Control Screen

The Access Control feature restricts administrative access and control of your router to a select group of hosts. In this web form, you can select which router services can be accessed from PCs. For each selected service, you can restrict the hosts that can manage the service remotely. Your options for each service are:

- Enable or disable host access to the service.
- Enable only hosts on the LAN to manage the service.
- Allow all hosts to manage the service (default).

If you are unsure of how to configure Access Control, leave the factory default settings. These settings can always be changed later by returning to this Access Control form.

Feature Activation

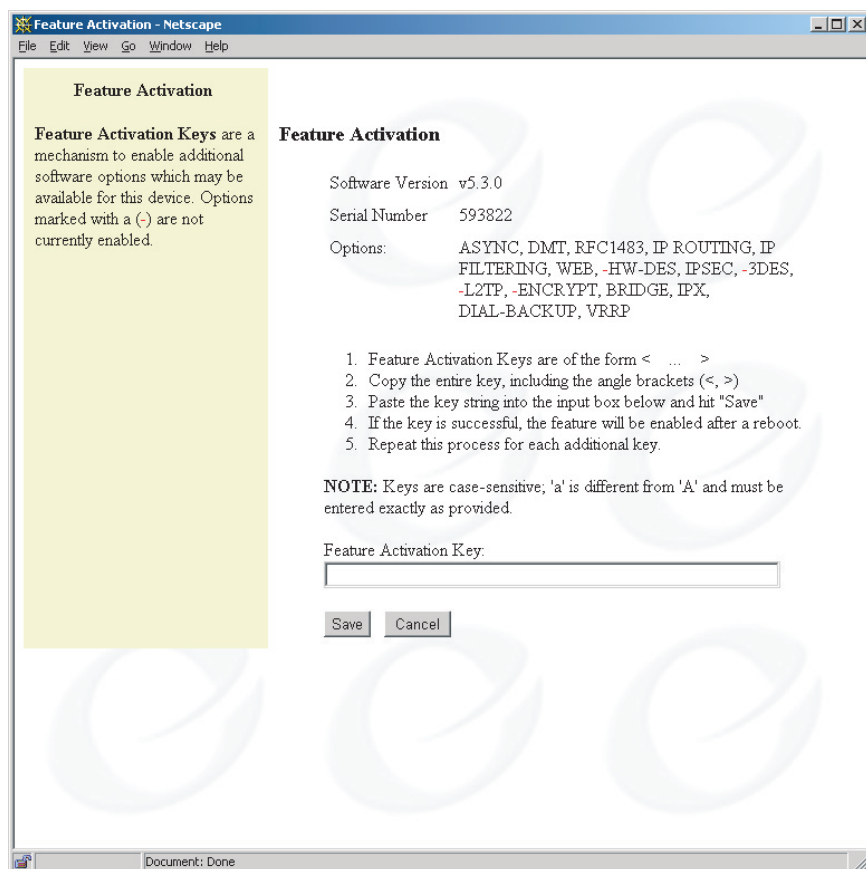


Figure 3-2: Feature Activation Screen

Several optional software features are available for your router, such as L2TP, IPSec, DES Encryption, and 3DES Encryption. These features can be purchased from the Efficient Networks web site (www.efficient.com). You will need your router serial number to purchase a feature activation key. For each optional feature purchased, you will be emailed a feature activation key.

Feature activation keys are used to enable additional features on your router. Features that are not activated on your router are marked with a dash (-) as shown on the screen to the right. Feature activation keys are long strings in the following format:

< 1234... >

To input a feature activation key:

1. Copy the entire key, including the brackets, from the email.
2. Paste the key into the input box on this form.
3. Press the **Save** button at the bottom of the Feature Activation form.
4. Repeat these steps for each feature activation key you have to input.
5. Reboot your router. Your new features will be active once the router is rebooted, provided that the feature activation key(s) have been correctly entered.

Setting The Date and Time

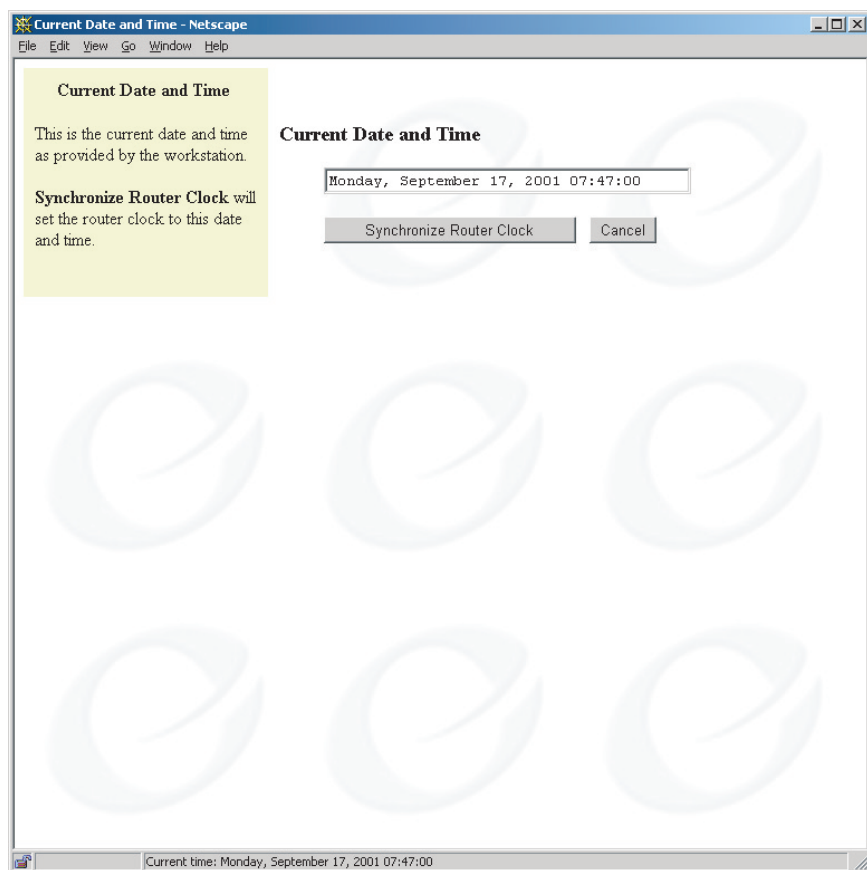


Figure 3-3: Current Date and Time Screen

This feature enables you to set the date and time on your router.

The current date and time from your PC are displayed in the field labeled **Current Date and Time**.

To synchronize the date and time on your router with the current date and time displayed, click on the **Synchronize Router Clock** button.

Set DHCP

DHCP Setting - Netscape

File Edit View Go Window Help

LAN DHCP Server Status

Shows current LAN DHCP setting and allows user to enable/disable it.

IP Addresses Pool Setting

Shows current first IP address/last IP address of IP address pool and allows user to change to different IP addresses. Remember - last IP address must be greater or equal to first IP address. Both first IP address and last IP address can not be subnet address or broadcast address.

Current DHCP Leases List

Shows current lease IP addresses including information like IP address, state, host name and expiration time.

LAN DHCP Server Status:

Current Setting	New Setting	
Enabled	Enable	Apply

IP Addresses Pool Setting:

	Current Setting	New Setting	
First IP Address	192.168.254.2		Apply
Last IP Address	192.168.254.20		

Current DHCP Leases List:

Client IP	State	Host Name	Expires (mm/dd/yy)
192.168.254.2	enabled	icalder	Jun 16 2001 3:30:36

Back to Home

Document: Done

Figure 3-4: Set DHCP Screen

This feature enables you to make and view the current Dynamic Host Configuration Protocol (DHCP) settings for your router. DHCP is a TCP/IP service protocol to provide dynamic leasing of IP addresses and other configuration information to client hosts on the network. Your router can perform as a DHCP server with central management of your IP address pool for simple and safe TCP/IP configuration and IP address conservation. When DHCP is combined with Network Address Translation (NAT), your router adds a measure of security to your network through the leasing and concealment of private IP addresses behind one unique public IP address. These private IP addresses also help avoid the costs associated with obtaining additional public IP addresses to support a growing network.

To activate DHCP, select **Enable** from the New Setting list and click on the **Apply** button. Conversely, selecting Disable will deactivate DHCP.

With DHCP, all IP addresses are assigned to network clients from a pool. The **IP Addresses Pool Setting** section provides fields for defining the range of IP addresses included in your pool. The fields under Current Setting display the current range of the IP Address pool. Use the fields under the New Setting label to define a new range of IP addresses for the pool. Click on the **Apply** button to establish the new IP addresses pool settings.

The **Current DHCP Leases List** shows the network clients that are currently leasing their IP addresses from the pool. From left to right, the following information is presented on each row:

- **Client IP:** Displays the leased IP address assigned to that specific client.
- **State:** Indicates whether the IP address is enabled or disabled.
- **Host Name:** Displays the name of the host leasing that specific IP address.
- **Expires (mm/dd/yy):** Displays the date when the IP address lease will expire. At that time (if not before), the leased IP address will be freed for re-assignment, and the network client will need to request a new IP address from the router.

After DHCP settings have been completed, click on the **Back to Home** button to return to the home screen.

NAT Settings

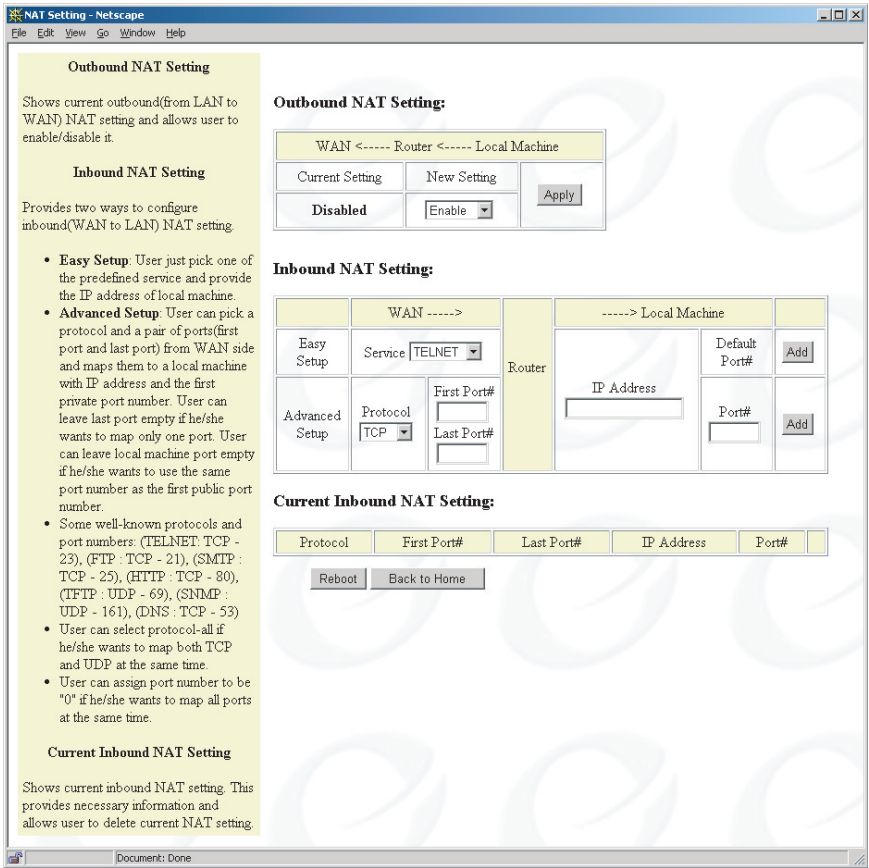


Figure 3-5: NAT Settings Screen

Network Address Translation (NAT) is a feature that can provide a level of security by hiding the private IP addresses of your LAN behind the single public IP address of your router. All connections must come through your router and be translated by NAT. Network addresses on inbound traffic are translated from public to private IP addresses, while addresses on outbound traffic are translated

from private IP addresses to the router's public IP address, thereby concealing the private IP addresses used on your Local Area Network (LAN). Network Address Translation can provide a level of security by obscurity that is acceptable to many users.

Outbound NAT Setting: Use this field to enable or disable Network Address Translation of outbound traffic; communications from your LAN to the Wide Area Network beyond your router (WAN). Click on the **Apply** button to complete the new setting.

Inbound NAT Setting: This section of the form is divided into two parts. The left side contains fields for WAN settings. The right side contains fields for local machine settings. A section labeled "router" divides these two parts. This layout is a simple diagram of how NAT works between the WAN and the local machine to translate network addresses.

Two methods are available for making inbound NAT settings:

Easy Setup: You can quickly configure your inbound NAT to support the most common network services with the Easy Setup fields. Select a network service from the drop down list on the WAN side of the form, and then enter the IP address of the local machine on the local machine side of the form. Click on the **Add** button next to the label "Default Port#", unless you want to specify an alternate port to use for the selected service. If you want to specify an alternate port, use the field marked "Port#" to enter your alternate port, and press its **Add** button to complete the service setup for inbound NAT.

Advanced Setup: The Advanced Setup fields give you the option of assigning specific network protocols to specific ports on the WAN side of NAT, while mapping the WAN settings to an IP address and port number of a local machine.

1. Select the protocol from the drop down list.
2. Enter the first port number for the protocol in the **First Port#** field. If you want to assign a range of ports for the protocol, enter the last port number in the range in the **Last Port#** field.
3. In the Local Machine part of the Advanced Setup section, enter the IP address of the local machine in the **IP Address** field.
4. Enter the port number on the local machine for the protocol to use. Leave this field blank if you want the local machine to use the same port number as the WAN.
5. Press the **Add** button next to the Default Port# or the Port# field (as appropriate) to finish your advanced NAT configuration. Repeat this process for each protocol you want to configure for NAT.

Press the **Reboot** button to restart the router with the new NAT settings. Press **Back to Home** to cancel your NAT settings and return to the home screen.

Set Firewall

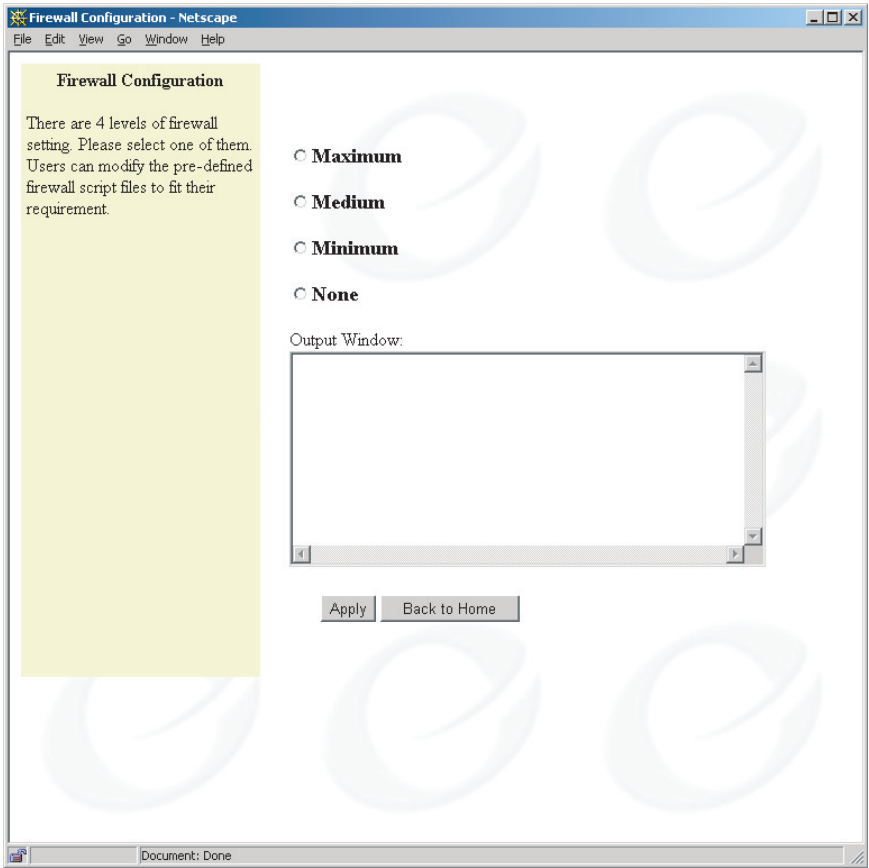


Figure 3-6: Set Firewall Screen

Your router can secure your network and data communications with built-in firewall capabilities. A firewall is any combination of hardware and software that secures a network and traffic to prevent interception or intrusion. Your router is equipped with predefined scripts that can be modified or used directly to construct firewalls. You can select from four firewall options:

- **Maximum:** Establishes a firewall with the most restrictive policies for maximum network security.
- **Medium:** Establishes a firewall with flexible policies for a moderate level of network security.
- **Minimum:** Establishes a firewall with a basic set of policies for a minimum level of network security.
- **None:** No firewall.

Make your selection, and press the **Apply** button to implement your firewall. To cancel, press the **Back to Home** button and return to the home screen.

For many networks, these predefined firewalls will protect against all but the most sophisticated attacks. For the experienced network security technician, these predefined scripts can serve as a starting point for custom configurations to support your own unique network policies.



CAUTION:

All network security efforts, including firewall configurations, should be performed by an experienced and qualified network security technician, who is familiar with the unique architecture and requirements of your network. Efficient Networks cannot be liable for security violations due to inadequate or incorrect firewall configurations.

Dial Backup

Dial Backup Setup - Netscape

File Edit View Go Window Help

Dial Backup

Use the console (serial) port to attach an external analog modem. To use the dial backup function, users must enable it first.

☒ **Enable Dial Backup**

User name

Password

Phone number

Alternative Phone number (optional)

☐ **Disable Dial Backup**

Document: Done

Figure 3-7: Dial Backup Screen

Dial Backup provides a backup connection to the Internet through an external V.90 modem, connected to the console port of your router. This backup connection can be activated in the event of a DSL service interruption. During a DSL interruption, your router will use the dialup modem connection while waiting for DSL service to be restored. Once the DSL link is active again, Dial Backup will automatically switch back to the DSL service. Voice service is disabled during dial backup.

A special console connector is required to configure Dial Backup. This connector can be ordered through your Internet Service Provider, or from the Efficient Networks web site at the following URL: <http://www.efficient.com/>

To access the Dial Backup screen, select the Dial Backup link from the Router Information screen. The Dial Backup screen will appear. To enable Dial Backup, follow these steps:

1. Enter your user name and password as provided from your ISP.
2. Enter at least one telephone number for dialup access to your ISP.
3. Click the **OK** button to continue with Dial Backup Configuration.
4. The next screen provides settings for Dial Backup Configuration:
 - Failover after connection is lost:** This setting specifies the time interval between losing the DSL connection and switching to the dialup modem connection.
 - Resume DSL after connection is lost:** The time interval between checks for service restoration is called the retry period. After each retry period, your router will test the DSL connection for service. If service is restored, the router will switch data traffic to the DSL connection. The serial port will revert to its default function as the console port.
 - Serial Port Data Rate:** This field specifies the maximum rate at which data can flow through the serial port. This setting should equal the maximum baud rate of the attached modem.
 - Modem Initialization String:** This field sets the initialization string used by the V.90 modem attached to the console port of the router.
 - Modem Dial String:** Sets the dial string for one of two possible dialing options; pulse or tone dialing. The default is tone dialing.
5. You will need to reboot your router to enable changes to Dial Backup.

IKE/IPSec Configuration

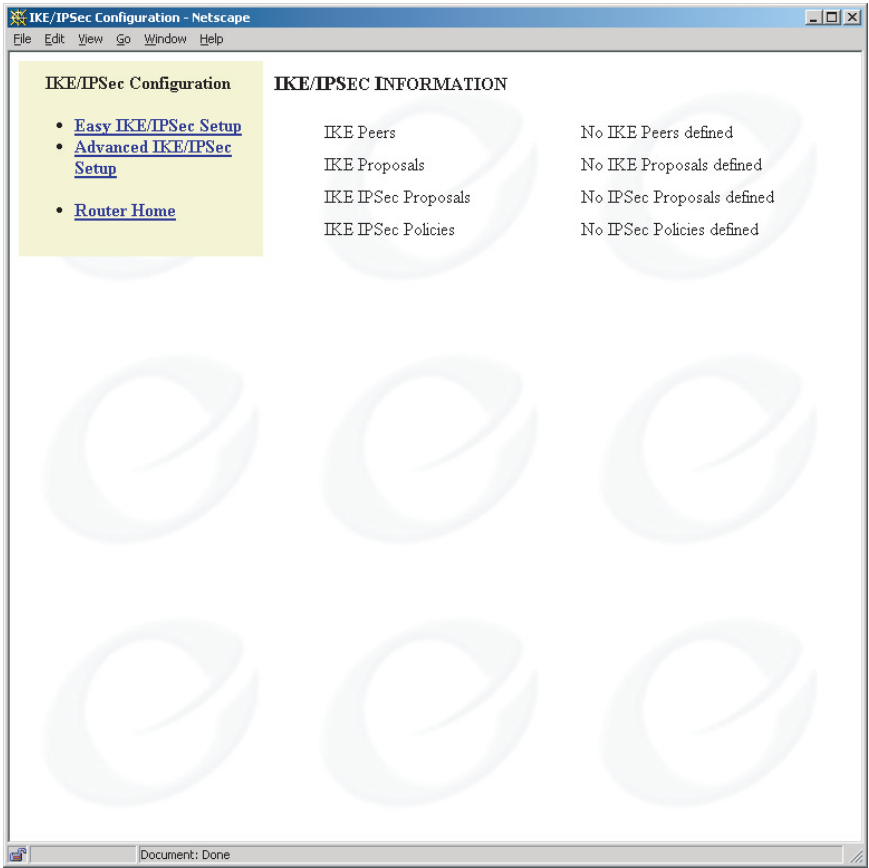


Figure 3-8: IKE/IPSec Information Screen

IKE/IPSec is an optional feature for your router. IKE/IPsec (Internet Key Exchange/Internet Protocol Security) configuration screens enable optional authentication and encryption of IP traffic for the authenticity, integrity and privacy of your communications. IPsec sessions are established through Security Associations (SAs) that enable secure devices to negotiate a level of security attributes needed for a Virtual Private Network (VPN).

The home screen for IKE/IPSec configuration displays current IKE and IPsec definitions. These definitions must be established by using the Easy IKE/IPSec Setup and Advanced IKE/IPSec Setup screens.

To begin the configuration of IKE/IPsec, click the **Easy IKE/IPSec Setup** link.

IKE/IPSec Setup

Easy IKE/IPSec Setup

Internet Key Exchange (IKE) is a means of dynamically creating IP Security (IPSec) connections. IPSec uses encryption and authentication to create virtual private networks over an insecure network.

This screen will create a default IKE configuration.

The **IKE Peer Name** is a logical name for an IKE Peer. This name has no significance to the remote party.

The **Pre-shared Secret** is a mutually agreed-upon secret between both parties.

The **Peer Gateway IP Address** specifies the IP address of the other end of the IKE connection.

The **Destination IP Address** is the IP address of the remote private network that uses this policy.

The **Destination Subnet Mask** is the subnetwork mask of the remote private network that uses this policy.

Easy IKE/IPSec Setup

IKE Peer Name

Pre-shared Secret

Peer Gateway IP Address

Destination IP Address

Destination Subnet Mask

Document: Done

Figure 3-9: Easy IKE/IPSec Setup Screen

1. **IKE Peer Name:** The first field in the Easy IKE/IPSec Setup screen is to assign a logical name to the IKE peer. This name is of no importance to the remote IKE peer. Choose a name that is meaningful to you. Enter the IKE Peer Name in the field provided.
2. **Pre-Shared Secret:** A pre-shared secret is a case-sensitive character string used for authentication. This secret can be up to 256 characters, with no spaces or non-printable characters. The pre-shared secret must be mutually agreed upon by both parties to the IKE connection. Enter your pre-shared secret in the field provided.
3. **Peer Gateway IP Address:** Enter the IP address of the gateway at the remote end of the IKE connection.
4. **Destination IP Address:** Enter the IP address of the remote private network that your router will authenticate using this IKE policy.
5. **Destination Subnet Mask:** Enter the destination subnet mask of the remote private network that your router will authenticate using this IKE policy.
6. Click on the **Save IKE Settings** button to establish your new IKE/IPSec policy and return to the router home screen.

Advanced IKE/IPSec Setup

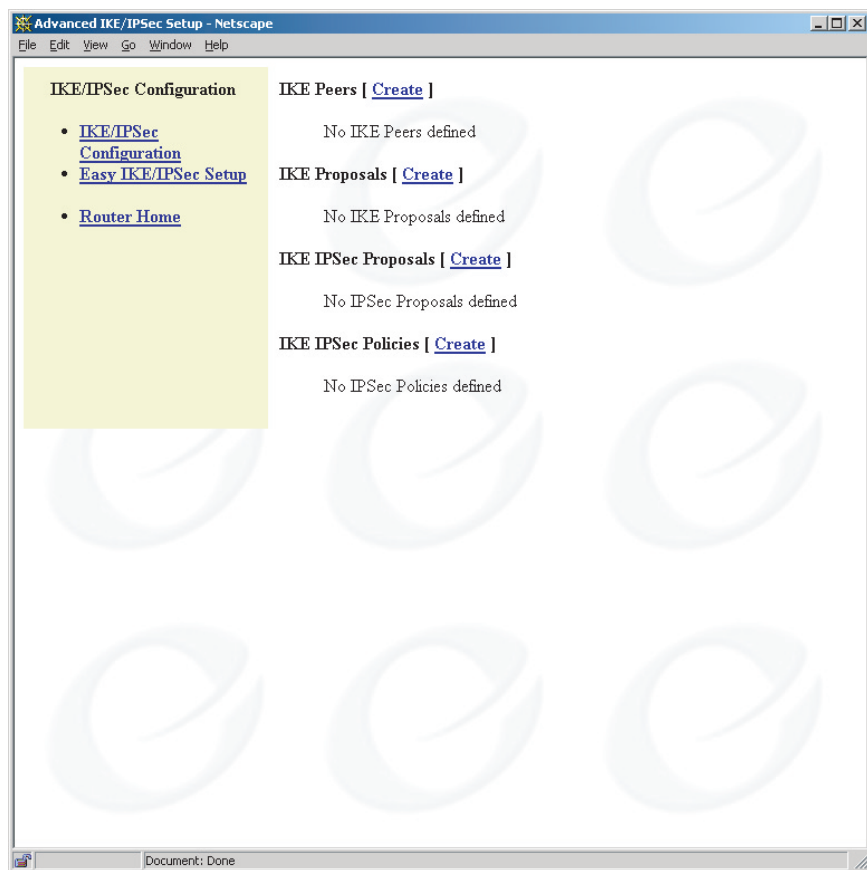


Figure 3-10: Advanced IKE/IPSec Setup Screen

The Advanced IKE/IPSec Setup screen presents information about your IKE and IPSec peers, policies and proposals. Each section of this screen includes a Create link to screens for establishing new IKE and IPSec definitions. On this Advanced IKE/IPSec Setup screen, the following types of information and links are provided:

- **IKE Peers:** Lists the IKE Peers that have been defined. IKE peers are those devices known to your router as capable of participating in IKE connections. Click on the **Create** link to define new IKE Peers.
- **IKE Proposals:** Lists the IKE Proposals that have been defined. IKE IPSec Proposals specify how packets will be encrypted/authenticated for the final SA. Then IKE IPSec Policies specify which packets will be encrypted/authenticated for the final SA. Click on the **Create** link to define new IKE Proposals.
- **IKE IPSec Proposals:** Lists the IPSec proposals that have been defined. Click on the **Create** link to define new IPSec proposals.
- **IKE IPSec Policies:** Lists the IPSec policies that have been defined. IPSec policies are criteria for packets that IPSec will recognize, and actions that IPSec will take upon such recognition. Click on the **Create** link to define new IPSec policies.

IKE Peer Definition

IKE Peer Definition

NOTE: If the remote peer does not have a fixed IP address, enter "0.0.0.0" for the Peer Gateway IP Address and use Aggressive Mode.

The **IKE Peer Name** is a logical name for an IKE Peer. This name has no significance to the remote party.

The **Pre-shared Secret** is a mutually agreed-upon secret between both parties.

The **Peer Gateway IP Address** specifies the IP address of the other end of the IKE connection.

IKE Peer Definition

IKE Peer Name

Pre-shared Secret

Peer Gateway IP Address

Document: Done

Figure 3-11: IKE Peer Definition Screen

1. **IKE Peer Name:** The first field in the IKE Peer Definition screen is to assign a logical name to the IKE peer. This name is of no importance to the remote IKE peer. Choose a name that is meaningful to you. Enter the IKE Peer Name in the field provided.
2. **Pre-Shared Secret:** A pre-shared secret is a case-sensitive character string used for authentication. This secret can be up to 256 characters, with no spaces or non-printable characters. The pre-shared secret must be mutually agreed upon by both parties to the IKE connection. Enter your pre-shared secret in the field provided.
3. **Peer Gateway IP Address:** Enter the IP address of the gateway at the remote end of the IKE connection. If the remote IKE peer does not have a fixed or permanent IP address, enter “0.0.0.0” to use Aggressive Mode in Phase 1 negotiations. Your router supports two Phase 1 IKE modes: Main and Aggressive. Your router will use Main Mode when both the source and destination IP addresses are known. Your router will use Aggressive Mode when either the source or destination IP addresses could change.
4. Click on the **Save IKE Settings** button to save your IKE peer definition and return to the home screen.

IKE Proposal Definition

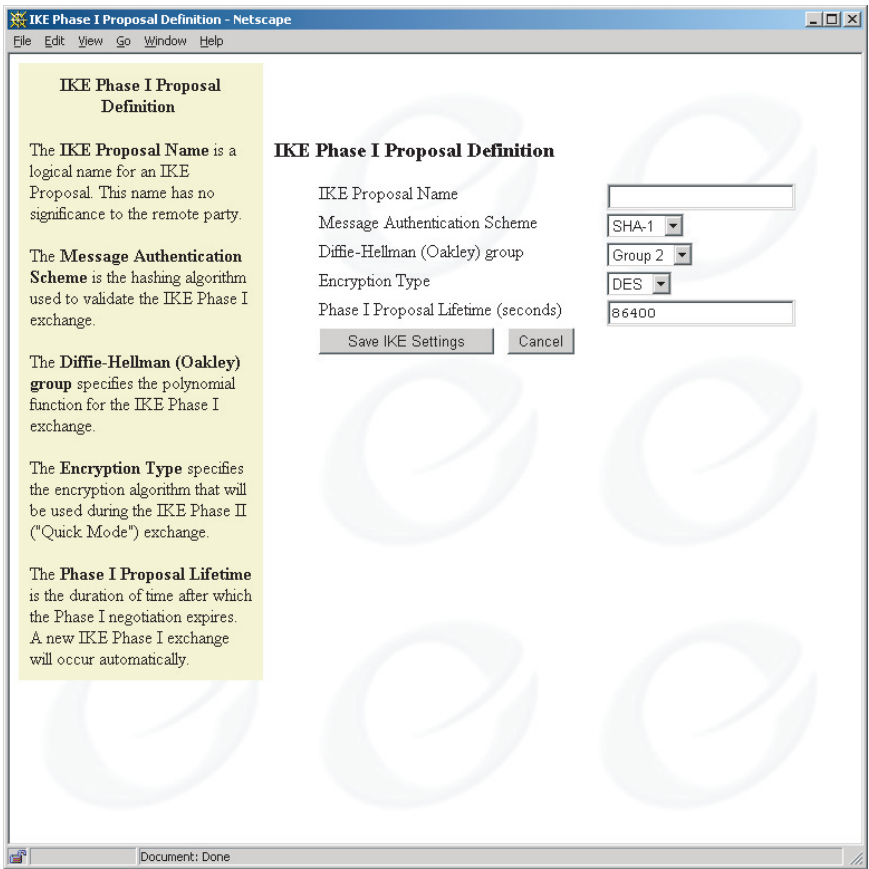


Figure 3-12: IKE Proposal Definition Screen

-
1. **IKE Proposal Name:** Enter a logical name for the IKE Proposal Definition. This name is of no importance to the remote IKE peer.
 2. **Message Authentication Scheme:** Select the message authentication scheme from two possible message authentication proposals:
 - **MD5:** Perform message authentication using Message Digest 5.
 - **SHA1:** Perform message authentication using Secure Hashing Algorithm 1 (default).
 3. **Diffie-Hellman (Oakley) Group:** Select the Diffie-Hellman key generation group from two Diffie-Hellman Group options:
 - **Group 1:** Use Diffie-Hellman Group 1 (768 bits).
 - **Group 2:** Use Diffie-Hellman Group 2 (1024 bits).
 4. **Encryption Type:** Select the type of encryption to be proposed:
 - **DES:** Encrypt using a 56-bit key.
 - **3DES:** Encrypt using three 56-bit keys to produce 168-bit encryption.
 5. **Phase 1 Proposal Lifetime:** Select the duration of this proposal, as measured in seconds. The default setting is 86400 seconds (24 hours). Once this lifetime is elapsed, your router will renegotiate the IKE connection.

IKE IPSec Proposal Definition

IKE IPSec Proposal Definition

The **IPSec Proposal Name** is a logical name for an IPSec Proposal. This name has no significance to the remote party.

The **AH Authentication Scheme** is the hashing algorithm used for Authentication Header (AH) IPSec.

The **ESP Authentication Scheme** is the hashing algorithm used for Encapsulating Security Payload (ESP) IPSec.

The **ESP Encryption Scheme** is the algorithm used to encrypt ESP IPSec packets.

The **IP Compression Method** is the algorithm used to compress IPSec packets.

The **Phase II Proposal Lifetime** is the duration of time after which the IKE Phase II negotiation expires. A new IKE Phase II exchange will occur automatically.

The **Phase II Proposal Lifedata** is the number of kilobytes of data after which the IKE Phase II negotiation expires. A new IKE Phase II exchange will occur automatically.

IKE IPSec Proposal Definition

IPSec Proposal Name:

AH Authentication Scheme:

ESP Authentication Scheme:

ESP Encryption Scheme:

IP Compression Method:

Phase II Proposal Lifetime (seconds):

Phase II Proposal Lifedata (KBytes):

Document: Done

Figure 3-13: IKE IPSec Proposal Definition Screen

1. **IKE IPSec Proposal Name:** Enter a logical name for the IKE IPSec Proposal Definition. This name is of no importance to the remote IKE IPSec peer.
2. **AH Authentication Scheme:** Select which AH method to propose:
 - **NONE:** Request no AH encapsulation.
 - **MD5:** Request AH encapsulation and authenticate using Message

Digest 5.

- **SHA1:** Request AH encapsulation and authenticate using Secure Hashing Algorithm 1.
3. **ESP Authentication Scheme:** Select which ESP message authentication to propose:
 - **NONE:** Perform no message authentication.
 - **MD5:** Perform message authentication using Message Digest 5.
 - **SHA1:** Perform message authentication using Secure Hashing Algorithm 1.
 4. **ESP Encryption Scheme:** Select the encryption method (if any) to propose:
 - **DES:** Use ESP encapsulation and 56-bit encryption.
 - **3DES:** Use ESP encapsulation and three 56-bit keys to produce 168-bit encryption.
 - **NULL:** ESP encapsulation, but no data encryption. ESP encapsulation enables verification of the source, but data is sent in the clear to increase throughput.
 - **NONE:** No ESP encapsulation and no encryption is used.
 5. **IP Compression Method:** Select whether to propose LZS IP compression, or none.
 6. **Phase II Proposal Lifetime:** Enter the length of time to propose, as measured in seconds, before the IPSec SA expires. The default setting is 1800 seconds. Once this lifetime is elapsed, your router will renegotiate the IKE connection.
 7. **Phase II Proposal Data:** Enter the amount of data, as measured in kilobytes, before the IPSec SA terminates. After the specified quantity of data has been transferred, your router will renegotiate the IKE connection. If you use zero, the data quantity will be unlimited. By setting a limit on the amount of data transferred, you can reduce the risk of a key becoming compromised.
 8. Click on the **Save IKE Settings** button to save your IKE IPSec proposal definition and return to the home screen.

IKE IPSec Policy Definition

IKE IPSec Policy Definition

The **IPSec Policy Name** is a logical name for an IPSec Policy. This name has no significance to the remote party.

The **Peer Binding** identifies the remote peer for which this policy applies.

The **PFS Group** identifies the Diffie-Hellman group for Perfect Forward Secrecy.

The **IPSec Proposal Bindings** identify the IPSec Proposals which may be used for this policy

The **IP Protocol** identifies the protocol of the IP traffic that uses this policy.

The **Source IP Address** is the IP address from the local private network that uses this policy.

The **Source Subnet Mask** is the subnetwork mask of the local private network that uses this policy.

The **Destination IP Address** is the IP address of the remote private network that uses this policy.

The **Destination Subnet Mask** is the subnetwork mask of the remote private network that uses this policy.

The **Source Port** is the source port of the TCP/UDP traffic that uses this policy.

The **Destination Port** is the destination port of TCP/UDP traffic that uses this policy.

IKE IPSec Policy Definition

IPSec Policy Name

Peer Binding

IPSec Proposal Bindings

PFS Group

none

IP Protocol

all

Source IP Address

192.168.254.254

Source Subnet Mask

255.255.255.0

Destination IP Address

0.0.0.0

Destination Subnet Mask

0.0.0.0

Source Port

all

Destination Port

all

Save IKE Settings

Cancel

Figure 3-14: IKE IPSec Policy Definition Screen

1. **IPSec Policy Name:** Enter a logical name for the IPSec policy. The name you choose is of no consequence to the other IPSec party.
2. **Peer Binding:** Specify the remote IKE peer to which this policy shall apply. This peer must be already defined with the IKE Peer Definition screen.
3. **IPSec Proposal Bindings:** Specify an IKE IPSec proposal to be used with this policy. The IKE IPSec proposal must be already defined with the IKE IPSec Proposal Definition screen.
4. **PFS Group:** Select the Perfect Forward Secrecy negotiation and Diffie-Hellman group to be used for each rekey. Perfect Forward Secrecy enhances the security of the key exchange. In the event of a key becoming compromised, only the data protected by that compromised key becomes vulnerable. You can choose None, Group 1 or Group 2.
5. **IP Protocol:** Specify a protocol to be used with this policy. You can also enable any protocol to be used by selecting “all”.
6. **Source IP Address:** Enter the IP address of the local area network that will use this policy. This will usually be the IP address assigned to the network local to your router.
7. **Source Subnet Mask:** Enter the subnet mask of the local area network that will use this policy. This will usually be the subnet mask assigned to the network local to your router.
8. **Destination IP Address:** Enter the IP address of the remote private network to which your router will connect using this policy.
9. **Destination Subnet Mask:** Enter the subnet mask of the remote private network to which your router will connect using this policy.
10. **Source Port:** Enter the port that will be the source of TCP/UDP traffic under this policy. You can specify All ports, a port number, or an IP application associated with a particular port. Because port numbers are TCP and UDP specific, a port filter is effective only when the protocol filter is TCP or UDP (see Step 5: IP Protocol).
11. **Destination Port:** Enter the port that will be the destination of TCP/UDP traffic under this policy. You can specify All ports, a port number, or an IP application associated with a particular port.
12. Click on **Save IKE Settings** to establish your IKE IPSec policy and return to the home screen.

Command Line Interface

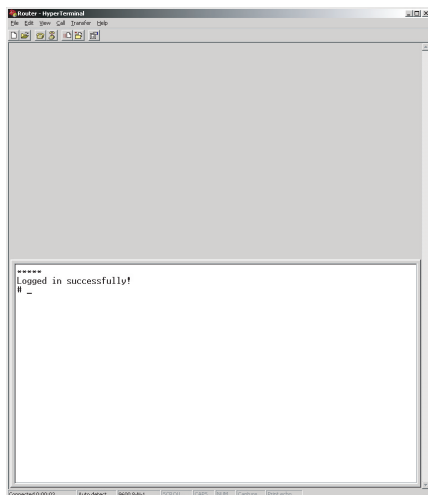


Figure 3-15: HyperTerminal Command Line Interface Screen

The Command Line Interface (CLI) is used for advanced router configuration. It can be accessed through a connection between your workstation and the console port of your router. Use a straight through (red label) cable and a DB9 adapter to connect your router to your PC serial port. Boot both systems and open a connection using your VT 100 terminal emulation program. Use the following port settings:

- Baud Rate: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware

Note: The console port is disabled if Dial Backup is enabled.

For specific configuration information and instructions, please refer to the *Command Line Interface Reference Manual* included on your CD-ROM.

Chapter 4

Frequently Asked Questions

Which cable do I use to connect a new LAN device to the router?

If you are connecting your LAN device to one of the Ethernet ports on your router, use a straight-through (red) cable.

If you are connecting your router directly to another hub, then use a crossover (yellow) cable. If your hub has a built-in crossover or uplink port, then you must use a straight-through (red) cable.

Can I connect the router to a 100Base-T hub?

Yes, if the hub has a 10/100 switch. You need to set the switch to 10 for the router connection.

What is the router password?

The default user name is `login` and the password is `admin`.

We strongly recommend that you change the router password from the default to your own password. If your NSP has changed the router password from the default, you'll need to contact them for assistance.

What security options do I have?

Network Address Translation (NAT) is a feature that can provide a level of security by hiding the private IP addresses of your LAN behind the single public IP address of your router. All connections must come through your router and be translated by NAT.

Further security is available with IP filtering firewall software. The firewall can be accessed through the Web GUI or Command Line Interface (CLI) and configured with scripts for a "quick" firewall. A qualified technician should perform all firewall configuration. Efficient Networks cannot be liable for vulnerabilities arising from inadequate firewall configurations.

To provide secure connections across the Internet, consider purchasing the Virtual Private Network (VPN) software option. Additional information on NAT, Firewall, and Secure VPN can be found in the CLI Reference Manual.

Can I have an FTP, Mail or Web server and use NAT?

Yes, but you need to configure your router appropriately using the NAT Setting screen or the Command Line Interface (CLI). By entering a `remote system` or `addServer` command, you can add FTP, Mail, NetMeeting or Web servers to your LAN. These can then be accessed from another LAN or the Internet while NAT is enabled.

What is MER?

MER (MAC Encapsulated Routing) allows your router to perform routing on the LAN side and bridging on the WAN side. MER is needed only when your Network Service Provider doesn't support IP routing. MER adds NAT functionality, thereby providing greater security and more IP addresses for your LAN than what is provided by your NSP.

Why can't I get a response after entering a URL in my browser?

If you do not get a response, try pinging the IP address. If you get a response to pinging, then your Domain Name Service (DNS) is probably failing. You should contact your NSP for DNS assistance. If you do not get a response, then try pinging the WAN Gateway address (of your NSP) to confirm that your router can connect with the NSP.

If pinging fails, check the router's lights. The Link lights on the router front should be green. Also check your cable connections. If everything appears correct, check your IP configuration and ensure that the gateway and LAN IP addresses match.

How can I connect my modem for dial backup if the connector on my dialup modem doesn't match the console port on the router?

You need a special DB9 to DB25 connector, available from the Efficient Networks web site at the following address: <http://www.efficient.com>

My modem is not a V.90. Can I use it for dial backup?

Yes, you can use a non-V.90 modem with your router for dial backup. Be sure to use the correct initialization string for your modem (consult your modem documentation).

Chapter 5

Product Specifications

Front Panel



Figure 5-1: 5800 Series Router Front Panel

Table 5-1: Front Panel Light Indications

Light	Color	Indications
PWR	Green Off	Power is ON Power is OFF
TEST	Yellow: Green: (2 sec blink) Off:	Running Power On Self Test Self Test successful Router is shut down
LINK	Yellow: Green: Off:	Establishing DSL modem link DSL modem link successful DSL modem link is shut down
WAN	Green flashing: Off:	WAN transmissions detected No WAN transmissions detected
LANT	Green flashing: Off:	Transmitting LAN traffic Not transmitting LAN traffic
LANR	Green flashing: Off:	Receiving LAN traffic Not receiving LAN traffic

5800 Series Back Panel

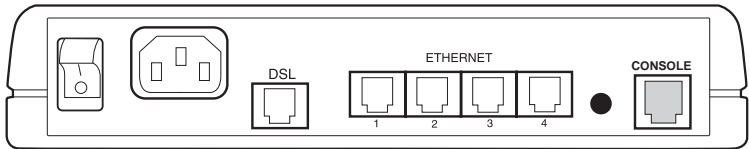


Figure 5-2: 5800 Series Router Back Panel

Table 5-2: 5800 Series Back Panel Port Functions

Connection	Function
Power	Uses an On/ Off switch and a standard AC power cord
DSL WAN Port	A 6-pin RJ-14 or RJ-45 port connects the DSL
Ethernet Ports	Four Ethernet 10Base-T ports (8 pin, RJ-45) built in a hub
Mgmt Pin	Use only when instructed by Technical Support.
Console Port	This 8-pin, RJ-45 port provides RS232 connectivity.

Hardware Specifications

Physical Specifications

- Dimensions: 8.4W x 7.0D x 1.7H inches
- 21.3W x 17.8D x 4.3H cm
- Weight: 1.5 lbs.
- .68 Kg.

Operational Environment

- Temperature: 40°F to 105°F
- 5°C to 40°C
- Humidity: 20% to 80% non-condensing

Power Requirements

- AC Voltage: 100 to 120V AC or 220 to 240V AC
- Frequency: 50/60 Hz
- Consumption: 10W maximum
- Built-in power supply, on/off switch

Processor

- Motorola® 32 MHz MPC850
- 4 MB DRAM, 1 MB Flash Memory (2MB on some models)
- 10K30 FPGA 3DES Assist (except 5871)

LAN Interface

- Built-in four port Ethernet hub with four RJ-45 connectors
- Green/Yellow LEDs
- LAN speed of 10 Mbps

WAN Interface

- One Digital Subscriber Line (DSL) interface as follows:
- RJ-14 - (5861/5865) 3/4 pinout
- Others: RJ-45 3/4 pinout

Serial Interface

- One RS-232 asynchronous console or modem port (RJ-45)

Agency Approvals

- CE Mark
- TUV
- Safety: UL 1950, CSA 22.2, EN 60950
- Emissions: FCC Part 15 Class B
- Immunity: EN50082-1

Modem Specifications

DMT/ADSL

- Up to 8 Mbps downstream
- Up to 1 Mbps upstream
- Supports full rate G.DMT (G.992.1), G.lite (G.992.2), G.HS (G.994.1), mgmt (G.997.1) and ANSI T1.413 Issue 2
- Analog telephone line support
- Co-operation with an external splitter
- Co-exists with active ISDN circuit Annex B or ETSI (model 5865)

IDSL

- 2B1Q modulation
- Data rates: 64, 128 or 144 Kbps (144 Kbps is the default)

SDSL

- 2B1Q modulation
- Data rates ranging from 160 to 2,300 Kbps
- Conexant Autobaud support

Software Specifications

Analog Telephone Line Support

- Co-operates with external line splitters

Bridging

- Transparent bridging including Spanning Tree protocol (IEEE 802.1D)
- Bridge filters

Routing

- TCP/IP with RIP1 (RFC 1058), RIP1 compatible and RIP2 (RFC 1389) or static routing on the LAN or WAN
- Novell® IPX with RIP/SAP (RFC 1552)
- DHCP client (RFC 2132)
- DHCP server - Automatic assignment of IP address, mask, default gateway and DNS server addresses to workstations (RFC 2131, 2132)
- DHCP relay agent (RFC 1542)
- DNS relay
- Multiple subnets on LAN
- Virtual routing
- Virtual Router Redundancy Protocol (RFC 2338)

Configuration Management

- Easy Setup web user interface
- Microsoft® Windows configuration management via SNMP
- TFTP download/upload of new software and configuration files
- Performance monitor
- Dynamic event and history logging
- Administration through HTTP, SNMP, Telnet or VT100 terminal
- Network boot uses the BootP server (RFC 2131, RFC 2132)

Dial Backup

- Failover to modem on console port

-
- Web graphical user interface
 - User selectable fail/restore criteria
 - Optional modem connector (DB9 or DB25)
 - Supports L2TP and IPSec tunnel failover

Asynchronous Transfer Mode (ATM)

- Encapsulation (IP, Bridging, and Bridge Encapsulated Routing) (RFC 1483)
- PPP over ATM (LLC and VC multiplexing) (RFC 2364)
- PPP over Ethernet
- Classical IP (RFC 1577)
- AAL5 for data
- Multiple Virtual Circuits (VCs)
- Virtual Circuit (VC) traffic shaping (UBR, VBR, CBR)
- L610 OAM F5 loopback

IP Address Translation

- Network renumbering (RFC 1631)
- Network Address Translation (NAT/PAT)
- LAN servers supported with NAT
- Support for NAT inside an IPSec tunnel

Protocol Conformance Testing

- RFC 1483 (Bay Networks™, Cabletron™, Cisco™, RedBack™)
- PPP over ATM (Cisco, Escalate™, RedBack) (RFC 2364)
- Tested with Copper Mountain™, Interspeed™, Lucent™, New Bridge™, Nokia™, Pair Gain™, Paradyne™, Promatory™, SDSL.

PPP (RFC 1661)

- Data compression of up to 4:1 (STAC™ LZS) (RFC 1974)
- Van Jacobsen header compression (RFC 1144)
- Spoofing and filtering (IP-RIP, IPX-RIP, SAP, Watchdog, serialization)

- Automatic IP and DNS assignment (RFC 1877)
- PPP over Ethernet (RFC 2516)

Security

- User authentication (PAP/CHAP) with PPP (RFC 1334, RFC 1994)
- Password control for Configuration Manager
- SNMP community name reassignment
- HTTP/Syslog/SNMP/Telnet port reassignment, access control list
- Optional VPN software (L2TP, IPSec, IKE, DES, 3DES)
- Firewall (IP filtering)
- 3DES hardware assist (on most models)

Safety and Certifications

Important Information about this device:

When using this device, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons including the following:

- Do not use this product near water. For example, near a bath tub, wash bowl, kitchen sink, or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Avoid blocking any vent openings or exhaust exits on this equipment.
- Caution - Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.

Save these Instructions!

Safety and Emissions Compliance for Efficient Networks Products

Federal Communications Commission (FCC) Statements

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesigned operation.

Radio Frequency Interference Statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. This equipment generates, uses and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause interference to radio communications.

The limits are designed to provide reasonable protection against such interference in a residential situation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna of the affected radio or television.
- Increase the separation between the equipment and the affected receiver.
- Connect the equipment and the affected receiver to power outlets on separate circuits.
- Consult the dealer or an experienced radio/TV technician for help.

This device is equipped with an FCC compliant modular jack and is designed to be connected to the telephone network through a compliant high pass port on a network interface with a PART 68 compliant compatible modular plug. If this device causes harm to the telephone network, the telephone service provider in your area may require the temporary discontinuance of service to your location. Usually advanced warning of a disconnect will be provided. However, if advanced notice is not practical, then the service provider company will notify you, the customer, as soon as possible.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advanced notice in order for you to make necessary modifications to maintain uninterrupted service. If trouble is experienced with this equipment, for repair or warranty information please contact:

Efficient Networks, Inc. Efficient Networks Technical Support Services:

4849 Alpha Road RMA service hours: 8:00am - 5:00pm (CST)
Monday - Friday

Dallas, TX 75244 USA Telephone: +1 (972) 852-1000

Attn: RMA #

Email: support@efficient.com

If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary. There are **NO SERVICABLE PARTS**. Please contact Efficient Networks, Inc. This equipment is not intended for use on public coin phone service provided by the telephone company. Connection to party line service is subject to state tariffs. (Contact the state public utility commission, public service commission or corporation commission for information.) The use of this equipment may be controlled by law in your country. This equipment is hearing aid compatible if used on standard telephone lines with the appropriate interface.

Modifications:

Changes or modifications not expressly approved by Efficient Networks, Inc. could void the users' authority to operate this equipment.

Canadian RF Interference Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of the Canadian Department of Communication.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

European Community (EC) Declaration of Conformity

Efficient Networks, Inc. declare under our sole responsibility that the product model to which this declaration relates is in conformity with the following standard(s) or other normative document(s):

EN 55022: 1994, Limits and methods of measurement of radio interference characteristics of information technology equipment, Class B.

EN 50081-1: 1992, Electromagnetic Compatibility - Generic emissions standard - Part 1: Residential, commercial and light industry following the provisions of The Electromagnetic Compatibility Directive, 89/336/EEC.

EN 50082-1: 1992, Electromagnetic Compatibility - Generic immunity standard - Part 1: Residential, commercial and light industry following the provisions of The Electromagnetic Compatibility Directive, 89/336/EEC.

EN 60950: 1992, Safety of Information Technology Equipment, including Electrical Business Equipment.

Information importante concernant cet appareil

Lorsque vous utilisez cet appareil, les précautions suivantes doivent être prises afin d'éviter les risques d'incendie, de décharge électrique ou de tout accident corporel:

1. Ne pas utiliser cet appareil à proximité de l'eau. Exemple: près d'une baignoire, toilette, lavabo, piscine, etc.
2. Éviter d'utiliser le téléphone (autre qu'un téléphone sans fils) durant un orage électrique. Il peut y avoir un risque possible de décharge électrique provenant de l'électricité dans l'air.
3. Ne pas utiliser le téléphone pour nous informer d'une fuite de gaz à proximité de la fuite.
4. Éviter d'obstruer les ouvertures faites pour la ventilation de cet appareil.
5. Attention - Vérifiez toujours que les fils qui vont à la prise de téléphone au mur sont bien débranchés avant de toucher à l'unité pour la réparer ou la démonter.

Conservez ces instructions!

Conformité des produits Efficient Networks aux normes de sécurité et de taux d'émission

Déclarations de la Commission fédérale des communications (FCC)

Cet appareil est conforme à la section 15 des règlements de la FCC. Son fonctionnement est permis suivant les deux conditions suivantes : (1) cet appareil ne doit pas causer de brouillage préjudiciable, et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences qui peuvent causer un type de fonctionnement non voulu.

Déclaration sur les parasites de haute fréquence

Note : cet équipement a été testé et reconnu conforme aux limites applicables qui ont été définies pour les appareils numériques de classe B, en vertu de la section 15 des règlements de la FCC. Cet équipement produit, utilise et peut émettre de l'énergie sous forme de fréquence radio. Si l'équipement n'est pas installé et utilisé conformément aux instructions, il peut causer une interférence avec les communications radio.

Les limitations sont conçues pour assurer une protection raisonnable contre de telles interférences pour les installations chez le particulier. Toutefois, rien ne garantit que l'interférence ne se produira pas dans certains cas. Si cet équipement cause un fort brouillage à la réception radio et télévision, (ce qui peut être déterminé en éteignant et allumant l'équipement), l'utilisateur est invité à essayer de corriger l'interférence au moyen de l'une ou de plusieurs des moyens suivantes:

- Réorienter ou déplacer l'antenne de réception de la radio ou de la télévision, selon le cas.
- Accroître la distance entre l'équipement et le récepteur concerné.
- Brancher l'équipement et le récepteur concerné dans des prises de courant sur des circuits séparés.
- Contacter le vendeur ou un technicien expérimenté en électronique pour obtenir assistance.

Cet équipement est doté d'une prise modulaire conforme aux normes FCC et est conçu pour être connecté au réseau téléphonique au moyen d'un port rapide d'interface de réseau via une fiche modulaire compatible et conforme à la section 68. Si ce dispositif cause un préjudice au réseau téléphonique, la compagnie de téléphone de votre région peut imposer une interruption temporaire du service à votre domicile. Généralement, un préavis d'interruption de service vous sera communiqué. Toutefois, si ce n'est pas le cas, ce sera votre fournisseur de service, qui vous le fera savoir le plus tôt possible.

Votre compagnie de téléphone peut apporter des changements à ses installations, ses équipements, ses opérations ou ses procédures qui pourraient affecter le fonctionnement du présent équipement. Dans ce cas, la compagnie de téléphone vous donnera un préavis afin de vous permettre de faire les modifications nécessaires pour maintenir un service sans interruption. Si vous éprouvez des difficultés avec cet équipement, contactez Efficient Networks, à l'adresse suivante pour obtenir les informations sur les réparations garanties offertes pour cet équipement:

Efficient Networks, Inc. Services de support technique Efficient Networks :

4849 Alpha Road Heures d'ouverture : 8 h à 17 h du lundi au vendredi

Dallas, TX 75244 USA Téléphone: +1 (972) 852-1000

Att : RMA # Courriel électronique : support@efficient.com

Si cet équipement cause des réels préjudices au réseau téléphonique, la compagnie de téléphone peut exiger que vous débranchiez l'équipement jusqu'à ce que le problème soit résolu. En outre, vous serez avisé de votre droit de déposer une plainte auprès de la FCC si vous le jugez nécessaire. IL N'EST PAS

POSSIBLE DE REPARER INDIVIDUELLEMENT LES COMPOSANTS DE CET EQUIPEMENT. Veuillez alors contacter Efficient Networks, Inc. Cet équipement n'est pas destiné à être utilisé avec les téléphones publics de la compagnie de téléphone. Dans le cas de plusieurs voix sur une même ligne, les tarifs appliqués sont ceux définis par la compagnie de téléphone utilisée. Pour plus d'information vous pouvez contacter votre commission de service public, ou la commission de la fonction publique. L'utilisation de cet équipement peut être juridiquement réglementée dans votre pays. Cet équipement est compatible avec les prothèses auditives lorsqu'elles sont utilisées avec des lignes téléphoniques standards au moyen d'une interface appropriée.

Modifications:

Des changements ou des modifications non formellement approuvés par Efficient Networks, Inc. peuvent annuler le droit de l'utilisateur de se servir de cet équipement.

Déclaration canadienne RF sur L'Interférence

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans les règlements sur l'interférence du ministère canadien des Communications.

AVIS : L'étiquette Industrie Canada identifie que l'équipement est certifié. Cette certification signifie que l'équipement satisfait les exigences de protection, de fonctionnement et de sécurité des réseaux de télécommunication définies dans les documents pertinents relatifs aux exigences techniques d'équipement terminal. Le ministère ne garantie pas que l'équipement fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer cet équipement, les utilisateurs devraient s'assurer qu'il est permis de brancher celui-ci aux installations de la compagnie locale de télécommunications. L'équipement doit également être installé selon une méthode acceptable de connexion. L'utilisateur doit savoir que la conformité aux conditions mentionnées ci-dessus ne peut pas empêcher la détérioration du service dans certains cas.

Les réparations de l'équipement certifié devraient être coordonnées par un représentant désigné du fournisseur. Toute réparation ou modification de l'équipement faite par l'utilisateur ou tout mauvais fonctionnement de l'équipement peut donner à la compagnie de télécommunications un motif pour exiger que l'utilisateur débranche l'équipement.

Les utilisateurs devraient s'assurer pour leur propre protection que les prises électriques de terre des services d'électricité, des lignes téléphoniques et du système métallique interne des conduites d'eau, s'il y a lieu, sont connectées ensemble. Cette précaution peut être particulièrement importante en région rurale. Attention : Les utilisateurs ne doivent pas tenter de faire ces connexions eux-mêmes, mais doivent communiquer avec les autorités d'inspection électrique appropriées ou avec un électricien, selon le cas.

Déclaration de conformité de la communauté européenne (CE)

Efficient Networks, Inc. déclare sous son entière responsabilité que le modèle de l'équipement auquel cette déclaration se rapporte est conforme aux normes ou documents normatifs suivants :

EN 55022 : 1994, Limites et méthodes de mesure des caractéristiques de brouillage radioélectrique de l'équipement de technologie de l'information, classe B.

EN 50081-1 : 1992, Compatibilité électromagnétique - Norme général d'émissions - Section 1 : Résidence, commerce et industrie légère selon les provisions de la directive de compatibilité électromagnétique, 89/336/EEC.

EN 50082-1 : 1992, Compatibilité électromagnétique - Norme générale d'immunité - Section 1 : Résidence, commerce et industrie légère selon les provisions de la directive de compatibilité électromagnétique, 89/336/EEC.

EN 60950 : 1992, Sécurité de l'équipement de technologie de l'information, y compris l'équipement des services d'électricité.

Información importante sobre el Equipo:

Cuando se use este equipo deben seguirse unas precauciones básicas de seguridad, para reducir el riesgo de incendio, descarga eléctrica y daño a personas, incluyendo las siguientes:

1. No usar este producto cerca del agua. Por ejemplo cerca de una bañera, palangana, fregadero de cocina, lavadero, sobre una base húmeda o cerca de una piscina.
2. Evitar el uso de teléfonos (excepto los inalámbricos) durante una tormenta eléctrica. Hay un cierto riesgo de descarga eléctrica procedente de rayos.
3. No usar el teléfono para avisar de un escape de gas en las proximidades del escape.
4. Evitar el bloqueo de cualquier abertura de ventilación o salida en este equipo.
5. Precaution - Desconecte siempre el cable de telefono de su conector mural antes de dar servicio o desensamblar este equipo.

¡Conserve estas instrucciones!

Cumplimiento de Seguridad y Emisiones de los Productos Efficient Networks

Declaración de la Comisión Federal de Comunicaciones (FCC)

Este dispositivo cumple con el apartado 15 de las normas de la FCC. Su operación está sujeta a las siguientes dos condiciones: (1) este dispositivo no debe causar interferencias perniciosas, y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluyendo las interferencias que puede causar una operación no prevista.

Declaración de Interferencias de Radiofrecuencia.

Nota: Este equipo ha sido testeado y está dentro de los límites de un aparato digital de Clase B conforme a la parte 15 de las reglas de la FCC. Este equipo genera, usa y puede irradiar energía de radiofrecuencia. Si no se instala y/o no se usa de acuerdo con las instrucciones, podría causar interferencias a las radiocomunicaciones.

Los límites recogidos en la parte 15 de la norma de la FCC para equipos de clase B están diseñados para proporcionar una protección razonable contra tales interferencias en una situación residencial. Sin embargo, no existe garantía de que no ocurrirán interferencias en una instalación particular. Si el equipo causa interferencias dañinas en la recepción de radio o televisión, lo cual puede determinarse encendiendo y apagando el equipo, se anima al usuario a intentar corregir la interferencia tomando una o más de las siguientes medidas:

- Reorientar o cambiar de sitio las antenas receptoras de las radios o televisores afectados.
- Aumentar la separación entre el equipo y el receptor afectado.
- Conectar el equipo y el receptor afectado en tomas de corriente correspondientes a circuitos separados.
- Consultar al distribuidor o a un técnico experimentado en radio/TV

Este aparato está equipado con una clavija modular que cumple las reglas de la FCC y está diseñada para ser conectada a una red telefónica a través de un puerto high pass en una interfaz de red con un enchufe compatible modular que cumpla el apartado 68. Si este aparato causa daño a la red telefónica, el proveedor del servicio telefónico en su área podría cortar temporalmente el servicio en su ubicación. Normalmente se facilitará un aviso de desconexión. Sin embargo si el avance del aviso no es posible, la compañía proveedora del servicio le notificará a Vd, el cliente, tan pronto sea posible.

Su compañía telefónica puede realizar cambios en instalaciones, equipamiento, operaciones o procedimientos que podrían afectar la operatividad de este equipo. Si esto ocurre, la compañía telefónica le avisará para que pueda realizar las modificaciones necesarias para mantener el servicio sin interrupción. Si se experimentan problemas con este equipo, puede contactar para su reparación u obtener información sobre la garantía con:

Efficient Networks, Inc. Servicio de Soporte Técnico Efficient Networks:
4849 Alpha Road Horario: 8:00am - 5:00pm (CST) Lunes - Viernes
Dallas, TX 75244 USA Teléfono: +1 (972) 852-1000
Attn: RMA # Email: support@efficient.com

Si el equipo causa daño a la red telefónica, la compañía telefónica podría solicitar que desconecte el equipo hasta que se solucione el problema. También podría aconsejarle formular una reclamación con las reglas de la FCC, si Vd. lo considera necesario. No existen RECAMBIOS. Por favor contacte con Efficient Networks, Inc. Este equipo no está preparado para funcionar en un teléfono público de monedas proporcionado por la compañía telefónica. La conexión a servicios de Party Line está sujeta a las tarifas estatales. (Contacte con la

Comisión de Utilidad del Estado Público, la Comisión del Servicio Público o la Comisión de la Corporación para más información). El uso de este equipo puede estar sujeto al control de la ley en su país. Este equipo es compatible con audífono si se usa en una línea de teléfono standard con el interfaz adecuado.

Modificaciones:

Los cambios o modificaciones que no sean aprobados expresamente por Effective Networks, Inc. podrían invalidar la autoridad de los usuarios para operar este equipo.

Declaración Canadiense de Interferencias de RF

Este aparato digital no excede los límites de la Clase B para emisiones de ruido en radiofrecuencia de aparatos digitales tal como se establece en las regulaciones de radio interferencia del Departamento Canadiense de Comunicación.

AVISO: La etiqueta Industry Canada identifica equipos certificados. Esta certificación significa que el equipo cumple los requerimientos de protección de redes de comunicación, operación y seguridad prescritos en los documentos apropiados de los Requerimientos Técnicos de Equipamiento de Terminal. El Departamento no garantiza que el equipo funcione a satisfacción del usuario.

Antes de instalar este equipo, los usuarios deben asegurarse que está permitido conectarlo a las instalaciones de la compañía local de telecomunicaciones. El equipo debe ser también instalado usando un método aceptable de conexión. El cliente debe ser consciente de que el cumplimiento de las condiciones anteriores no excluye la degradación del servicio en algunas situaciones.

Las reparaciones de equipos certificados deben ser coordinadas por un representante designado por el proveedor. Cualquier reparación o alteración hecha por el usuario a este equipo o mal funcionamiento del equipo podría hacer solicitar a la compañía de telecomunicaciones que el usuario desconecte el equipo.

Los usuarios, por su propia protección deben asegurarse que las tomas de tierra eléctricas de la instalación eléctrica, líneas de teléfono y tuberías de agua internas - si existen - están conectadas conjuntamente. Esta precaución es particularmente importante en áreas rurales. Precaución: Los usuarios no deben intentar realizar dichas conexiones por ellos mismos, sino que deben contactar con los inspectores eléctricos o electricistas apropiados.

Declaración de Conformidad de la Comunidad Europea (EC)

Efficient Networks, Inc. declara bajo su única responsabilidad que el equipo al que se refiere esta declaración es conforme a los siguientes standards u otros documentos normativos

EN 55022: 1994, Límites y métodos de medida de radio interferencias característicos de tecnología de equipos informáticos, Clase B.

EN 50081-1: 1992, Compatibilidad Electromagnética - Standard de emisiones genérico - Apartado 1: Residencial, comercial y luz industrial siguiendo las previsiones de la Directiva de Compatibilidad Electromagnética, 89/336/EEC

EN 50082-1: 1992, Compatibilidad Electromagnética -Standard de inmunidad genérico - Apartado 1: Residencial, comercial y luz industrial siguiendo las previsiones de la Directiva de Compatibilidad Electromagnética, 89/336/EEC

EN 60950: 1992, Seguridad en Equipos de Tecnología Informática, incluyendo Equipamiento Eléctrico de Empresa.

Wichtige Information über das Gerät

Bei der Verwendung des Gerätes müssen grundsätzliche Sicherheitsbedingungen berücksichtigt werden, um Feuerrisiko, elektrischen Schock und Verletzung von Personen zu vermeiden, unter anderem:

1. Verwenden Sie dieses Produkt nicht in der Nähe von Wasser, zum Beispiel neben Badewanne, Waschbecken, Spüle oder Waschmaschine, in einem feuchten Keller oder neben einem Swimmingpool.
2. Meiden Sie Telefone (außer Schnurlostelefone) und an die Telefonleitung angeschlossene Geräte wie dieses während eines Gewitters. Es besteht das Risiko eines elektrischen Schlags durch Blitze.
3. Falls Sie eine undichte Gasleitung melden, benutzen Sie hierzu kein Telefon in der Nähe des Lecks.
4. Die Be- und Entlüftungsöffnungen am Gerät dürfen nicht blockiert werden.
5. Trennen Sie das Gerät immer vollständig vom Stromnetz und ziehen Sie alle weiteren Kabel vom Gerät ab, bevor Sie das Gerät in irgendeiner Weise warten oder öffnen.

Heben Sie diese Informationen unbedingt auf!

Konformität für Sicherheit und Störausstrahlung für Produkte von Efficient Networks

Konformität mit den Regelungen der Federal Communications Commission (FCC)

Dieses Gerät entspricht Teil 15 der FCC-Regelungen. Die Benutzung ist den folgenden zwei Bedingungen unterworfen: (1) Dieses Gerät darf keine schädliche Störstrahlung verursachen, und (2) dieses Gerät muß jegliche, empfangene Störstrahlung akzeptieren, einschließlich Störstrahlung, die ein nicht erwünschte Verhalten verursacht.

Konformität bezüglich Hochfrequenzstörungen

Anmerkung: Dieses Gerät ist geprüft worden und entspricht den Grenzwerten für Klasse-B-Digitalgeräte, gemäß Teil 15 der FCC-Regelungen. Dieses Gerät erzeugt, benötigt und kann Hochfrequenzenergie abgeben. Wenn das Gerät nicht korrekt gemäß dieser Anleitung installiert oder verwendet wird, kann es Störungen bei anderen Hochfrequenzgeräten verursachen.

Diese Grenzwerte sind zum angemessenen Schutz gegen solche Störungen innerhalb von Wohngebieten vorgesehen worden. Es besteht jedoch keine Garantie, daß Störungen unter bestimmten Umständen und bei bestimmten Installationen nicht doch auftreten. Wenn dieses Gerät Störungen beim Radio- oder Fernsehempfang verursacht, was durch Ein- und Ausschalten des Gerätes festgestellt werden kann, versuchen Sie bitte, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Ändern Sie die Ausrichtung oder den Standort der Antenne des gestörten Radios oder Fernsehempfänger.
- Erweitern Sie den Abstand zwischen dem Gerät und dem betroffenen Empfänger.
- Schließen Sie das Gerät und den betroffenen Empfänger an verschiedene Stromkreise an.
- Konsultieren Sie bitte den Händler oder einen erfahrenen Rundfunk- und Fernsehtechniker.

Dieses Gerät ist mit einer FCC-gemäßen Anschlussbuchse ausgestattet und zum Anschluss an das Telefonnetz entwickelt. Dies erfolgt über einen standardkonformen Hochpassanschluß an eine Netzwerk-Anschlussbuchse mit einem Modularstecker (kompatibel mit FCC Part 68). Sollte dieses Gerät eine Störung im Telefonnetz verursachen, könnte Ihr Telefonnetzbetreiber zeitweise den Dienst oder Anschluß unterbrechen. Gewöhnlich werden Sie hierüber im Voraus unterrichtet. Sollte dies jedoch nicht möglich sein, wird Ihr Telefonnetzbetreiber Sie so früh wie möglich verständigen.

Telefonnetzbetreiber könnte die Einrichtung, Ausrüstung, Anwendung o.ä. Ihres Anschlusses oder des Dienstes ändern, was sich auf die Verwendung dieses Gerätes auswirkt. Sollte dies geschehen, wird Ihr Telefonnetzbetreiber versuchen, Sie im Voraus zu benachrichtigen und Ihnen so die Möglichkeit geben, notwendige Modifizierungen vornehmen, um eine ununterbrochene Leistung zu gewähren. Sollten Sie Schwierigkeiten mit diesem Gerät haben, oder im Falle einer Reparatur oder bei Fragen zur Garantie, wenden Sie sich bitte an: Efficient Networks, Inc. Efficient Networks Technischer Support:

4849 Alpha Rd.	Servicezeiten: 8:00 - 17:00 (CST; 7 Std. Zeitdifferenz zu MEZ) Montag - Freitag
Dallas, TX 75244 USA	Telefon USA: +1 (972) 852-1000
Attn: RMA #	Email: support@efficient.com

Sollte das Gerät eine Störung des Telefonnetzes verursachen, kann Ihr Telefonnetzbetreiber verlangen daß Sie das Gerät abstellen, bis das Problem gelöst ist. Sie werden auch über Ihr Recht belehrt, bei Bedarf eine Beschwerde bei der FCC einzureichen. Dieses Gerät hat keine auswechselbaren Teile. Bitte kontaktieren Sie bei Bedarf Efficient Networks, Inc. wie oben angegeben. Diese Einrichtung ist nicht zur Verwendung mit einem öffentlichen Fernsprecher

gedacht. Der Betrieb an einem Telefonanschluß, der mit weiteren Personen geteilt wird, kann von Ihrem Telefonnetz- oder Dienstbetreiber oder von der Telekommunikationsbehörde Ihres Landes reglementiert sein. (Für weitere Information wenden Sie sich bitte an Ihren Telefonnetz- oder Dienstbetreiber oder die Telekommunikationsbehörde). Die Verwendung dieses Gerätes kann durch Gesetze in Ihrem Land geregelt sein. Dieses Gerät ist vertraglich mit Hörgeräten im Zusammenhang mit Standardtelefonanschlüssen mit geeigneten Schnittstellen.

Modifizierungen:

Änderungen oder Modifizierungen die nicht ausdrücklich von Efficient Networks, Inc. genehmigt sind, können die Anwendungsgenehmigung zum Betrieb dieses Geräts hinfällig machen.

Konformität bezüglich Hochfrequenzstörungen (für Kanada)

Dieses Digitalgerät überschreitet nicht die für Klasse B festgelegten Grenzwerte für Hochfrequenz Störausstrahlung von Digitalgeräten, wie sie in den *radio interference regulations* vom *Canadian Department of Communication* festgelegt sind.

ANMERKUNG: Das *Industry Canada*-Etikett identifiziert geprüfte Geräte. Dieses Zertifikat bedeutet daß die Geräte Schutz-, Anwendungs- und Sicherheitsvorschriften in Telekommunikationsnetzen entsprechen, wie sie in den relevanten technischen Vorschriften für Terminalgeräte vorgeschrieben sind. Das Ministerium übernimmt keine Garantie für die Betriebsfähigkeit der Geräte.

Vor der Installation des Gerätes stellen Sie bitte sicher, daß eine Genehmigung vorliegt, die den Anschluß an das örtliche Telekommunikationsnetz erlaubt. Das Gerät muß entsprechend den relevanten Anschluss-Standards installiert sein. Sie sollten wissen, daß selbst bei Einhaltung der genannten Standards in bestimmten Situationen eine Verschlechterung des Dienstes eintreten kann.

Reparaturen an geprüften Geräten sollten durch einen Repräsentanten des Lieferanten erfolgen oder koordiniert werden. Jegliche Reparaturen oder Änderungen an den Geräten durch den Verbraucher oder Gerätestörungen können den Telefonnetzbetreiber veranlassen, die Außerbetriebnahme des Gerätes zu verlangen.

Der Verbraucher sollte zum eigenen Schutz sicherstellen, daß die Erdungen der Stromversorgung, der Telfonleitung und von Metallrohrsystemen, falls vorhanden, gemeinsam angeschlossen sind. Diese Sicherheitsmaßnahmen können von besonderer Bedeutung in ländlichen Gegenden sein. Vorsicht: Verbraucher sollten nicht versuchen solche Anschlüsse selbst herzustellen, sie sollten sich wie vorgeschrieben an die geeignete Autorität zur Inspizierung der Elektrik, oder an einen Elektriker wenden.

Europäische Kommunale (EC) Deklaration der Übereinstimmung

Efficient Networks, Inc. erklärt, daß das Produkt, auf welches sich diese Erklärung bezieht, mit den folgenden Normen und Standards übereinstimmt:

EN 55022: 1994, Begrenzungen und Methoden zum Messen der Radiointerferenzcharakteristiken von Informationstechnologiegeräten, Klasse B.

EN 50081-1: 1992, Elektromagnetische Kompatibilität – Generische Abgabemaßstäbe – Teil 1: Heim-, kommerzielle- und Leichtindustrie folgen den Bestimmungen der Elektromagnetischen Übereinstimmungsdirektive, 89/336/EEC.

EN 50082-1: 1992, Elektromagnetische Kompatibilität – Generische Immunitätsmaßstab – Teil 1: Heim-, kommerzielle- und Leichtindustrie folgen den Bestimmungen der Elektromagnetischen Übereinstimmungsdirektive, 89/336/EEC.

EN 60950: 1992, Sicherheit von Informationstechnologiegeräten, inklusive elektrischen Bürogeräten. Die CE-Konformitätserklärung gemäß EMC Klasse B für dieses Gerät wird erfüllt, wenn Aufbau und Verkabelung nach den Angaben im Handbuch und den darin aufgeführten Unterlagen, wie z.B. Montageanleitungen, Montagevorschriften, Kabellisten u.ä. vorgenommen wird. Abweichungen von den Vorgaben oder eigenständige Änderungen beim Aufbau können zu einer Verletzung der CE-Anforderungen führen. In solchen Fällen wird die Konformitätserklärung ungültig und die Verantwortung geht auf den Verursacher der Abweichung über.

Support

For specific product support, contact the organization that provided or sold the equipment to you. If you need to contact your Network Service Provider for technical support, please have the following information ready:

- Router model number (on the bottom of the unit)
- Router software version (displayed on the Command Line and Web User Interface)
- Date of purchase
- OS Type (e.g. Windows 95, 98, 2000, NT, MacOS, or Unix)
- A detailed description of the problem



CAUTION:

Instructions for trained service personnel only: Danger of explosion if the battery is incorrectly installed. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

A

Access Control.....	3-2
Additional Features	3-1
Administration Login.....	1-5
ADSL Specifications	5-5
Agency Approvals	5-5
Analog telephone line support.....	5-6
ATM specifications	5-7

B

Back Panel, 5800 Series.....	5-3
Bridging specifications	5-6

C

Command Line Interface	3-30
Configuration management specifications	5-6
Configuring Your Computer	1-4
Connecting Your Router	1-3
Contents, package	1-2

D

Dial Backup	3-14
Dial Backup specifications	5-6
DMT/ADSL.....	5-5
Dynamic Host Configuration Protocol	2-14

E

Easy Setup.....	2-1, 2-2
Environment	
operational	5-4
environmental.....	5-4

F

Feature Activation.....	3-4
Features, Additional	3-1
Front Panel	5-1

H

Hardware Specifications	5-4
-------------------------------	-----

I

IDSL Specifications	5-5
IKE/IPSec Configuration.....	3-16

Installation	1-1
Installation requirements	1-1
Interface	
LAN	5-4
serial.....	5-5
WAN.....	5-4
Introduction	1-1
IP address translation specifications	5-7

L

LAN Interface.....	5-4
Local Area Network Configuration	2-16
Login.....	1-5

M

Modem specifications	5-5
----------------------------	-----

N

NAT Settings	3-10
Network Service Provider requirements	1-1

O

Operational environment	5-4
-------------------------------	-----

P

Package contents	1-2
PC requirements	1-1
Physical specifications	5-4
Point-to-Point Protocol over ATM.....	2-4
Point-to-Point Protocol over Ethernet over PPPoA.....	2-6
Point-to-Point Protocol over Ethernet over RFC 1483	2-8
Power requirements	5-4
PPP specifications	5-7
Processor.....	5-4
Product specifications	5-1
Protocol conformance testing.....	5-7

R

Requirements	
installation	1-1
Network Service Provider.....	1-1
PC	1-1
power	5-4
RFC 1483 MAC Encapsulated Routing.....	2-12
RFC 1483 Networking.....	2-10

Router	
Connecting	1-3
Login	1-5
Router Information Screen	2-1
Routing specifications	5-6

S

Screen	
Access Control	3-2
Current Date and Time.....	3-6
Dial Backup	3-14
Dynamic Host Configuration Protocol	2-14
Feature Activation	3-4
IKE/IPSec Information.....	3-16
Local Area Networking Configuration.....	2-16
NAT Settings	3-10
Point-to-Point Protocol	2-4
Point-to-Point Protocol over Ethernet over PPPoA	2-6
Point-to-Point Protocol over Ethernet over RFC 1483	2-8
RFC 1483 MER Networking.....	2-12
RFC 1483 Networking.....	2-10
Router Information	2-1
Set DHCP	3-8
Set Firewall	3-12
SDSL Specifications	5-5
Security specifications	5-8
Serial Interface	5-5
Set DHCP	3-8
Set Firewall	3-12
Setting The Date and Time	3-6
Software Specifications	5-6
Specifications	5-4
ADSL/DMT	5-5
analog telephone line support.....	5-6
ATM.....	5-7
bridging	5-6
configuration management.....	5-6
Dial Backup	5-6
hardware	5-4
IDSL	5-5
IP address translation	5-7
LAN Interface	5-4
modem	5-5
physical	5-4
power	5-4
PPP	5-7
processor	5-4
protocol conformance testing	5-7
routing	5-6

SDSL.....	5-5
security.....	5-8
Serial interface	5-5
software.....	5-6
WAN Interface.....	5-4
Specifications, product	5-1

T

Testing, protocol conformance	5-7
-------------------------------------	-----

W

WAN Interface	5-4
---------------------	-----