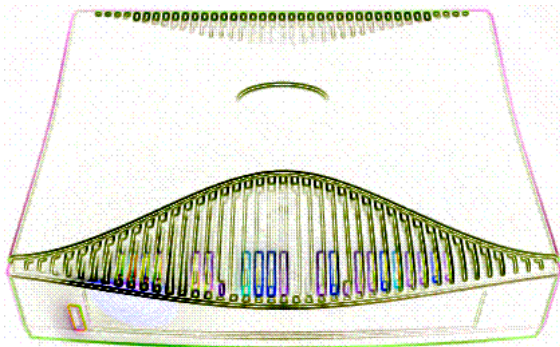


NETOPIA™ D- AND R-SERIES EQUIPMENT

Firmware Version 4.10 Addendum



netopia®

Copyright

©2001, Netopia, Inc., v.112901
All rights reserved. Printed in the U.S.A.

This manual and any associated artwork, software, and product designs are copyrighted with all rights reserved. Under the copyright laws such materials may not be copied, in whole or part, without the prior written consent of Netopia, Inc. Under the law, copying includes translation to another language or format.

Netopia, Inc.
2470 Mariner Square Loop
Alameda, CA 94501-1010
U.S.A.

Part Number

For additional copies of this electronic manual, order Netopia part number
6160038-PF-01

Contents

Chapter 1 — Introduction.....	1-1
Chapter 2 — What's New in 4.10	2-1
R5300 T1 Router Data Link Encapsulation Enhancements	2-2
Telnet Server Port, Client Destination Port, and Web Security Access.....	2-4
Configurable Ping Source IP Address	2-6
Log Packet Filter Violations.....	2-7
Layer 2 Failure Timer for Backup	2-9
IPsec and PPTP Application Level Gateways for VPNs	2-10
Unaccelerated 3DES Encryption Support	2-10
Scheduled Connection Enhancements	2-10
New default behavior: Demand Allowed.....	2-10
New Scheduled Connection type: Random Retry...	2-10
Worm Attack Protection TCP Stack Changes	2-12
Chapter 3 — CompuServe Login Protocol	3-1
CompuServe Login Protocol Configuration.....	3-1
Chapter 4 — RADIUS Client Support and Web Security Enhancements	4-1
Overview	4-1
RADIUS Client Configuration	4-2
Restricting Device Web Server Access to the LAN	4-4
Warning alerts	4-5
MultiNAT Enhancements.....	4-6
Multiple ATM Permanent Virtual Circuit Support	4-6
Multiple ATM PVC overview	4-6
Multiple ATM PVC configuration	4-7
Changing a circuit	4-8

Adding a circuit	4-10
Monitoring multiple virtual circuits	4-11
Multilink PPP-based DSL Bonding Support for ADSL and SDSL Routers	4-14
RFC1973 LMI Support	4-16
Copper Mountain DHCP Server Support.....	4-17
Overview	4-17
Configuration	4-18
PPP Ethernet LAN Reconfiguration	4-22
Configuration	4-22
Quick View	4-23
RIP Profile Options	4-24
Connection Profile Changes Require COMMIT.....	4-25
Backup Enhancements.....	4-26
47-Character PPP Authentication String Support.....	4-26
Chapter 5 — Multiple ATM Permanent Virtual Circuit Support	5-1
Multiple ATM PVC overview	5-1
Multiple ATM PVC configuration	5-2
Changing a circuit	5-3
Adding a circuit.....	5-5
Monitoring multiple virtual circuits	5-6
Chapter 6 — Enhanced Netopia Router SDSL Interoperability Support.....	6-1
Operation Mode	6-2
Non-zero Virtual Path Identifier (VPI) support	6-3
LLC/SNAP encapsulated PPP support (RFC 2364) ..	6-4
Chapter 7 — Filtering on the LAN interface.....	7-1
Chapter 8 — PPP over Frame Relay for R3100 and R7100 Routers.....	8-1
Easy Setup method	8-2
Advanced WAN Configuration method.....	8-4

Chapter 9 — PPP over Ethernet	9-1
Chapter 10 — Version 4.6 Feature Enhancements	10-1
Extended IP Compression Protocol Options.....	10-1
Increased Static Route Count	10-1
Internet Control Message Protocol Filtering.....	10-2
Console Password Confirmation.....	10-4
Delayed Remote Configuration Change Toggle	10-6
User-definable DHCP Lease Times	10-8
RFC1973 LMI Support	10-9
Copper Mountain DHCP Server Support.....	10-10
Overview	10-10
Configuration	10-11
PPP Ethernet LAN Reconfiguration.....	10-15
Configuration	10-15
Quick View.....	10-16
RIP Profile Options	10-17
Connection Profile Changes Require COMMIT.....	10-18
47-Character PPP Authentication String Support.....	10-19
Chapter 11 — DSL Bonding.....	11-1
About DSL Bonding	11-1
Supported equipment.....	11-1
What DSL Bonding does	11-2
Netopia DSL Bonding.....	11-2
Bonded DSL Configuration	11-3
Multilink PPP for Bonded IDSL and Leased ISDN Routers	11-6
Multilink PPP Configuration	11-7
Easy Setup method	11-7
Advanced WAN Configuration method.....	11-9
Monitoring.....	11-12
Quick View.....	11-12
System Information	11-12
WAN Event History	11-13

Multilink PPP-based DSL Bonding Support for ADSL and SDSL Routers.....	11-14
Chapter 12 — DSL and Leased Line Backup.....	12-1
WAN Configuration	12-3
Backup Configuration screen.....	12-7
IP Setup screen	12-8
Connection Profiles	12-9
Using Scheduled Connections with Backup	12-9
Management/Statistics.....	12-11
QuickView	12-13
Event Logs	12-13
SNMP Support	12-13
Backup Enhancements.....	12-14
Chapter 13 — IP Address Serving Enhancements	13-1
Overview	13-1
Configuring the IP Address Server	13-2
DHCP Relay Agent.....	13-7
Chapter 14 — Virtual Private Networks (VPNs).....	14-1
Overview	14-1
About PPTP Tunnels	14-4
PPTP configuration.....	14-4
PPTP Tunnel Configuration for Windows NT.....	14-7
Encryption Support	14-8
VPN Default Answer Profile	14-10
VPN QuickView	14-11
Dial-Up Networking for VPN	14-12
Installing Dial-Up Networking	14-12
Creating a new Dial-Up Networking profile	14-13
Configuring a Dial-Up Networking profile	14-14
Installing the VPN Client	14-16
Windows 95 VPN installation.....	14-16

Windows 98 VPN installation.....	14-16
Connecting using Dial-Up Networking	14-17
About ATMP Tunnels.....	14-18
ATMP configuration	14-18
Allowing VPNs through a Firewall	14-22
PPTP example	14-23
ATMP example	14-26
Windows Networking Broadcasts.....	14-28
Chapter 15 — Internet Key Exchange (IKE) IPsec Key Management.....	15-1
Overview	15-1
Internet Key Exchange (IKE) Configuration.....	15-2
Adding an IKE Phase 1 Profile	15-4
Changing an IKE Phase 1 Profile.....	15-8
Key Management	15-9
IPsec WAN Configuration Screens.....	15-14
IPsec Manual Key Entry	15-16
VPN Quickview.....	15-17
WAN Event History Error Reporting.....	15-18
Chapter 16 — Multiple Network Address Translation (MultiNAT)	16-1
Overview	16-2
Features.....	16-2
Enhancements.....	16-5
Supported traffic.....	16-6
MultiNAT Configuration	16-7
Basic configuration – Easy Setup Profile.....	16-7
Advanced configuration – Server Lists and Dynamic NAT.....	16-8
IP setup.....	16-9
Modifying map lists	16-14
Moving maps	16-16

Adding Server Lists	16-18
Modifying server lists	16-21
Deleting a server	16-23
Binding Map Lists and Server Lists	16-24
IP profile parameters	16-24
IP Parameters (WAN Default Profile)	16-26
WAN Ethernet configuration	16-28
Default Answer Profile	16-30
NAT Associations	16-31
MultiNAT Configuration Example	16-33
Firmware Upgrades and NAT	16-37
Chapter 17 — Connection Metering	17-1
Web-based management pages	17-1
System Information page	17-2
Frame Relay Statistics page	17-4
Connection Status page	17-5
Connect/Disconnect page	17-6
Router Budget Configuration page	17-7
Connection Budgets page	17-8
Connection Budget Configuration page	17-9
Budget Statistics page	17-10
Event History pages	17-11
Console-based management screens	17-13
Chapter 18 — R5300-Series T1 Router Feature Enhancements	18-1
T1 Line Configuration	18-1
Management LED Indication of Local/Remote Loopback and Blue Alarm States	18-3
T1 Diagnostics for R5300 Routers	18-3
T1 Line Statistics and Diagnostics screen	18-3
Chapter 19 — Configurable Hardware (MAC) Address for R9100 Routers	19-1

Chapter 20 — New R7100 SDSL Router Features	20-1
PPP over SDSL for R7100 Routers	20-1
Priority Queuing for R7100 Routers	20-4
Chapter 21 — Miscellaneous Notes.....	21-1
DNS Proxy and Caching Behavior	21-1
SNMP Community String Defaults	21-1
16 Filter Rule Limitation Change	21-1
Correction to Filtering Documentation.....	21-1

Index

Chapter 1

Introduction

This addendum includes important information that supplements the *Netopia Router User's Reference Guide* with information for the Netopia version 4.10 firmware release. Please read it carefully, along with the *Netopia Router User's Reference Guide*.

The version 4.10 firmware release contains several major new features and feature enhancements, covered in the following chapters:

- "What's New in 4.10" in Chapter 2
 - "R5300 T1 Router Data Link Encapsulation Enhancements" on page 2-2
 - "Telnet Server Port, Client Destination Port, and Web Security Access" on page 2-4
 - "Configurable Ping Source IP Address" on page 2-6
 - "Log Packet Filter Violations" on page 2-7
 - "Layer 2 Failure Timer for Backup" on page 2-9
 - "IPsec and PPTP Application Level Gateways for VPNs" on page 2-10
 - "Unaccelerated 3DES Encryption Support" on page 2-10
 - "Scheduled Connection Enhancements" on page 2-10
 - "Worm Attack Protection TCP Stack Changes" on page 2-12

- "CompuServe Login Protocol" in Chapter 3

Some ISPs use the CompuServe Login Protocol to authenticate dialup connections. Introduced in firmware version 4.9, the firmware provides the ability to use the CompuServe Login Protocol when establishing a remote connection over an asynchronous WAN interface.

- "RADIUS Client Support and Web Security Enhancements" in Chapter 4
- "Multiple ATM Permanent Virtual Circuit Support" in Chapter 5

Introduced in version 4.8, the firmware supports up to eight permanent virtual circuits on cell-based SDSL (ATM over SDSL) and ADSL routers.

- "Enhanced Netopia Router SDSL Interoperability Support" in Chapter 6

Introduced in version 4.7.2, the firmware offers SDSL support for DSLAM vendors including Lucent Stinger, Paradyne, and Nortel Networks, as well as Nokia DSLAM settings including Locked, Fixed, and EOC Fast.

- "Filtering on the LAN interface" in Chapter 7

This permits multiple IP addresses or subnets on the Ethernet LAN to be kept separate from one another and operate as virtual independent networks sharing a single Internet connection.

- "PPP over Frame Relay for R3100 and R7100 Routers" in Chapter 8
- "PPP over Ethernet" in Chapter 9

■ “Version 4.6 Feature Enhancements” in Chapter 10

- “Extended IP Compression Protocol Options” on page 10-1
- “Increased Static Route Count” on page 10-1
- “Internet Control Message Protocol Filtering” on page 10-2
- “Console Password Confirmation” on page 10-4
- “Delayed Remote Configuration Change Toggle” on page 10-6
- “User-definable DHCP Lease Times” on page 10-8
- “RFC1973 LMI Support” on page 10-9
- “Copper Mountain DHCP Server Support” on page 10-10
- “PPP Ethernet LAN Reconfiguration” on page 10-15
- “RIP Profile Options” on page 10-17
- “Connection Profile Changes Require COMMIT” on page 10-18
- “47-Character PPP Authentication String Support” on page 10-19

■ “DSL Bonding” in Chapter 11

Introduced in firmware version 4.5, a technique called DSL bonding, also known as inverse multiplexing, permits combining two SDSL links or up to four IDSL links into a single high-bandwidth connection. The firmware supports DSL bonding as implemented in Copper Mountain Networks DSL carrier equipment.

Netopia's Bonded IDSL and leased ISDN routers, which support up to four BRI circuits, allow customers who, because of line quality problems, were previously limited to a 144 Kbps IDSL connection, to enjoy speeds of up to 576 Kbps.

This bonding technology supports:

- The Netopia R7171 SDSL Router and the Netopia D7171 SDSL DSU, which support two SDSL circuits for speeds of over 3 Mbps.
- The Netopia R3232-I IDSL Router and Netopia D3232-I IDSL DSU, which support up to four BRI circuits for speeds of up to 576 Kbps

■ “DSL and Leased Line Backup” in Chapter 12

Introduced in firmware version 4.5, this feature provides all Ethernet, DSL, and traditional leased line models a failure and recovery mechanism in the event of a physical or data link protocol failure on the primary WAN connection. The dial backup is provided through an asynchronous device such as a V.90 or ISDN modem connected to the auxiliary serial port or, if installed, a V.90 modem or ISDN WAN module installed in the second internal WAN interface slot.

■ “IP Address Serving Enhancements” in Chapter 13

Introduced in version 4.6, the firmware adds flexibility to the built-in IP address serving capability of all Netopia Routers. You now have the ability to:

- Exclude one or more IP addresses from the address serving pool so the addresses will not be served to clients.
- Reserve a particular IP address for a client with a particular Ethernet MAC address.

- View the host name associated with a client to the router has leased an IP address.
- Have the router's Ethernet IP address(es) to overlap the DHCP address serving pool(s).
- Forward DHCP requests (DHCP Relay Agent) from clients on the LAN to a remote DHCP server, and to pass the replies back to the requesting client systems.

■ "Virtual Private Networks (VPNs)" in Chapter 14

Introduced in firmware version 4.4, this feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around two key technologies: PPTP and ATMP.

Beginning with firmware version 4.6, Netopia routers support Microsoft's Challenge Handshake Protocol, version 2 (MS-CHAP-V2) and 128-bit ("strong") encryption.

See "MS-CHAP V2 and 128-bit strong encryption" on page 14-9.

- "PPTP Tunnel Configuration for Windows NT" on page 14-7

Some VPN networks that use Microsoft Windows NT PPTP Network Servers require additional authentication information, called *Windows NT Domain Name*, when answering PPTP tunnel connection requests. Version 4.8 supports this option.

■ "Internet Key Exchange (IKE) IPsec Key Management" in Chapter 15

The version 4.10 firmware supports Internet Key Exchange (IKE) for secure encrypted communication over a VPN tunnel.

IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs).

■ "Multiple Network Address Translation (MultiNAT)" in Chapter 16

Introduced in firmware version 4.4, these enhancements offer businesses and service providers added security, convenience, and flexibility in designing their IP addressing scheme. Using MultiNAT, businesses can benefit from the inherent security of address translation, without giving up the flexibility of multiple "real" Internet addresses. Further, providers can offer their LAN customers dedicated blocks of IP addresses without requiring changes to the IP addresses of individual workstations.

An enhancement added in firmware version 4.6 is 1:1 dynamically assigned NAT mapping, in which an internal private address can be assigned to a public address from a NAT address pool.

- [“Connection Metering” in Chapter 17](#)

Introduced in firmware version 4.3.4, this feature offers system-wide time- and packet-based connection metering and budgeting through the Web-based management screens. It allows monitoring and enforcing of preset budget rules on three separate Connection Profiles.

- [“T1 Diagnostics for R5300 Routers” in Chapter 18](#)

Introduced in firmware version 4.3.4, this feature offers real-time diagnostic and loopback testing with cumulative statistics for a variety of tests for Netopia R5300 routers with integrated T1 CSU/DSUs.

- [“Configurable Hardware \(MAC\) Address for R9100 Routers” in Chapter 19](#)

Introduced in firmware version 4.3.4, for Netopia R9100 Ethernet-to-Ethernet routers, this feature offers the capability of configuring an arbitrary hardware (MAC) address on the Ethernet WAN port.

- [“New R7100 SDSL Router Features” in Chapter 20](#)

Introduced in firmware version 4.4, for Netopia R7100 routers the firmware offers PPP data link encapsulation over the SDSL link.

It also offers the ability to prioritize delay-sensitive data, such as voice, over the SDSL link (priority queuing).

- [“Miscellaneous Notes” in Chapter 21](#)

- [“DNS Proxy and Caching Behavior” in Chapter 21](#)

- [“SNMP Community String Defaults” in Chapter 21](#)

- [“16 Filter Rule Limitation Change” in Chapter 21](#)

- [“Correction to Filtering Documentation” in Chapter 21](#)

Chapter 2

What's New in 4.10

The version 4.10 firmware release adds major new functionality to all Netopia R-Series routers. The version 4.10 firmware offers the following new features:

- [“R5300 T1 Router Data Link Encapsulation Enhancements” on page 2-2](#)
R5300 T1 Router data link encapsulation enhancements include Multiprotocol Encapsulation over ATM Adaptation Layer 5 (RFC 1483) support (Bridged and Routed), PPPoE support, and LLC SNAP PPP support.
- [“Telnet Server Port, Client Destination Port, and Web Security Access” on page 2-4](#)
- [“Configurable Ping Source IP Address” on page 2-6](#)
- [“Log Packet Filter Violations” on page 2-7](#)
- [“Layer 2 Failure Timer for Backup” on page 2-9](#)
- [“IPsec and PPTP Application Level Gateways for VPNs” on page 2-10](#) to allow multiple tunnels to multiple remote hosts.
- [“Unaccelerated 3DES Encryption Support” on page 2-10](#)
- [“Internet Key Exchange \(IKE\) IPsec Key Management” in Chapter 15](#)
A compatibility option has been added to IKE to allow “dangling” Phase 2 SAs, as well as several other enhancements and bug fixes.
- [“Scheduled Connection Enhancements” on page 2-10](#), including:
 - New default behavior: Demand Allowed
 - Random Retry Scheduled Connection Type, which attempts to bring connection up three times as quickly as possible, then backs off a specified number of minutes per retry.
- [“Worm Attack Protection TCP Stack Changes” on page 2-12](#)
TCP stack changes have been introduced to avoid, and allow for recovery of, “stuck” TCP connections (SYN and TIMED-WAIT).

R5300 T1 Router Data Link Encapsulation Enhancements

The version 4.10 firmware release adds Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5) encapsulation, also called RFC1483 encapsulation. RFC1483 support includes both Bridged and Routed 1483, and, in Bridged 1483 mode, includes PPP over Ethernet (PPPoE) support.

Previously, the R5300 T1 router supported only Frame Relay, HDLC, and PPP. PPP support included only VC Multiplexed PPP, and not LLC SNAP PPP. The version 4.10 firmware adds LLC SNAP PPP support. The **T1 Line Configuration** screen offers the new options.

You can access the T1 Line Configuration screen either from the Easy Setup Menus or from the WAN Configuration menus. The WAN Configuration menus offer some additional options not found in the Easy Setup menus. The sample screen shown below is from the WAN Configuration menus.

T1 Line Configuration

Operation Mode...	Normal
Line Encoding...	B8ZS
Framing Mode...	ESF
Transmit ANSI PRMs:	No
Number of DS0 Channels:	1
First DS0 Channel:	1
Buildout (-dB)...	0-0.6
Channel Data Rate...	+-----+
Clock Source...	+-----+
Data Link Encapsulation...	PPP
PPP over Frame Relay Enabled:	HDLC
	Frame Relay
	RFC1483
	+-----+

The **Data Link Encapsulation** pop-up menu allows you to choose among PPP, HDLC, Frame Relay, or RFC1483.

- If you select **Frame Relay** data link encapsulation, the **PPP over Frame Relay Enabled** toggle item appears. This allows you to toggle PPP over Frame Relay **On** or **Off**.

If you toggle **PPP over Frame Relay** to **On**, the next two fields, **DLCI** and **LMI** appear, allowing you to specify these settings. If PPP over Frame Relay is Off, these fields do not appear.

Data Link Encapsulation...	Frame Relay
PPP over Frame Relay Enabled:	On
DLCI:	16
LMI:	None

- If you select **RFC1483** data link encapsulation, the next field **RFC1483 Mode** appears. This allows you to select either **Bridged 1483** or **Routed 1483** from a pop-up menu.

If you are using **Bridged 1483** mode, the next field **PPP over Ethernet (PPPoE)** appears. You can toggle PPPoE either **On** or **Off**.

Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Bridged 1483
PPP over Ethernet (PPPoE):	Off

- If you select **PPP** data link encapsulation, a **PPP Mode** pop-up menu option appears. You can choose either **VC Multiplexed** or **LLC SNAP**.

Data Link Encapsulation...	PPP
PPP Mode...	VC Multiplexed

Telnet Server Port, Client Destination Port, and Web Security Access

The version 4.10 firmware release offers the ability to specify the port number on which the router listens for incoming telnet management sessions. Previously, Netopia routers could listen only on port 23.

You specify the Telnet Server Port in the **Advanced Security Options** screen.



Advanced Security Options

Security Databases... Local only

RADIUS Server Addr/Name:

RADIUS Server Secret:

Alt RADIUS Server Addr/Name:

Alt RADIUS Server Secret:

RADIUS Identifier:

RADIUS Server Authentication Port: 1812

Telnet Server Port: 23

Device Web Server via LAN only: Yes

LAN (EN Hub) IP Filter Set...

Remove Filter Set

By default, the **Telnet Server Port** is set to the standard telnet reserved port number 23. The range of port numbers that are allowed is 1 through 65535, except port 80, port 1723, and any other port on which the Netopia is listening. When the port number is changed, new incoming telnet sessions may connect only to the new port, and all existing sessions will remain connected to the old port number.

Certain kinds of Internet worm attacks overburden web servers by consuming their resources and effectively causing them to cease functioning.

Beginning with firmware version 4.9.4, the router defaults to disallowing web access to its own internal web server from the WAN. In other words, you will be able to access the router's web server from the LAN only. This prevents web-propagated worms on the Internet from disabling routing functions.

- By default, **Device Web Server via LAN only** is set to **Yes**.
- Some administrators use web-based monitoring tools that access the Netopia Router's built-in web server remotely, from the WAN. In that case, **Device Web Server via LAN only** should be toggled to **No**.

When originating a telnet client session from the router, you also have the ability to specify the port number on which to connect to the remote host.

You specify the Telnet Destination Port in the **Telnet** screen.



Telnet

Host Name or IP Address:

Destination Port: 23

Control Character to Suspend: Q

START A TELNET SESSION

Resume Suspended Session...

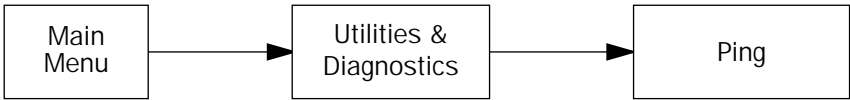
Terminate Suspended Session...

Enter the IP Address/Domain Name of a host.

Configurable Ping Source IP Address

The version 4.10 firmware offers the ability to specify which router interface IP address to use as a source address when sending pings. If the ping goes out through an interface that has NAT enabled, the ping source address will be translated. The ability to specify the source IP address is optional. If you do not specify the source IP address, the router will decide which IP address to use.

You specify the Source IP Address in the **ICMP Ping** screen.



ICMP Ping

Name of Host to Ping:

Packets to Send: 5

Data Size: 56

Delay (seconds): 1

Specify source address: Yes

Source IP address: 0.0.0.0

START PING

Status:

Packets Out: 0

Packets In: 0

Packets Lost: 0 (0%)

Round Trip Time (Min/Max/Avg): 0.000 / 0.000 / 0.000

Enter the IP Address/Domain Name of a host to ping.
Send ICMP Echo Requests to a network host.

- If you toggle **Specify source address** to **Yes** (the default is **No**), the next field **Source IP address** appears.
- **Source IP address** is editable. Enter an IP address to use as the source address.

If the source address is not a valid router interface IP address, you will not be allowed to ping using that source IP address. The screen will display an “Illegal value” message on the **Status** line.

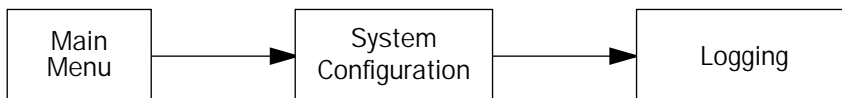
When the ping is started, the source address is checked again to ensure that the specified source address is a valid router interface IP address.

Log Packet Filter Violations

The version 4.10 firmware offers the ability to output filter violations to a log via syslog.

Previously, there was no way of finding out when, or how many packets were filtered. The version 4.10 firmware provides an option to enable logging filter violations via the syslog daemon. If you enable it, each time a packet is filtered, the router will send a message to the configured Syslog client. It reports the name of the filter set that filtered the packet, and enough information about the packet to facilitate surveillance on the filtered interface.

You enable filter violations logging in the **Logging Configuration** screen.



Logging Configuration

WAN Event Log Options	
Log Boot and Errors:	Yes
Log Line Specific:	Yes
Log Connections:	Yes
Log PPP, DHCP, CNA:	Yes
Log IP:	Yes
Syslog Parameters	
Syslog Enabled:	No
Hostname or IP Address:	
Facility...	Local 0
Log Filter Violations:	No
DUMP WAN LOG	
Return/Enter accepts * Tab toggles * ESC cancels.	

The **Syslog Parameters** section of the Logging Configuration screen includes the **Log Filter Violations** toggle item.

- First, toggle **Syslog Enabled** to **Yes**.
- Then you can enable **Log Filter Violations** by toggling it to **Yes**, or disable it by toggling it to **No**. When enabled, the router will log filter violations via the syslog daemon.

2-8 Firmware Version 4.10 Addendum

The vital packet specifications are: source/destination IP address, packet size, protocol type, and additional protocol information if the protocol is: TCP, UDP, or ICMP. The additional protocol information, in the case of TCP or UDP, will be the source and destination ports. In the case of ICMP, the additional information will be the ICMP type and code.

Example messages captured by the Syslog client:

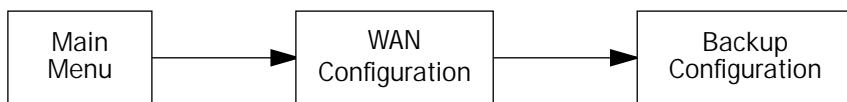
```
DateTime, Facility, Priority, Source, Message
7/9/01 2:05:43 PM, 16, 4, 192.168.2.2, Filter set 'Basic Firewall'
Violation - srcIP = 192.168.2.1 dstIP = 192.168.1.1 size: 132,
protocol: 50.
7/9/01 2:05:33 PM, 16, 4, 192.168.2.2, Filter set 'Basic Firewall'
Violation - srcIP = 192.168.2.5 dstIP = 192.168.1.1 size: 78,
protocol: ICMP, type: 8 code: 0.
7/9/01 2:05:27 PM, 16, 4, 192.168.2.2, Filter set 'Basic Firewall'
Violation - srcIP = 192.168.2.1 dstIP = 192.168.1.1 size: 124,
protocol: UDP, src port: 514 dst port: 514.
7/9/01 2:05:16 PM, 16, 4, 192.168.2.2, Filter set 'Basic Firewall'
Violation - srcIP = 192.168.2.5 dstIP = 192.168.1.1 size: 66,
protocol: TCP, src port: 1109 dst port: 23.
```

Layer 2 Failure Timer for Backup

The version 4.10 firmware offers an option to specify a **Layer 2 Failure Timer**. The timer is used to specify a shorter time period to attempt to recover from a failure. For Netopia routers with the backup feature, the layer 2 failure timer offers increased flexibility and reduced connectivity downtime.

Previously, the automatic backup and recovery functions for all non-physical connection failures were controlled by two timers: a failure timer, and a recovery timer. The router would switch into backup mode when it detected the primary connection being down after the failure timer expired. When in backup mode, the router would switch into primary mode when the recovery timer expired. While attempting to recover to primary mode, the failure timer would count down. For the entire failure timer countdown the router remained disconnected from the network.

You specify the **Layer 2 Failure Timer** in the Backup Configuration screen.



Backup Configuration

Backup Parameters	
Backup to Auxiliary Port...	Automatic
Requires Failure of (minutes):	2
Ping Host Name or IP Address:	
Recovery to EN...	Automatic
Requires Recovery of (minutes):	10
Auto-Recovery on loss of Layer 2:	Yes
Layer 2 Failure Timer (seconds):	20
Clear Backup Call only if idle:	No
Data Link Encapsulation is	Async PPP

Enter override Failure timer on loss of Layer 2. 0 is default Failure timer.
Enter Information supplied to you by your telephone company.

Setting **Layer 2 Failure Timer** to zero will cause it to be equal to the **Requires Failure of** value that you specify. The maximum allowed setting for this item is 65535.

IPsec and PPTP Application Level Gateways for VPNs

The version 4.10 firmware supports an *IPsec Application Level Gateway* (ALG) and a *PPTP Application Level Gateway*. This feature allows multiple hosts behind a single PAT address simultaneously to establish and maintain tunnels to multiple remote hosts.

No special configuration is required and the number of simultaneous tunnels is unlimited. See “[Virtual Private Networks \(VPNs\)](#)” on page 14-1 and “[Internet Key Exchange \(IKE\) IPsec Key Management](#)” on page 15-1 for more information on IPsec and PPTP tunnels.

Note: IKE negotiations and the first ESP exchange may not be overlapped to a single remote host.

Unaccelerated 3DES Encryption Support

The version 4.10 firmware now supports 3DES encryption on all R-Series routers for VPN tunnels, as a standard configurable option. Previously, 3DES encryption was only supported on Netopia XL model R-Series routers with the XL VPN accelerator card installed. See “[Virtual Private Networks \(VPNs\)](#)” on page 14-1 and “[Internet Key Exchange \(IKE\) IPsec Key Management](#)” on page 15-1 for more information.

Additionally, IPcomp compression is supported only on XL model routers.

Scheduled Connection Enhancements

The version 4.10 firmware offers several changes and enhancements to the Scheduled Connections features. For more information about Scheduled Connections, see the *User's Reference Guide* section “Scheduled Connections.”

New default behavior: Demand Allowed

The version 4.10 firmware provides that outside the defined window for *all* Scheduled Connection types the default behavior is *Demand Allowed*. Should two or more Scheduled Connections that use the same Connection Profile have overlapping windows, then the following criteria determine which one is active:

1. The one that starts first (has the earliest time to start) is active;
2. If they all have the same start time then the one that appears first in the list in the **Display/Change Scheduled Connection** screen list is active.

New Scheduled Connection type: Random Retry

The version 4.10 firmware adds the Scheduled Connection type **Random Retry**. Random Retry operates as follows:

- First, it will wait 0 to 60 seconds before starting, then it will try three times to bring the connection up as quickly as possible;
- Second, on each successive retry after these first three attempts it will wait a random number of seconds between zero and a user-specified maximum.

Add Scheduled Connection

Scheduled Connection Enable:

On

How Often...

+-----+

Schedule Type...

+-----+

Forced Up
Forced Down
Demand-Allowed
Demand-Blocked
Periodic
Random Retry

+-----+

Set Weekly Schedule...

Use Connection Profile...

Should the connection come up, and subsequently go down, the Scheduled Connection will start over with three retries. Switched connections have a variable redial back-off time depending on the interface type. Consequently, the first three attempts for such connections will be slower. Once the connection is up it will be forced to remain up.

If you select **Set Weekly Schedule** a new item **Retry interval (minutes)** appears.

Set Weekly Schedule

Monday:

No

Tuesday:

No

Wednesday:

No

Thursday:

No

Friday:

No

Saturday:

No

Sunday:

No

Scheduled Window Start Time:

02:39

AM or PM:

PM

Scheduled Window Duration Per Day:

00:00

Retry interval (minutes):

5

Retry interval (minutes) allows you to set the upper limit for the number of minutes to use for the retry time (the attempts after the first three attempts). It accepts values of 1 – 255 minutes; the default setting is 5 minutes. With a setting of 5 minutes it will try every 0 – 300 seconds after the first three retries to bring up the connection.

Worm Attack Protection TCP Stack Changes

Certain kinds of Internet worm attacks overburden router capacity by potentially taking up all of available memory and effectively causing them to cease functioning.

The version 4.10 firmware improves management of TCP resources so that the primary function of the router is not compromised by proliferating management connections. The following changes have been made in order to minimize TCP allocation failures:

- Increased number of TCP resources.
- The web server aborts the connection on most responses to requests for which the request cannot be fulfilled. This closes the connection immediately and recovers the TCP resource at once.
- Syn (connection request) flood protection: Up to one quarter of the TCP resources can be in a syn received state. If another syn is received, one of the embryonic TCP resources is randomly recycled for the new syn received.
- time_wait recovery: TCP resources are recovered from the time wait list in oldest-first order.

Chapter 3

CompuServe Login Protocol

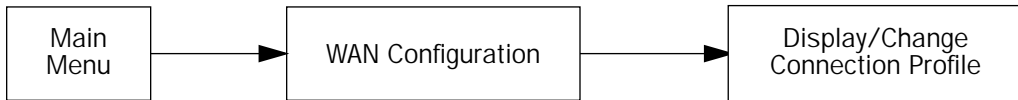
Some ISPs use the CompuServe Login Protocol to authenticate dialup connections. The CompuServe Login Protocol is a three-step authentication process that originated on the CompuServe Information Systems network. If your ISP uses the CompuServe Login Protocol they will supply you with a host name, a user name, and password separate from your PPP user name and password.

Introduced in firmware version 4.9, the firmware provides the ability to configure a Connection Profile to use the CompuServe Login Protocol when establishing a remote connection over an asynchronous WAN interface on an R2020 router.

CompuServe Login Protocol Configuration

Once you have created a Connection Profile, either by using the Easy Setup menus or by adding a new Connection Profile using the WAN Configuration menus, you can enable CompuServe Login authentication in the Telco Options screen. You must configure the Host Name, User Name, and Password.

To access the Telco Options screen from the Main Menu select **WAN Configuration, Display/Change Connection Profile**, and from the pop-up menu, select the Connection Profile you want to modify.



The Change Connection Profile screen appears.

Change Connection Profile

Profile Name:	Easy Setup Profile
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
Telco Options...	
COMMIT	CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
 Modify Connection Profile here. Finished? COMMIT or CANCEL to exit.

Select **Telco Options** and press Return.

The Telco Options screen appears.

Telco Options	
Dial...	Dial In/Out
Dialing Prefix:	
Number to Dial:	
Alternate Site to Dial:	
Dial on Demand:	Yes
Idle Timeout (seconds):	300
CNA Validation Number:	
Callback:	No
CompuServe Login Enabled:	Yes
CompuServe Host Name:	claire
CompuServe User Name:	tonyf
CompuServe Password:	*****

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

- Toggle **CompuServe Login Enabled** to **Yes**. Setting this item to Yes enables use of the protocol and displays the next three editable fields.
- **CompuServe Host Name**, **CompuServe User Name**, and **CompuServe Password** allow you to enter the Host Name, User Name, and Password that your ISP provides for this purpose. They will be sent as part of a three-step CompuServe Login Protocol exchange. These items are visible only when **CompuServe Login Enabled** is set to Yes.

Chapter 4

RADIUS Client Support and Web Security Enhancements

The version 4.10 firmware introduces enhanced menu console and web security features. This chapter covers the following topics:

- [“Overview” on page 4-1](#)
- [“RADIUS Client Configuration” on page 4-2](#)
- [“Restricting Device Web Server Access to the LAN” on page 4-4](#)
- [“Warning alerts” on page 4-5](#)

Overview

Netopia router firmware releases earlier than version 4.8 introduced a local authentication database. The database consisted of between one and four username and password pairs. This required someone seeking menu console or command line interface configuration access to log in with a username and password when at least one username and password pair had been configured locally in the router. If no username and password pairs were defined, someone could gain access without being required to log in.

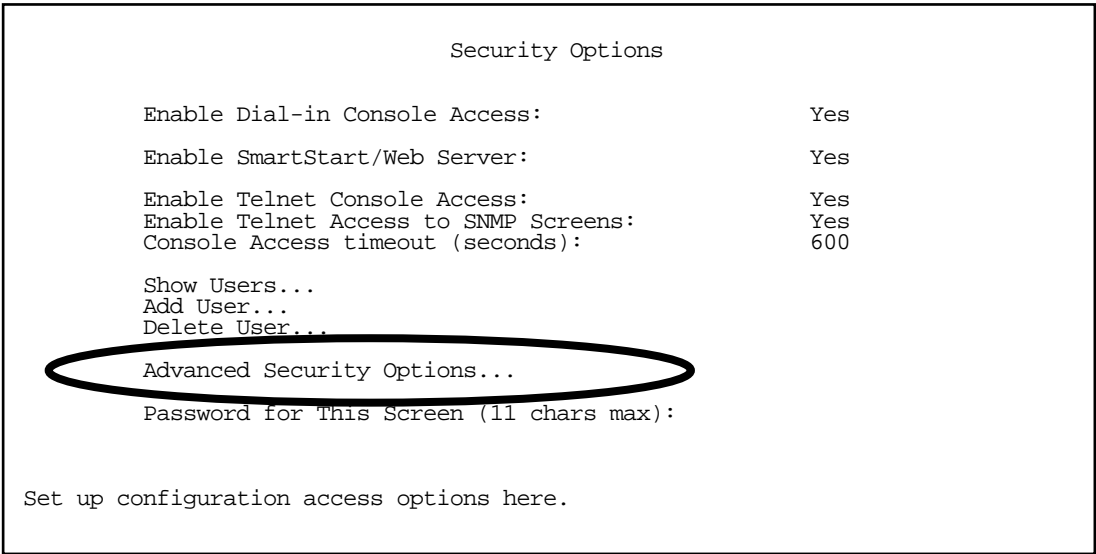
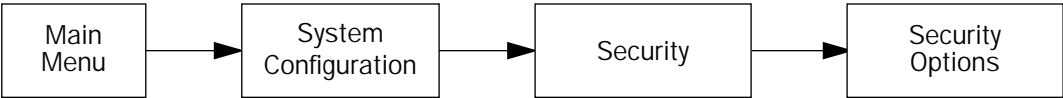
The version 4.8 firmware added the ability to authenticate users by using a remote authentication database. The remote authentication database is maintained by a Remote Authentication Dial-In User Service (RADIUS) server. It supported four security database modes: Local Only, Local then RADIUS, RADIUS then Local, and RADIUS only. Choosing Local Only, the default, selected the pre-4.8 authentication mechanism described above. Choosing RADIUS Only caused the router to ignore the local database and to authenticate users using the configured RADIUS server(s). Choosing Local then RADIUS caused the router to attempt to authenticate a user first using the local authentication database, and then, if that failed, using the configured RADIUS server(s). Choosing RADIUS then Local caused the router to attempt to authenticate a user first using the configured RADIUS server(s) and then, if that failed, using the local authentication database.

Note: In the latter two modes that involve both RADIUS and the local database, if the local database includes no username and password pairs, authentication succeeds only if the RADIUS server authenticates the user. This differs from the Local Only mode where no authentication is performed when the local database is empty.

Introduced in firmware version 4.9, the firmware supports a fifth security database mode: RADIUS then Lcl-Ser. Only. This mode is similar to the RADIUS then Local mode, except that if RADIUS authentication fails, the router will authenticate the user using the local authentication database only if the user is accessing the menu console or CLI through the built-in serial console port. Users attempting to access the menu console or CLI through telnet or modem dial-in will not be authenticated using the local authentication database.

RADIUS Client Configuration

To display the Security Options screen, from the Main Menu select System Configuration, Security, then Security Options.



If you select **Advanced Security Options** and press Return, the Advanced Security Options screen appears.

Advanced Security Options	
Security Databases...	<div style="border: 1px dashed black; padding: 5px;"> Local only RADIUS only RADIUS then Local RADIUS then Lcl/Ser. Only Local then RADIUS </div>
RADIUS Server Addr/Name:	
RADIUS Server Secret:	
Alt RADIUS Server Addr/Name:	
Alt RADIUS Server Secret:	
RADIUS Identifier:	
RADIUS Server Authentication Port:	1812
Device Web Server via LAN only:	Yes
LAN (EN Hub) IP Filter Set...	
Remove Filter Set	

- You select your desired mode by using the **Security Databases** pop-up menu.
 - Choosing **Local Only**, the default, selects the pre-4.8 authentication mechanism.
 - Choosing **RADIUS Only** causes the router to ignore the local database and to authenticate users using the configured RADIUS server.
 - Choosing **RADIUS then Local** causes the router to attempt to authenticate a user first using a RADIUS server and then, if that fails, using the local authentication database.
 - Choosing **RADIUS then Lcl/Ser. Only** causes the router to attempt to authenticate a user first using a RADIUS server and then, if that fails, using the local authentication database. If RADIUS authentication fails, the router will authenticate the user using the local authentication database only if the user is accessing the menu console or CLI through the built-in serial console port.
 - Choosing **Local then RADIUS** causes the router to attempt to authenticate a user first using the local authentication database, and then, if that fails using the configured RADIUS server.

Note: In the latter two modes that involve both RADIUS and the local database, if the local database includes no username/password pairs, authentication will succeed only if the RADIUS server authenticates the user. This differs from the Local Only mode where no authentication is performed when the local database is empty.

If the primary RADIUS server responds with an access rejection or an access challenge, the alternate RADIUS server is not contacted. Only if the primary RADIUS server fails to respond at all is the alternate RADIUS server contacted.

Therefore, do not attempt to select any of the RADIUS options unless you have a RADIUS server correctly configured for this purpose. If you attempt to use RADIUS authentication without a RADIUS server, you will lose your configuration access to the router.

The Advanced Security Options screen supports both a primary RADIUS server and an alternate RADIUS server. When the router is configured to authenticate using RADIUS, it will first attempt to contact the primary RADIUS server; if the primary RADIUS server responds, RADIUS authentication succeeds or fails based on the response returned by the primary server. If and only if the primary server fails to respond, the router will attempt to contact the alternate RADIUS server to authenticate the user. The router makes two attempts per server, three seconds apart.

- You can specify the **RADIUS Server Addr/Name** and the **Alt RADIUS Server Addr/Name** either by using a hostname to be resolved using the Domain Name System (DNS) information configured in the router or by using an IP address in dotted-quad notation. The RADIUS Server Addr/Name items are limited to 63 characters.
- In addition to specifying the server's hostname or IP address, you must also specify a **RADIUS Server Secret** and an **Alt RADIUS Server Secret** (if configured) known to both the router and the RADIUS server. The secret is used to encrypt RADIUS transactions in transit. The RADIUS Server Secret items are limited to 31 characters.

The router's RADIUS client implementation supports passwords longer than 16 characters and properly encrypts such passwords per RFC 2138. Not all RADIUS server implementations handle passwords longer than 16 characters.

- **RADIUS Identifier** can be either an IP address or an arbitrary string to be used as the identifier in the router's outgoing Access-Request packets. The RADIUS identifier is limited to 63 characters.
- **RADIUS Server Authentication Port** specifies the UDP destination port to which the router's RADIUS authentication requests will be sent. The default value is 1812, the official IANA-assigned UDP port number for the RADIUS authentication service.

Restricting Device Web Server Access to the LAN

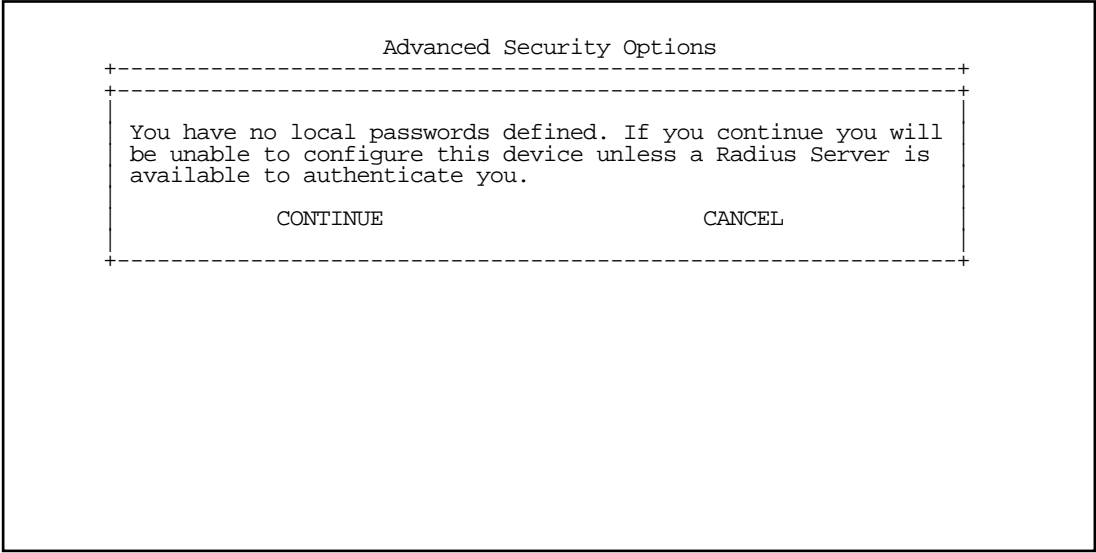
Certain kinds of Internet worm attacks overburden web servers by consuming their resources and effectively causing them to cease functioning.

Beginning with firmware version 4.9.4, the router defaults to disallowing web access to its own internal web server from the WAN. In other words, you will be able to access the router's web server from the LAN only. This prevents web-propagated worms on the Internet from disabling routing functions.

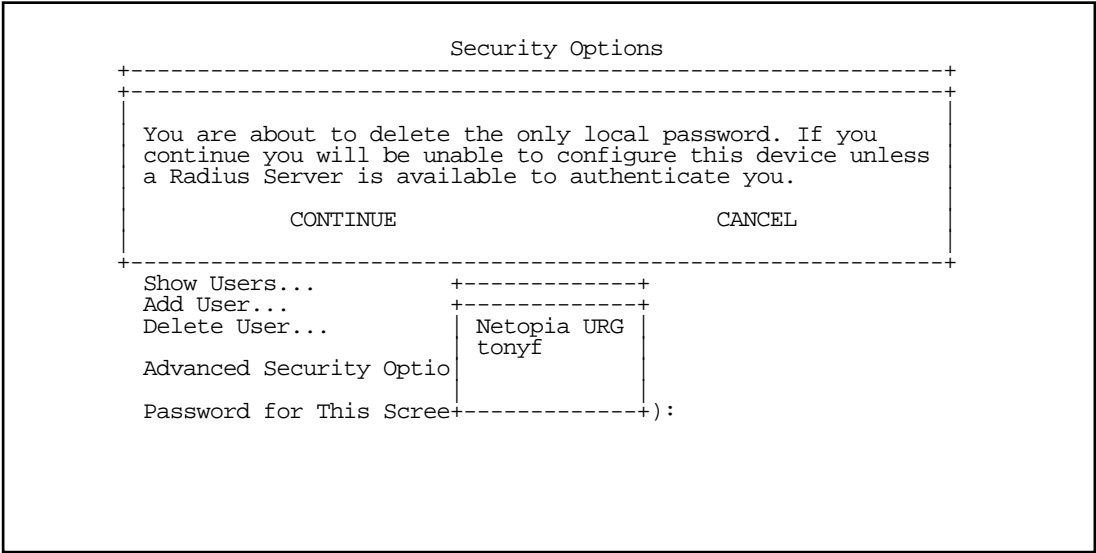
- By default, **Device Web Server via LAN only** is set to **Yes**.
- Some administrators use web-based monitoring tools that access the Netopia Router's built-in web server remotely, from the WAN. In that case, **Device Web Server via LAN only** should be toggled to **No**.

Warning alerts

Certain security-related configuration changes cause the router to display a warning alert. Choosing either **Local then RADIUS** or **RADIUS then Local** from the Security Databases pop-up menu when there are no configured username/password pairs causes the router to present the following warning alert:



Attempting to delete the last non-URG username/password pair from the local authentication database when the Security Databases pop-up menu is set to either **Local then RADIUS** or **RADIUS then Local** causes the router to present the following warning alert:



MultiNAT Enhancements

The version 4.8 firmware adds the following changes to the MultiNAT functionality:

- **NetBIOS Datagram service** – NetBIOS datagram service is transparently mapped so that the domain login service will be available. It is possible to browse a remote network from behind NAT if the remote network has an NT server and domain login. The resources of the host behind NAT will not be available to the remote network.
- **Arbitrary IP protocol pass-through for Static and Dynamic NAT addresses** – All IP protocols are passed through the Static and Dynamic NAT mappings.
- **Unmapped IP address support** – IP addresses can be passed through the router unmapped. The (un)mapping is indicated by a Static map with the Public range and Private map addresses equal to each other. The unmapped addresses function as though they are routed without NAT applied.
- **QuickTime 4 (RTP and RTSP) support** – Transparent support for QuickTime 4 and RealAudio® native streaming protocols has been added. Multiple streams and multiple hosts are supported.
- **Transparent NetMeeting Gateway** – A single NetMeeting session at a time can be supported.
- **Default service export is no longer necessary** – Although the EasyServers list is created by default, it does not contain any entries. Creating a server list no longer adds a default entry for the router. Additionally, all such entries are removed by the upgrade to version 4.8. The service exports are added to the end of the list (similar to NAT rules) rather than to the beginning as in firmware versions earlier than 4.8.

See [“Multiple Network Address Translation \(MultiNAT\)” on page 16-1](#) for more information.

Multiple ATM Permanent Virtual Circuit Support

The version 4.8 firmware adds support for up to eight permanent virtual circuits on cell-based SDSL (ATM over SDSL) and ADSL routers.

Multiple ATM PVC overview

On cell-based SDSL and ADSL WAN interfaces, the ATM connection between the router and the central office equipment (DSLAM) is divided logically into one or more virtual circuits (VCs). A virtual circuit may be either a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). Netopia Routers support PVCs.

VCs are identified by a Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). A VPI is an 8-bit value between 0 and 255, inclusive, while a VCI is a 16-bit value between 0 and 65535, inclusive.

Versions of router firmware earlier than 4.8 supported only a single PVC on cell-based SDSL and ADSL WAN interfaces. The version 4.8 firmware adds support for up to eight PVCs on these interfaces.

- Circuits now support attributes in addition to their VPI and VCI values. When configuring a circuit, you can specify an optional circuit name of up to 14 characters. The circuit name is used only to identify the circuit for management purposes as a convenience to aid in selecting circuits from lists. The default circuit name is “Circuit <n>”, where <n> is some number between one and eight corresponding to the circuit’s position in the list of up to eight circuits.
- You can also individually enable or disable a circuit without deleting it. This is useful for temporarily

removing a circuit without losing the configured attributes.

- In order to function, each circuit must be bound to a Connection Profile or to the Default Profile. Among other attributes, the profile binding specifies the IP addressing information for use on the circuit. Each circuit must be bound to a distinct Connection Profile. You cannot bind multiple circuits to the same Connection Profile. Thus it is not possible to construct point-to-multipoint meshes with ATM as is possible with Frame Relay.

Multiple ATM PVC configuration

You configure Virtual Circuits in the Add/Change Circuit screen. From the Main Menu, navigate to the SDSL Line Configuration screen.



SDSL Line Configuration

Operation Mode...	Nokia Fixed
Clock Source...	Network
Data Rate Mode...	Hunt
Data Rate...	384
Display/Change Circuit...	
Add Circuit...	
Delete Circuit...	
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Routed 1483

Enter Information supplied to you by your telephone company.

Select **Display/Change Circuit** and press Return.

Choosing **Display/Change Circuit** (or **Delete Circuit**) displays a pop-up menu that allows you to select the circuit to be modified or deleted.

SDSL Line Configuration

Operation Mode...
Clock Source...
Data Rate Mode...
Data Rate...

Display/Change Circuit...
Add Circuit...
Delete Circuit...

Data Link Encapsulation...
RFC1483 Mode...

Nokia Fixed

Network
+---Circuit Name---VPI/VCI---+
+-----+
Circuit 1 0/38
Circuit 2 0/0
+-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Changing a circuit

If you want to make any changes to the circuit you select, you make them in the Change Circuit screen.

Change Circuit

Circuit Name:
Circuit Enabled:
Circuit VPI (0-255):
Circuit VCI (0-65535):
Connection Profile is

Circuit 1
Yes
0
38
Default Profile

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

- **Circuit Name** allows you to associate a one- to fourteen-character name with the circuit. The default circuit name is "Circuit <n>", where <n> is some number between one and eight corresponding to the circuit's position in the list of up to eight circuits.

- **Circuit Enabled** allows you to enable or disable the circuit, using the Tab key. The default is enabled.
- **Circuit VPI** allows you to specify the Virtual Path Identifier (VPI) value for the circuit. The default VPI value for both ADSL and cell-based SDSL is zero (0).
- **Circuit VCI** allows you to specify the Virtual Channel Identifier (VCI) value for the circuit. The default VCI value for circuits on ADSL is 35, while the default VCI value for circuits on cell-based SDSL is 38.
- **Use Connection Profile** and **Use Default Profile for Circuit** are visible when there is more than one enabled circuit. Choosing Use Connection Profile presents a pop-up menu that lists all of your enabled Connection Profiles. Choosing a profile from the list statically binds the circuit to the selected profile. Choosing Use Default Profile for Circuit statically binds the circuit to the Default Profile. When the circuit is bound to a Connection Profile, Use Connection Profile displays the name of the profile; when the circuit is associated with the Default Profile, Use Connection Profile displays Default Profile.

When more than one circuit is enabled, you must explicitly statically bind each circuit to the Connection Profile to be used on the circuit, or to the Default Profile. To do this you use Use Connection Profile or Use Default Profile for Circuit.

Note: With multiple VCs you must explicitly statically bind the *second* (and all subsequent) VCs to a profile. The first VC will automatically statically bind according to pre-defined dynamic binding rules when you add the second VC. It will revert back to dynamic binding if the number of VCs is reduced to one; for example, by deleting previously defined VCs.

When the link comes up the router binds the VC dynamically to the first suitable Connection Profile or to the Default Profile if there is no Connection Profile configured.

- If you factory default the router, the VC binds to the Default Profile.
- If you delete a Connection Profile that is statically bound to a VC, the VC binding is set back to the Default Profile. If there is only one VC defined, the VC dynamically binds to the first suitable profile or to the Default Profile. If there are multiple VCs defined, it binds to the Default Profile.
- If you add a second VC, it is initialized to the Default Profile, and the menu screens display the VC Connection Profile-related items, allowing you to bind to a specific Connection Profile instead of the Default Profile. In addition, the router statically binds the first VC according to the rules used to select a profile for dynamic binding. At this point, each profile uses static binding when the link is brought up.

If there are no VCs when you add a VC -- for example, if you deleted all your previous VCs and started adding them again -- dynamic binding will occur when the link comes up. If you delete a VC, leaving only one VC, that VC resumes dynamically binding again.

Adding a circuit

Choosing **Add Circuit** displays the Add Circuit screen.

Add Circuit

Circuit Name:

Circuit 2

Circuit Enabled:

Yes

Circuit VPI (0-255):

0

Circuit VCI (0-65535):

0

Use Connection Profile...

Default Profile

Use Default Profile for Circuit

ADD Circuit NOW

CANCEL

The fields in the Add Circuit screen are the same as the fields in the Change Circuit screen described above. You can add up to seven circuits (for a total of eight) and bind them to separate Connection Profiles.

Monitoring multiple virtual circuits

The General Statistics screen adds a selection for ATM VC Statistics.

To access the ATM VC Statistics screen navigate from the Main Menu to Statistics & Logs then General Statistics.



The General Statistics screen appears.

General Statistics

Physical I/F	Rx Bytes	Tx Bytes	Rx Pkts	Tx Pkts	Rx Err	Tx Err
Ethernet Hub	0	0	0	0	0	0
Aux Async	0	0	0	0	0	0
ATM SDSL 1	22152	5092	403	404	0	0

Network	Rx Bytes	Tx Bytes	Rx Pkts	Tx Pkts	Rx Err	Tx Err
IP	0	0	0	0	0	0

VC Traffic Statistics...

Select **VC Traffic Statistics**.

The ATM VC Statistics screen appears.

ATM VC Statistics						
View Statistics for WAN Module...			ATM SDSL 1			
VPI/VCI-----	Local IP Addr-----	Frames Rx--	Frames Tx---	Bytes Rx---	Bytes Tx	
-----SCROLL UP-----						
0/39	111.222.333.4	0	0	0	0	
8/36	--	1	0	70	0	
-----SCROLL DOWN-----						

View Statistics for WAN Module only appears if there is more than one WAN module installed. If you select it and press Return, a pop-up menu allows you to choose between WAN modules.

ATM VC Sta+-----+						
View Statistics for WAN Module...			ATM	ATM SDSL 1		
VPI/VCI-----	Local IP Addr-----	Frames	ATM SDSL 2	---	Bytes Rx---	Bytes Tx
-----SCROLL +-----+						
-----SCROLL DOWN-----						

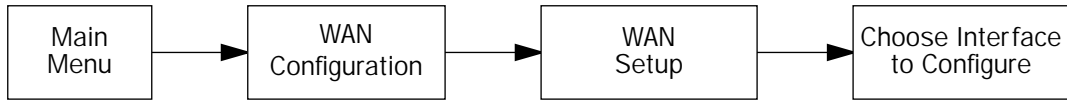
- You can then display circuit information for each WAN interface module.
- To display more information about each circuit associated with the selected WAN module, use the up or down arrow key to highlight the circuit you want to view. Press Return.

A pop-up window appears, displaying detailed information for the selected circuit.

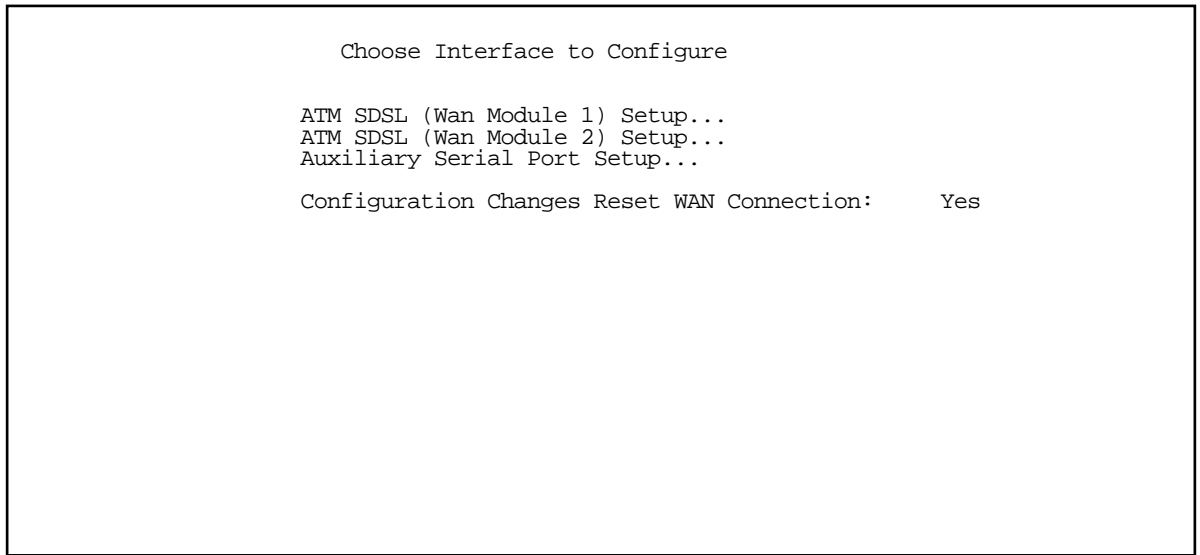
ATM VC Statistics			
View St	-----+		
VPI/VCI	-----+		
0/39	Circuit Name:	Circuit 4	
8/36	Connection Profile Name:	Profile 4	
	Bytes Rx:	0	
	Bytes Tx	0	
	Frames Rx:	0	Frames Tx: 0
	Frames Rx Discarded:	0	Frames Tx Discarded: 0
	Errors Rx:	0	
	Errors Tx:	0	
	OK		
	-----+		

Multilink PPP-based DSL Bonding Support for ADSL and SDSL Routers

The version 4.8 firmware offers Multilink PPP-based DSL Bonding support for new R6161 ADSL and R7272 SDSL routers. R7171 routers gain Multilink PPP DSL Bonding support as well. This requires that PVCs be set on a per-WAN interface basis. You access this feature in the Choose Interface to Configure screen under the WAN Setup menu.



When there are two ADSL or SDSL WAN interface modules installed in the router, the Choose Interface to Configure screen changes to the following:



The second WAN module configuration screen, and the menu that takes you to it, are accessible when:

- both WAN modules are the same
- both WAN modules are capable of Multilink PPP
- both WAN modules make use of ATM PVCs.

This currently includes the R6161 and R7272.

When you select **ATM SDSL (Wan Module 2) Setup** above and press Return, the secondary WAN module screen appears.

SDSL Line 2 Configuration

Display/Change Circuit...
Add Circuit...
Delete Circuit...

Enter Information supplied to you by your telephone company.

This is because the only configuration that is allowed is the configuration of PVCs. See [“Multiple ATM Permanent Virtual Circuit Support”](#) on page 4-6 for more information.

RFC1973 LMI Support

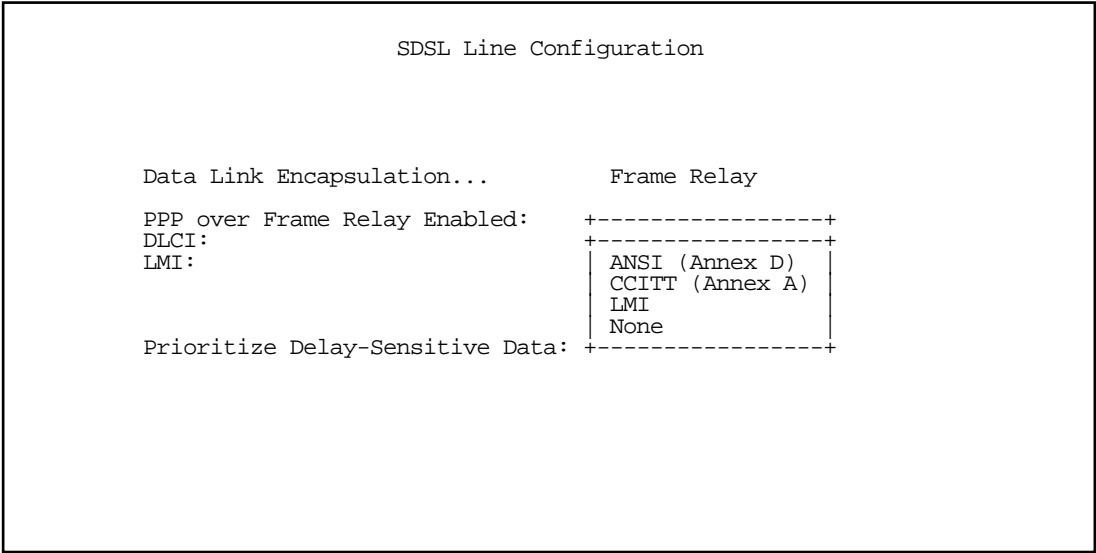
The version 4.8 firmware provides RFC 1973 Local Management Interface (LMI) support. LMI is a set of enhancements to the basic Frame Relay specification that includes support for:

- a keep-alive mechanism, which verifies that data is flowing
- a multicast mechanism, which provides the network server with its local DLCI and the multicast DLCI
- global addressing, which gives DLCIs global rather than local significance in Frame Relay networks
- a status mechanism, which provides an on-going status report on the DLCIs known to the switch

RFC1973 LMI support applies to all routers that support RFC1973 (R3000-series and R7100-series routers).

The console menu contains new pop-up menus that permit you to configure the LMI when you choose RFC1973 encapsulation, as shown in the following example screen.

Note: The example is an R7100 Easy Setup screen, but the same applies for the R3000-series and corresponding Advanced Configuration screens.



When you choose **Frame Relay** as the data link encapsulation method and **PPP over Frame Relay Enabled** is set to **On**, the LMI option becomes available in the pop-up menu.

Copper Mountain DHCP Server Support

The version 4.8 firmware offers Dynamic Host Configuration Protocol (DHCP) client support for the Copper Mountain proprietary operation mode necessary to interoperate with a Copper Mountain Networks Copper Edge 200 DSLAM-based DHCP server. This operation mode supplements but does not replace the existing standards-based mode of operation.

You set the DHCP operation mode for each Connection Profile either by modifying the default setting in the Easy Setup Profile or by adding a new Connection Profile through the WAN Configuration menus and specifying the mode in the appropriate IP Profile Parameters screen.

Overview

Netopia firmware version 4.1 introduced support for the frame-based R7100 SDSL Router compatible with the CE200 DSLAM. This release included the ability to automatically configure the SDSL WAN interface via DHCP when the data link encapsulation was set to RFC1483 MAC-Encapsulated Routing (MER) and no local WAN IP address was configured. This implementation was a standards-based implementation that conformed in all respects with the Dynamic Host Configuration Protocol specification in RFC 2131.

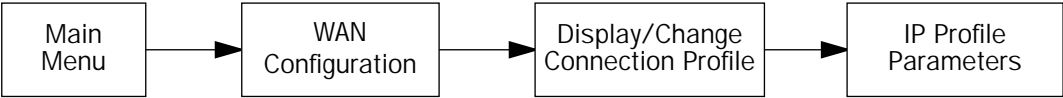
Beginning with CE200 firmware release 2.1, Copper Mountain added the ability for the DSLAM itself to act as a DHCP server. In this mode, the CE200 DSLAM intercepts and responds to DHCP requests from CPE routers.

Prior to Netopia version 4.8 firmware, the Netopia router DHCP client implementation did not interoperate with the CE200-based DHCP server. The 4.8 firmware release adds support for the Copper Mountain proprietary mode of operation necessary to interoperate with a CE200-based DHCP server.

Configuration

You configure a Connection Profile’s DHCP mode in the [IP Profile Parameters](#) screen or the [IP Parameters \(Default Profile\)](#) screen.

You access the IP Profile Parameters screen for a Connection Profile through the WAN Configuration menus.



Change Connection Profile

Profile Name:	Easy Setup Profile
Profile Enabled:	Yes
Data Link Encapsulation...	RFC1483
PPPoE Enabled:	No
IP Enabled:	Yes
→ IP Profile Parameters...	
Interface Group...	Primary
COMMIT	CANCEL

Modify Connection Profile here. Finished? COMMIT or CANCEL to exit.

Set **Data Link Encapsulation** to **RFC1483** and select **IP Profile Parameters**.

IP Profile Parameters

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Filter Set...	NetBIOS Filter
Remove Filter Set	+-----+-----+
DHCP Client Mode:	+-----+-----+
	Standards-Based
	Copper Mountain Specific
	+-----+-----+
	+-----+-----+

The **Local WAN IP Address** must be set to acquire an IP address from the DHCP server; that is, it must be 0.0.0.0.

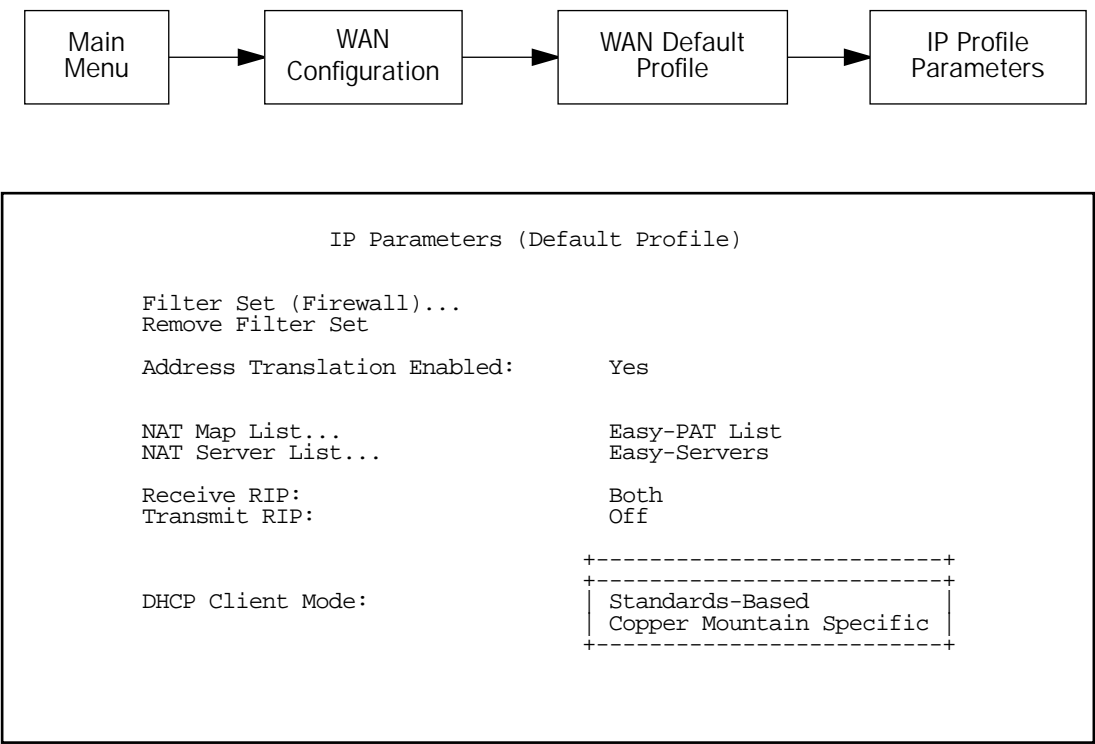
By selecting **DHCP Client Mode**, you can choose either Standards-Based (the default) or Copper Mountain Specific.

DHCP Client Mode is visible for RFC1483 MAC-Encapsulated Routing (MER) Connection Profiles configured to act as a DHCP client; that is, no Local WAN IP Address is configured.

- **Standards-Based** selects the DHCP client behavior specified by RFC 2131.
- **Copper Mountain Specific** selects the Copper Mountain proprietary DHCP client behavior.

IP Parameters (Default Profile)

You configure the DHCP mode for the WAN Default Profile in an analogous manner on the IP Parameters (Default Profile) screen of the WAN Default Profile menu.

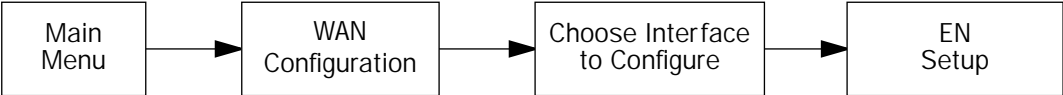


By selecting **DHCP Client Mode**, you can choose either Standards-Based (the default) or Copper Mountain Specific.

Note: The **Local WAN IP Address** must be set to acquire an IP address from the DHCP server; that is, it must be 0.0.0.0. DHCP Client Mode is visible for RFC1483 MAC-Encapsulated Routing (MER) Connection Profiles configured to act as a DHCP client; that is, no Local WAN IP Address is configured.

WAN Ethernet Configuration

For an R9100 Ethernet-to-Ethernet router, you configure the DHCP mode for the WAN Ethernet Configuration on the WAN Ethernet Configuration screen.



WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set...	
Remove Filter Set	
Enable PPP over Ethernet:	On
Wan Ethernet MAC Address:	00:00:c5:78:5d:12
DHCP Client Mode:	<div>+-----+ Standards-Based Copper Mountain Specific +-----+</div>
RIP Options...	

PPP Ethernet LAN Reconfiguration

The version 4.8 firmware adds the ability for PPP to reconfigure the router’s Ethernet LAN when establishing an unnumbered, non-NAT connection.

In firmware versions earlier than 4.8, when establishing an unnumbered, non-NAT connection, PPP would not request or accept a different IP address from the PPP peer. When establishing a numbered connection, PPP does request an IP Address for the WAN interface if no local WAN IP address was configured.

The version 4.8 firmware allows a central site router to supply an entire IP subnet, rather than a single IP address, for use by a Netopia router. If the applicable Connection Profile specifies an unnumbered, non-NAT connection and Negotiate LAN IP Addr/Mask is set to On, PPP will attempt to negotiate both an IP Address and subnet mask.

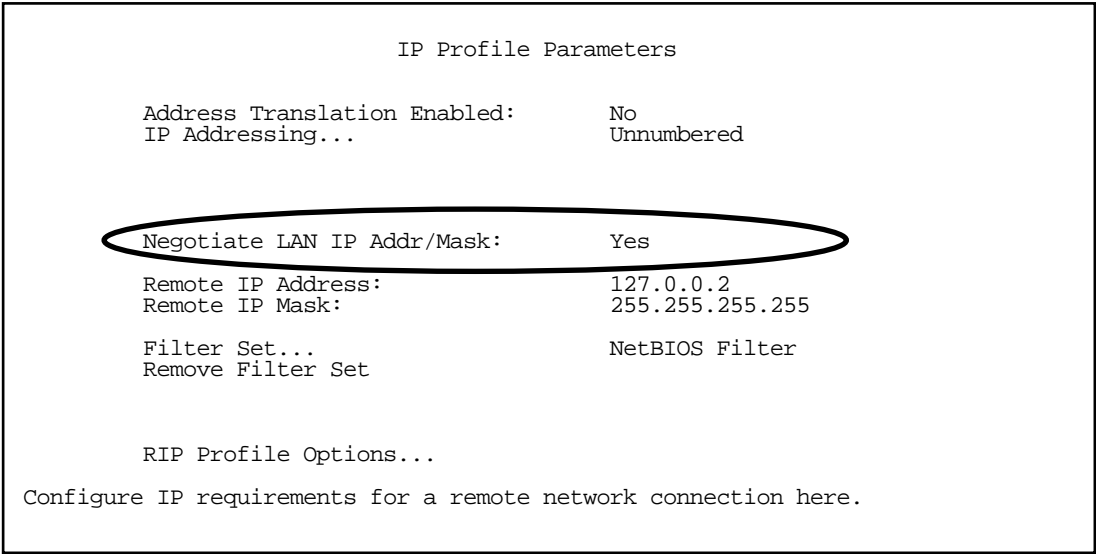
Note: Once the router has reconfigured the address serving pool only to conform to the negotiated subnet, you can adjust the base or extent of the pool and reboot the router. Your adjustments will not be overwritten when the connection is next renegotiated because the router only reconfigures the address serving pool if it lies outside the negotiated subnet.

The router does not adjust any address serving parameters other than the base and extent of the address serving pool. This allows you to otherwise configure address serving as you please using the normal address serving configuration items. For example, if you disable address serving, the router will not enable address serving when it reconfigures the address serving pool.

Configuration

To enable PPP Ethernet LAN configuration, navigate to the IP Profile Parameters screen of the Connection Profile you want to use. This can be either the Easy Setup Profile or any other Connection Profile you have added.

The IP Profile Parameters screen for a Connection Profile displays a Negotiate LAN IP Addr/Mask toggle:



- This toggle is visible only if the profile’s Data Link Encapsulation is set to **PPP**, the Address Translation Enabled toggle is set to **No** and IP Addressing is set to **Unnumbered**. The default value is **No**.
- RIP Profile Options is not visible if Negotiate LAN IP Addr/Mask is set to **Yes** and the Remote IP Mask is set to **0.0.0.0**. See “RIP Profile Options” on page 4-24 for more information.

Quick View

The Quick View screen (as shown below) displays both Primary and Secondary DNS Server addresses. This is useful because both may be served via PPP.

Quick View

8/8/2000 10:46:14 AM

Default IP Gateway: 163.176.12.1

CPU Load: 6%

Unused Memory: 232 KB

Primary DNS Server: 163.176.4.31

WAN Interface Group -- EN

Secondary DNS Server: 163.176.4.10

Domain Name: isp.com

-----MAC Address-----IP Address-----

Ethernet Hub: 00-00-c5-78-5d-10 192.168.1.1

Ethernet WAN1: 00-00-c5-78-5d-12 0.0.0.0

Current WAN Connection Status

Profile Name-----Rate--%Use-Remote Address-----Est.-More Info-----

VPN QuickView

LED Status

PWR+-----WAN1-----+--CON--AUX--+-----EN--+-----LEDS-----

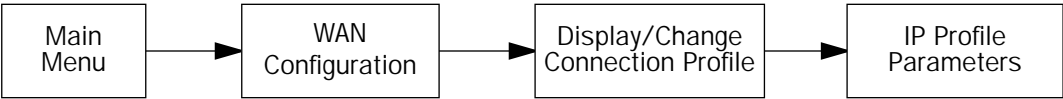
LNK RDY CH1 CH2 LNK LNK DATA | '- '= Off 'G'= Green

G - G - - Y - - | 'R'= Red 'Y'= Yellow

RIP Profile Options

The version 4.8 firmware changes the IP Profile Parameters RIP Profile Parameters screen for Connection Profiles.

The three Routing Information Protocol (RIP) options, Receive RIP, Transmit RIP, and TX RIP Policy, have been moved to a new RIP Profile Parameters screen. To access the RIP Profile Parameters screen you navigate from the Main Menu to WAN Configuration, Display/Change Connection Profile (or Add Connection Profile), and IP Profile Parameters.



You access the RIP Profile Parameters screen via the **RIP Profile Options** item on the IP Profile Parameters screen.

IP Profile Parameters

Address Translation Enabled:	No
IP Addressing...	Unnumbered
Negotiate LAN IP Addr/Mask:	Yes
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	NetBIOS Filter
Remove Filter Set	
RIP Profile Options...	

Configure IP requirements for a remote network connection here.

When you select **RIP Profile Options** and press Return, the RIP Profile Parameters screen appears.

RIP Profile Parameters	
Receive RIP:	Both
Transmit RIP:	v2 (multicast)
TX RIP Policy...	Poison Reverse

For detailed information on these RIP options, see the chapter on "IP Setup" in the *User's Reference Guide*.

Connection Profile Changes Require COMMIT

In order to ensure that Connection Profile configurations can be changed without immediately affecting your connection, the Add/Change Connection Profile menus now operate on an internal *copy* of the profile until you press **COMMIT**. If you change your mind and decide not to make the changes as you have entered them, press **CANCEL** and your changes are discarded.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
Interface Group...	Primary
COMMIT	CANCEL
Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.	

Backup Enhancements

The Backup and Recovery timers now allow you to enter your own values in minutes. The value zero is not permitted for these fields. If you are upgrading from 4.7.x or earlier your previous settings will be preserved; however a value of 30 seconds is rounded up to 1 minute.

By setting **Clear Backup Call only if idle** to **Yes** you can access **Requires idle time of**. You enter this value in seconds. When in backup mode and the primary interface comes up, the router waits the specified time entered in the Recovery timer field. In earlier firmware versions, after this expires the router would normally switch back to the Primary interface (depending on various settings). Starting with firmware version 4.8, if you want a backup call to be cleared only when idle, the router will wait until the call has been idle for the time you specified. After this expires the router will tear down the call and switch to the Primary interface.

Note: Backup and Recovery have resolutions of five seconds. This is how often the router evaluates the state of the connections and makes decisions.

For a detailed description of the Dial Backup features, see [Chapter 12, “DSL and Leased Line Backup.”](#)

47-Character PPP Authentication String Support

PPP authentication strings for username and password (PAP) and hostname and secret (CHAP) may now be up to 47 characters.

Chapter 5

Multiple ATM Permanent Virtual Circuit Support

Introduced in version 4.8, the firmware supports up to eight permanent virtual circuits on cell-based SDSL (ATM over SDSL) and ADSL routers.

This chapter covers the following topics:

Multiple ATM PVC overview

On cell-based SDSL and ADSL WAN interfaces, the ATM connection between the router and the central office equipment (DSLAM) is divided logically into one or more virtual circuits (VCs). A virtual circuit may be either a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). Netopia Routers support PVCs.

VCs are identified by a Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). A VPI is an 8-bit value between 0 and 255, inclusive, while a VCI is a 16-bit value between 0 and 65535, inclusive.

Versions of router firmware earlier than 4.8 supported only a single PVC on cell-based SDSL and ADSL WAN interfaces. The version 4.8 firmware adds support for up to eight PVCs on these interfaces.

- Circuits now support attributes in addition to their VPI and VCI values. When configuring a circuit, you can specify an optional circuit name of up to 14 characters. The circuit name is used only to identify the circuit for management purposes as a convenience to aid in selecting circuits from lists. The default circuit name is "Circuit <n>", where <n> is some number between one and eight corresponding to the circuit's position in the list of up to eight circuits.
- You can also individually enable or disable a circuit without deleting it. This is useful for temporarily removing a circuit without losing the configured attributes.
- In order to function, each circuit must be bound to a Connection Profile or to the Default Profile. Among other attributes, the profile binding specifies the IP addressing information for use on the circuit. Each circuit must be bound to a distinct Connection Profile. You cannot bind multiple circuits to the same Connection Profile. Thus it is not possible to construct point-to-multipoint meshes with ATM as is possible with Frame Relay.

Multiple ATM PVC configuration

You configure Virtual Circuits in the Add/Change Circuit screen. From the Main Menu, navigate to the SDSL Line Configuration screen.



SDSL Line Configuration

Operation Mode...	Nokia Fixed
Clock Source...	Network
Data Rate Mode...	Hunt
Data Rate...	384
Display/Change Circuit...	
Add Circuit...	
Delete Circuit...	
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Routed 1483

Enter Information supplied to you by your telephone company.

Select **Display/Change Circuit** and press Return.

Choosing **Display/Change Circuit** (or **Delete Circuit**) displays a pop-up menu that allows you to select the circuit to be modified or deleted.

```

                                SDSL Line Configuration

Operation Mode...                Nokia Fixed
Clock Source...                 Network
Data Rate Mode...              +---Circuit Name---VPI/VCI---+
Data Rate...                    +-----+
                                | Circuit 1      0/38  |
                                | Circuit 2      0/0   |
                                +-----+

Display/Change Circuit...
Add Circuit...
Delete Circuit...

Data Link Encapsulation...
RFC1483 Mode...

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

Changing a circuit

If you want to make any changes to the circuit you select, you make them in the Change Circuit screen.

```

                                Change Circuit

Circuit Name:                   Circuit 1
Circuit Enabled:                Yes
Circuit VPI (0-255):            0
Circuit VCI (0-65535):          38
Connection Profile is           Default Profile

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

```

- **Circuit Name** allows you to associate a one- to fourteen-character name with the circuit. The default circuit name is "Circuit <n>", where <n> is some number between one and eight corresponding to the circuit's position in the list of up to eight circuits.

- **Circuit Enabled** allows you to enable or disable the circuit, using the Tab key. The default is enabled.
- **Circuit VPI** allows you to specify the Virtual Path Identifier (VPI) value for the circuit. The default VPI value for both ADSL and cell-based SDSL is zero (0).
- **Circuit VCI** allows you to specify the Virtual Channel Identifier (VCI) value for the circuit. The default VCI value for circuits on ADSL is 35, while the default VCI value for circuits on cell-based SDSL is 38.
- **Use Connection Profile** and **Use Default Profile for Circuit** are visible when there is more than one enabled circuit. Choosing Use Connection Profile presents a pop-up menu that lists all of your enabled Connection Profiles. Choosing a profile from the list statically binds the circuit to the selected profile. Choosing Use Default Profile for Circuit statically binds the circuit to the Default Profile. When the circuit is bound to a Connection Profile, Use Connection Profile displays the name of the profile; when the circuit is associated with the Default Profile, Use Connection Profile displays Default Profile.

When more than one circuit is enabled, you must explicitly statically bind each circuit to the Connection Profile to be used on the circuit, or to the Default Profile. To do this you use Use Connection Profile or Use Default Profile for Circuit.

Note: With multiple VCs you must explicitly statically bind the *second* (and all subsequent) VCs to a profile. The first VC will automatically statically bind according to pre-defined dynamic binding rules when you add the second VC. It will revert back to dynamic binding if the number of VCs is reduced to one; for example, by deleting previously defined VCs.

When the link comes up the router binds the VC dynamically to the first suitable Connection Profile or to the Default Profile if there is no Connection Profile configured.

- If you factory default the router, the VC binds to the Default Profile.
- If you delete a Connection Profile that is statically bound to a VC, the VC binding is set back to the Default Profile. If there is only one VC defined, the VC dynamically binds to the first suitable profile or to the Default Profile. If there are multiple VCs defined, it binds to the Default Profile.
- If you add a second VC, it is initialized to the Default Profile, and the menu screens display the VC Connection Profile-related items, allowing you to bind to a specific Connection Profile instead of the Default Profile. In addition, the router statically binds the first VC according to the rules used to select a profile for dynamic binding. At this point, each profile uses static binding when the link is brought up.

If there are no VCs when you add a VC -- for example, if you deleted all your previous VCs and started adding them again -- dynamic binding will occur when the link comes up. If you delete a VC, leaving only one VC, that VC resumes dynamically binding again.

Adding a circuit

Choosing **Add Circuit** displays the Add Circuit screen.

Add Circuit	
Circuit Name:	Circuit 2
Circuit Enabled:	Yes
Circuit VPI (0-255):	0
Circuit VCI (0-65535):	0
Use Connection Profile...	Default Profile
Use Default Profile for Circuit	
ADD Circuit NOW	CANCEL

The fields in the Add Circuit screen are the same as the fields in the Change Circuit screen described above. You can add up to seven circuits (for a total of eight) and bind them to separate Connection Profiles.

Monitoring multiple virtual circuits

The General Statistics screen adds a selection for ATM VC Statistics.

To access the ATM VC Statistics screen navigate from the Main Menu to Statistics & Logs then General Statistics.



The General Statistics screen appears.

General Statistics									
Physical I/F	-----Rx	Bytes	---Tx	Bytes	---Rx	Pkts	---Tx	Pkts	---Rx
Ethernet Hub		0		0		0		0	
Aux Async		0		0		0		0	
ATM SDSL 1		22152		5092		403		404	
Network	-----Rx	Bytes	---Tx	Bytes	---Rx	Pkts	---Tx	Pkts	---Rx
IP		0		0		0		0	
VC Traffic Statistics...									

Select **VC Traffic Statistics**.

The ATM VC Statistics screen appears.

ATM VC Statistics						
View Statistics for WAN Module...						
VPI/VCI	Local IP Addr	Frames Rx	Frames Tx	Bytes Rx	Bytes Tx	
0/39	111.222.333.4	0	0	0	0	
8/36	--	1	0	70	0	
-----SCROLL DOWN-----						

View Statistics for WAN Module only appears if there is more than one WAN module installed. If you select it and press Return, a pop-up menu allows you to choose between WAN modules.

ATM VC Sta+-----+						
View Statistics for WAN Module...						
VPI/VCI	Local IP Addr	Frames	ATM SDSL 1	Bytes Rx	Bytes Tx	
		SCROLL UP	ATM SDSL 2			
-----SCROLL DOWN-----						

- You can then display circuit information for each WAN interface module.
- To display more information about each circuit associated with the selected WAN module, use the up or down arrow key to highlight the circuit you want to view. Press Return.

A pop-up window appears, displaying detailed information for the selected circuit.

ATM VC Statistics

View St
VPI/VCI

0/39
8/36

Circuit Name:
Connection Profile Name:

Bytes Rx: 0
Bytes Tx 0

Frames Rx: 0
Frames Rx Discarded: 0

Errors Rx: 0
Errors Tx: 0

Circuit 4
Profile 4

Frames Tx: 0
Frames Tx Discarded: 0

OK

Chapter 6

Enhanced Netopia Router SDSL Interoperability Support

Introduced in version 4.7.1, the firmware provides a more feature-rich SDSL Line Configuration screen for R7200 routers:

SDSL Line Configuration

Operation Mode...	Generic
Clock Source...	Lucent
Data Rate Mode...	Nokia EOC Fast
Data Rate...	Nokia Fixed
	Paradyne
	Nortel UE IMAS
VPI:	38
VCI:	
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Routed 1483

Enter Information supplied to you by your telephone company.

Note: These values are usually preconfigured for you by your service provider. If not, or if you are changing these values yourself for any reason, you must obtain this information from your service provider in order for the router to communicate with the service provider’s equipment.

Versions of WAN interface module firmware up to and including version 1.0.6 support only the **Nokia Fixed** mode of operation. Versions of WAN interface module firmware beginning with version 1.0.20 also support the **Nokia EOC Fast** and **Generic** modes of operation. The Nokia EOC Fast mode is appropriate for connections to a Nokia SpeedLink D50 DSLAM port configured for Embedded Operations Channel (EOC) mode. The **Generic** mode is appropriate for connections to an access concentrator, other than the pre-defined options available in the Operations Mode pop-up menu, that uses *Generic* (also called *transparent*) mode SDSL framing.

If necessary, you should upgrade the WAN module firmware. You can check the current WAN interface module firmware level in the **System Information** screen under the **Statistics & Logs** menu.

System Information	
Serial Number	70-03-48 (7340872)
Firmware Version	4.7.1
Processor Speed (MHz)	33
Flash ROM Capacity (MBytes)	1
DRAM Capacity (MBytes)	4
Ethernet	8 Port 10Base-T
Auxiliary Serial Port	Async Modem
WAN 1 Interface	ATM SDSL, fw v1.0.20
WAN 2 Interface	Not Installed
AppleTalk Feature Set	Not Installed
Analog Dial-In Kit	Not Installed



For information about upgrading WAN module firmware, see the *User's Reference Guide* chapter "Utilities and Diagnostics."

Operation Mode

- The **Operation Mode...** pop-up menu item is visible if the SDSL WAN interface module supports more than one operation mode. The router makes this determination by examining the WAN interface module firmware version.
- If you select any operation mode other than Nokia Fixed (the default), a dialogue box appears asking you if you want to reset the defaults to those used by the selected DSLAM.

SDSL Line Configuration	
Operation Mode...	Generic
Reset to default settings for this DSLAM?	
NO	YES
Data Link Encapsulation...	RFC1483
RFC1483 Mode...	Routed 1483

Each access concentrator (DSLAM) has a different set of default data rates and other parameters.

Your service provider should supply you with the appropriate information about the type and capabilities of the access concentrator equipment they use.

- The **Data Rate Mode...** pop-up menu item is invisible if the Operation Mode is set to any setting other than **Nokia Fixed** (or if the Operation Mode pop-up menu is hidden, since then Nokia Fixed is presumed). In **Hunt** mode (the default), the router cycles through the sequence of data rates present in the Data Rate pop-up menu when attempting to establish a connection. The router begins at the rate currently selected from the Data Rate pop-up menu, makes two connection attempts at each successive data rate, stopping as soon as it makes a successful connection. If the router fails to connect at the highest data rate after two attempts, it continues with the lowest data rate. In **Locked** mode, the router will attempt to establish a connection only at the single data rate specified in the Data Rate pop-up menu. The router will continuously attempt a connection at the specified rate. The connection behavior in Generic mode is the same as if this item were set to Locked.
- The **Data Rate...** pop-up menu item is visible if the Operation Mode pop-up menu is set to any setting other than either **Nokia EOC Fast** (or if the Operation Mode pop-up menu is hidden, since then Nokia Fixed is presumed). For Nokia Fixed mode, the Data Rate pop-up menu includes the following values (in Kbps): 192, 384, 768, 1152, and 1536. For Generic Mode, the Data Rate pop-up menu includes the following values (in Kbps): 144, 160, 192, 208, 272, 384, 400, 416, 528, 768, 784, 1040, 1152, 1168, 1536, 1552, 1568, and 2320. The default value for both modes is 384.

Non-zero Virtual Path Identifier (VPI) support

- The **VPI** and **VCI** items allow you to configure the Virtual Path Identifier and Virtual Channel Identifier which together identify the ATM permanent virtual circuit used between the router and the remote device. The values configured for these items must match those configured in the remote device for data to flow between the devices. The **VPI** item may be set to any value between zero (0) and 255. (Earlier firmware versions allowed only a VPI value of zero (0). This restriction has been removed beginning with router firmware version 4.7.1. However, the ability to set a non-zero VPI value depends on both the router

firmware revision and the WAN interface module firmware revision. In order to use a non-zero VPI value, the WAN interface module firmware version must be version 1.0.20 or later. If an earlier version of WAN interface module firmware is present on the SDSL WAN interface module, the VPI value will be restricted to zero (0).) The **VCI** item may be set to any value between 0 and 65535.

LLC/SNAP encapsulated PPP support (RFC 2364)

- The **Data Link Encapsulation...** pop-up menu offers the choice of **RFC1483** and **PPP** encapsulations. Depending on which encapsulation you select, one of the following pop-up menu items will appear below the Data Link Encapsulation pop-up menu:
 - An **RFC1483 Mode...** pop-up menu is visible if the Data Link Encapsulation is set to RFC1483 and allows the choice between **Bridged 1483** (MAC-encapsulated Routing, also known as MER) and **Routed 1483**.
 - A **PPP Mode...** pop-up menu is visible if the Data Link Encapsulation is set to PPP and allows the choice between **VC Multiplexed** and **LLC/SNAP** encapsulated PPP.

Chapter 7

Filtering on the LAN interface

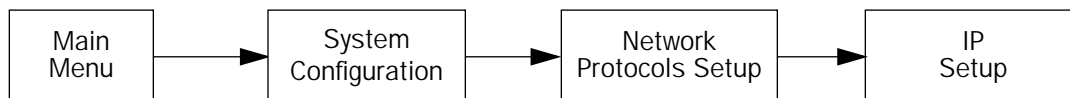
Introduced in version 4.7.1, the firmware offers LAN-side filtering on the Ethernet hub. This permits multiple IP addresses or subnets on the Ethernet LAN to be kept separate from one another and operate as virtual independent networks sharing a single Internet connection. Small- to medium-sized offices can benefit by using a single router to connect to the Internet, with multiple businesses within the office using independent subnets on the network. Schools can benefit by separating the administrative network from the student network.

The main advantage of filtering from the LAN is to limit users (or a set of users on a subnet) from accessing services such as telnet to the router to do configuration changes or accessing the internet via HTTP.

Companies desiring to limit certain departments from accessing to the Internet can use LAN-side filtering as well as schools desiring to prevent their student network from downloading files via FTP etc.

For information on creating multiple subnets, see the *User's Reference Guide* chapter on "IP Setup".

To attach a filter set to the Ethernet hub interface, navigate to the **IP Setup** screen from the **Main Menu**.



Any customized filter set you create can be associated with the Ethernet hub, as well as the WAN interface, as shown below:

IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP...	Both
Transmit RIP...	Off
LAN (EN Hub) Filter Set...	
Remove Filter Set...	
Static Routes...	IP Address Serving...
Network Address Translation (NAT)...	Filter Sets...

Set up the basic IP attributes of your Netopia in this screen.

Select **LAN (EN Hub) Filter Set** and from the pop-up menu, select the filter set you want to associate with the LAN interface. Press **Return**.

IP Setup

Ethernet IP Address: 192.168.1.1
 Ethernet Subnet Mask: 255.255.255.0
 Define Additional Subnets...

Default IP Gateway: 0.0.0.0
 Backup IP Gateway: 0.0.0.0
 Primary Domain Name Server: 0.0.0.0
 Secondary Domain +-----+
 Domain Name: +-----+

Receive RIP... Transmit RIP... LAN (EN Hub) Filt Remove Filter Set Static Routes... Network Address Tran	Basic Firewall NetBIOS Filter My LAN Filter Set 1 My LAN Filter Set 2
---	--

The filter set you select will be applied to the Ethernet hub interface.

Caution! You should not attach the default filter sets **Basic Firewall** or **NetBIOS Filter** to the Ethernet LAN or its subnets. This may result in a loss of connectivity to the network or subnet. Instead, create a **new** filter set in accordance with the standard filtering rules described in your *User's Reference Guide*.

To remove the filter set from the Ethernet hub interface, select **Remove Filter Set** and press **Return**. The filter set will be disconnected from the LAN interface.

Note: Removing the filter set from the LAN does not delete the filter set. It is still available to be reassociated with the same or another interface, or modified further.

For more information on filters and filter sets, see the on-line *User's Reference Guide* chapter on "Security."

Chapter 8

PPP over Frame Relay for R3100 and R7100 Routers

Many service providers that use Copper Mountain access concentrator equipment require the capability of encapsulating PPP information via Frame Relay. Authenticated Internet accounts require User Name and Password information to allow you to connect. Firmware version 4.6.2 introduced support for PPP Data Link Encapsulation for all R-series routers that support Frame Relay. This permits user authentication via PPP over the Frame Relay WAN link.

This is not the same as Multilink PPP (MLPPP) discussed in [Chapter 11, “DSL Bonding.”](#) PPP over Frame Relay is primarily intended to facilitate user authentication, as well as to provide a Data Link Encapsulation method used by service providers who require it.

To use PPP over Frame Relay, first enable Frame Relay as the Data Link Encapsulation method on the WAN link in the appropriate Line Configuration screen. Next, enable PPP over Frame Relay and create a corresponding Connection Profile. Finally, provide your authentication information in that Connection Profile.

This can be done in either:

- the series of Easy Setup console screens (see [“Easy Setup method” on page 8-2](#))

or, for advanced users, who need more than one Connection Profile or require additional features in the Connection Profile,

- in the WAN Configuration screens (see [“Advanced WAN Configuration method” on page 8-4](#))

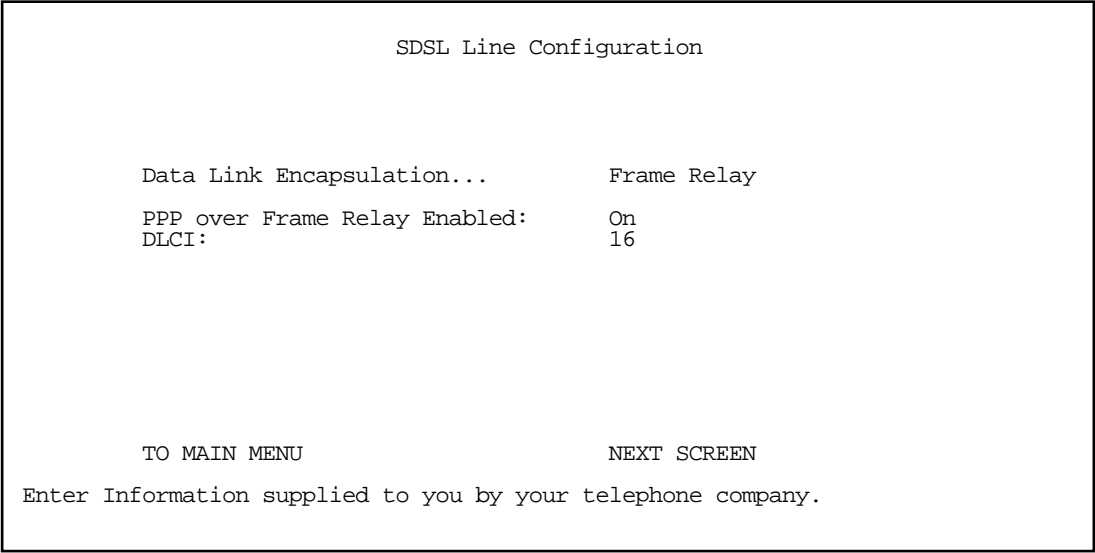
Note: In the examples that follow, the configuration screens shown are for a Netopia R7100 SDSL router. For other R-series router models, your screens may show variations appropriate to your specific model.

Easy Setup method

In the Easy Setup screens you first enable Frame Relay on the WAN interface, using the Easy Setup Line Configuration screen, then define the PPP Connection Profile, using the Easy Setup Profile screens, as follows:

From the Main Menu, select **Easy Setup** and press **Return**.

The **Line Configuration** screen appears (in this example, the **SDSL Line Configuration** screen).



- If you select **Frame Relay** from the **Data Link Encapsulation** pop-up menu, the **PPP over [WAN_Interface_Type] Enabled** toggle item becomes visible. To enable PPP, toggle this item to **On**, using the Tab key and press **Return**.
- Select **NEXT SCREEN** and press **Return**.

The **Easy Setup Profile** screen appears.

Connection Profile 1: Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Unnumbered

Remote IP Address:

0.0.0.0

Remote IP Mask:

0.0.0.0

Send User Name:

michaelt

Send Password:

PREVIOUS SCREEN

NEXT SCREEN

Enter basic information about your WAN connection with this screen.

- Using the **Down** arrow key, navigate down the menu items and select **Send User Name**. Type the user name that identifies you to your service provider. Press **Return**.
- Select **Send Password** and type the password that authenticates you to your service provider. Press **Return**.
- Select **NEXT SCREEN** and press **Return**. When you exit the Easy Setup profile screen, a Connection Profile is created that contains the information that you have entered.

If you need to change any of the other parameters in the Easy Setup screens, you can do so by accessing Easy Setup from the Main Menu. For more information on Easy Setup and Connection Profiles, see the respective sections in the on-line *User's Reference Guide* on your Netopia CD.

Advanced WAN Configuration method

In the WAN Configuration screens you first enable Frame Relay on the WAN interface, using the Line Configuration screen, then add a PPP Connection Profile, using the Add Connection Profile screens, as follows:

From the Main Menu, select **WAN Configuration** then **WAN Setup** and press **Return**.

The **Choose Interface to Configure** screen appears.

Choose Interface to Configure

CMN SDSL (Wan Module 1) Setup...

Auxiliary Serial Port Setup...

Configuration Changes Reset WAN Connection: Yes

Select [*WAN_Interface_Type*] (**Wan Module 1**) **Setup** and press **Return**.

The **Line Configuration** screen appears (in this example, the **SDSL Line Configuration** screen).

SDSL Line Configuration

Clock Source...

Network

Data Link Encapsulation...

Frame Relay

PPP over Frame Relay Enabled:

On

DLCI:

16

Prioritize Delay-Sensitive Data:

No

Enter Information supplied to you by your telephone company.

- If you select **Frame Relay** from the **Data Link Encapsulation** pop-up menu, the **PPP over [WAN_Interface_Type] Enabled** toggle item becomes visible. To enable PPP, toggle this item to **On**, using the Tab key and press **Return**.
- Press **Escape** twice to return to the WAN Configuration screen. Select **Add Connection Profile** and press **Return**.

The **Add Connection Profile** screen appears.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
IPX Enabled:	No
Interface Group...	Primary
Telco Options...	
ADD PROFILE NOW	CANCEL
Configure a new Conn. Profile. Finished? ADD or CANCEL to exit.	

- Select **PPP** from the **Data Link Encapsulation** pop-up menu, then select **Data Link Options** and press **Return**.

The **Datalink (PPP/MP) Options** screen appears.

Datalink (PPP/MP) Options

Data Compression...	Standard LZS
Send Authentication...	PAP
Send User Name:	michaelt
Send Password:	*****
Receive User Name:	
Receive Password:	
Maximum Packet Size:	1500

In this Screen you will configure the PPP/MP specific connection params.

- Select **Send User Name** and type the user name that identifies you to your service provider. Press **Return**.
- Select **Send Password** and type the password that authenticates you to your service provider. Press **Return**.
- Press **Escape** to return to the **Add Connection Profile** screen. Select **ADD PROFILE NOW** and press **Return**.

When you exit the screen, a Connection Profile is created that contains the information that you have entered. If you need to change any of the other parameters in the WAN Configuration screens, you can do so by accessing them from the Main Menu. For more information on WAN Configuration and Connection Profiles, see the respective sections in the on-line *User's Reference Guide* on your Netopia CD.

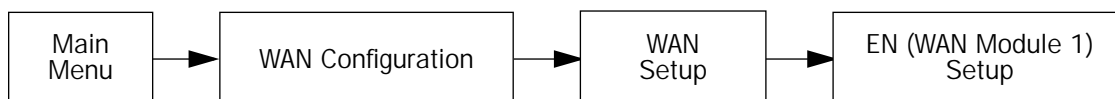
Chapter 9

PPP over Ethernet

The firmware supports the Point-to-Point protocol over Ethernet (PPPoE) for R9100 routers that are required to use PPP to connect through a DSL or cable modem. Some ISPs require user name and password authentication to connect you with their DSL or cable service. PPPoE allows user name and password authentication to the ISP via your R9100's Ethernet interface to your DSL or cable modem.

To configure PPP authentication in your R9100, you first enable PPP over Ethernet and then create a Connection Profile for your Internet connection.

From the **Main Menu** select **WAN Configuration**, **WAN Setup**, and then **EN (Wan Module 1) Setup**. Press **Return**.



The WAN Ethernet Configuration screen appears.

WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set...	
Remove Filter Set	
Receive RIP:	Both
Enable PPP over Ethernet:	On
Wan Ethernet MAC Address:	00:00:c5:70:03:4a

Toggle **Enable PPP over Ethernet** to **On**, using the Tab key. Press **Return**, and then **Escape** twice to return to **WAN Configuration**. Select **Add Connection Profile**. Press **Return**.

The **Add Connection Profile** screen appears.

```

                                Add Connection Profile

Profile Name:                    My_ISP
Profile Enabled:                 Yes
Data Link Encapsulation...      PPP
Data Link Options...
IP Enabled:                     Yes
IP Profile Parameters...

Interface Group...              Primary

ADD PROFILE NOW                 CANCEL

Configure a new Conn. Profile. Finished? ADD or CANCEL to exit.
```

From the **Data Link Encapsulation** pop-up menu, select **PPP**.

Select **Data Link Options** and press **Return**.

The **Datalink (PPP/MP) Options** screen appears.

```

                                Datalink (PPP/MP) Options

Data Compression...             Standard LZS
Send Authentication...           PAP
Send User Name:                 jagdip
Send Password:                  *****
Receive User Name:
Receive Password:

Dial...                         Dial In/Out
Dial on Demand:                 Yes

Idle Timeout (seconds):         300
Maximum Packet Size:            1500

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
```

Enter your User Name and Password and press **Return**. Press **Escape** to return to the Add Connection Profile screen.

Select **ADD PROFILE NOW** and press **Return**. Your Connection Profile will be created and activated with your authentication information to connect to your ISP's service.

Chapter 10

Version 4.6 Feature Enhancements

Introduced in the version 4.6 firmware the current release contains several feature enhancements:

- “Extended IP Compression Protocol Options” on page 10-1
- “Increased Static Route Count” on page 10-1
- “Internet Control Message Protocol Filtering” on page 10-2
- “Console Password Confirmation” on page 10-4
- “Delayed Remote Configuration Change Toggle” on page 10-6
- “User-definable DHCP Lease Times” on page 10-8
- “RFC1973 LMI Support” on page 10-9
- “Copper Mountain DHCP Server Support” on page 10-10
- “PPP Ethernet LAN Reconfiguration” on page 10-15
- “RIP Profile Options” on page 10-17
- “Connection Profile Changes Require COMMIT” on page 10-18
- “47-Character PPP Authentication String Support” on page 10-19

Extended IP Compression Protocol Options

The firmware supports extended IPCP options for DNS resolution. See the *User’s Reference Guide* chapter on “IP Setup” for information about DNS configuration.

- The DNS address serving behavior is changed beginning with firmware version 4.6. Previously, when the remote end would request a DNS server address via IPCP, the Netopia router would supply the DNS configured in the router. Beginning with firmware version 4.6, the Netopia router will supply whatever DNS address that is either manually configured or acquired dynamically. This permits a DNS to be served that was acquired via DHCP, for example.
- When there is no static DNS configured in the Netopia router (locally set to 0.0.0.0), the router will request both a primary and a secondary DNS via IPCP (as outlined in RFC 1877). This will eliminate the need to locally configure a DNS when the ISP supports this feature. The DNS address will be visible in the Quickview screen.

Increased Static Route Count

The firmware supports an increased number of static routes. You can assign up to 32 static routes. See the *User’s Reference Guide* for information about assigning static routes.

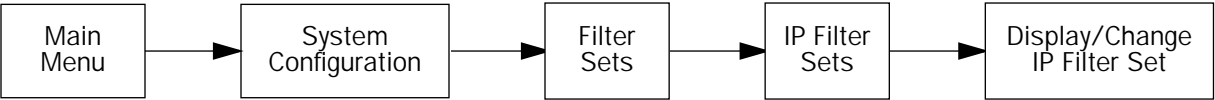
Internet Control Message Protocol Filtering

The firmware offers ICMP Type and Code filtering.

IP Filtering is enhanced to allow for identifying and filtering ICMP packets, in addition to both UDP and TCP packets. Both the console menu and SNMP support this feature. See the “Security” chapter in the *User’s Reference Guide* for information about setting up Filters and Filter Sets.

Console-based management

You access the Filtering features in the console menu from the Main Menu by navigating to **System Configuration, Filter Sets**, then **IP Filter Sets**.



Select **Add IP Filter Set** to add a new one or **Display/Change IP Filter Set** to alter an existing one.

You are permitted to enter either “ICMP” or “1” (ICMP’s Protocol Type) in the **Protocol Type** field of an Input or Output filter as shown in the sample screen below. If you enter ICMP or 1, the **ICMP Type Compare** and **ICMP Code Compare** fields display.

Add Input Filter

Enabled:	Yes
Forward:	No
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	ICMP
ICMP Type Compare...	Equal
ICMP Type:	0
ICMP Code Compare...	No Compare
ICMP Code:	0
ADD THIS FILTER NOW	CANCEL

Enter a type: 'ICMP', 'UDP', 'TCP', 'Any', or a number between 0 and 255.

- **ICMP Type Compare** – Select one of the following options from the pop-up menu: No Compare, Not Equal To, Less Than, Less Than or Equal, Equal, Greater Than or Equal, or Greater Than.
- Every ICMP packet has an 8-bit integer field, *Type*, that identifies what kind of ICMP packet (of 13 possible

packet types) it is. **ICMP Types** you can enter can include the following:

Type	Description
0	Echo reply
3	Destination unreachable
8	Echo request

- **ICMP Code Compare** – Select one of the following options from the pop-up menu: No Compare, Not Equal To, Less Than, Less Than or Equal, Equal, Greater Than or Equal, or Greater Than.
- In addition to the Type, an 8-bit field, *Code*, gives more information about the Type. **ICMP Codes** include:

Code	Description
0	Network Unreachable
1	Host unreachable
6	Destination network unknown
7	Destination host unknown

It is unlikely that you would need to filter on ICMP code types. However, if you should find it necessary, refer to standard texts on internetworking with TCP/IP for more information.

SNMP

For SNMP management, the latest **Netopia MIB** is modified so that old leaves have been renamed generically. The following table shows the old and new names.

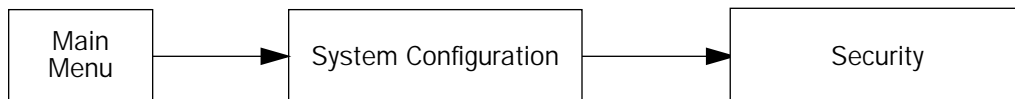
old leaf name	new leaf name
ipFilterSrcPortComparison	ipFilterData1Comparison
ipFilterSrcPort	ipFilterData1
ipFilterDstPortComparison	ipFilterData2Comparison
ipFilterDstPort	ipFilterData2

The MIB textual descriptions have been modified to reflect the fact that these fields are now used by UDP and TCP for port matching, and ICMP for code and type field matching.

Console Password Confirmation

The console menu includes a Password Confirmation field in the Security Options screen. This verifies that you have assigned the correct password when configuring password protection on the router configuration menus.

From the **Main Menu** select **System Configuration** and then **Security**. Press **Return**.



The **Security Options** screen appears.

The password you enter is displayed as asterisks as shown below, rather than clear text.

Security Options	
Enable Dial-in Console Access:	Yes
Enable SmartStart/Web Server:	Yes
Enable Telnet Console Access:	Yes
Enable Telnet Access to SNMP Screens:	Yes
Console Access timeout (seconds):	600
Show Users...	
Add User...	
Delete User...	
Password for This Screen (11 chars max):	*****
Configuration Changes Reset WAN Connection:	Yes

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

When you enter your password, you are prompted to confirm it by re-entering it in a pop-up window.

```

Security Options

+-----+
En+-----+
En      Password Confirmation
En
En      Please re-enter Password:      *****
Co
Co
Sh      CANCEL
Ad
De+-----+

Password for This Screen (11 chars max):      *****

Configuration Changes Reset WAN Connection:      Yes

```

Re-type your password to confirm your entry. When you press **Return**, the password becomes effective.

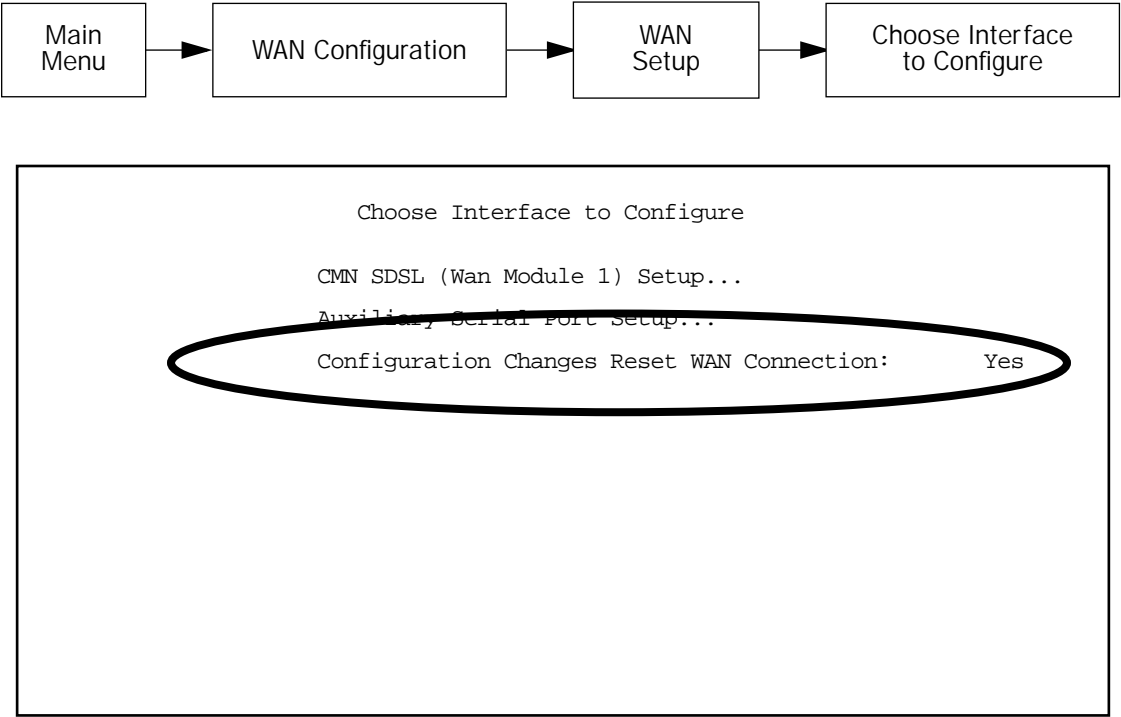
Delayed Remote Configuration Change Toggle

The console menu supports delaying some configuration changes until after the router is restarted.

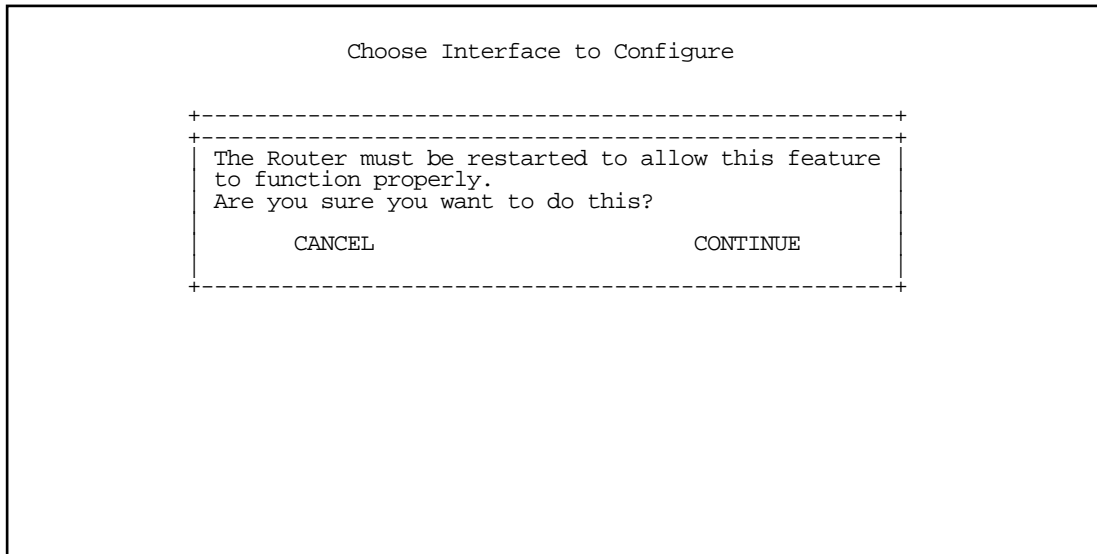
If your router is preconfigured by your service provider, or if you are not remotely configuring the router, you can leave this setting unchanged.

The purpose of this feature is to defer configuration changes *only* when remotely configuring or reconfiguring the router to prevent premature console disconnection. When this feature is enabled, no changes to the WAN setup, datalink encapsulation, Connection Profiles, DLCIs, or Default Gateways will take effect until after the router is restarted. Until the router is restarted the WAN link and the routing table remain unaffected.

A single setting in the **Choose Interface to Configure** screen controls this feature, as shown below.



When you toggle **Configuration Changes Reset WAN Connection** either to Yes or No using the Tab key and press Return, a pop-up window asks you to confirm your choice.



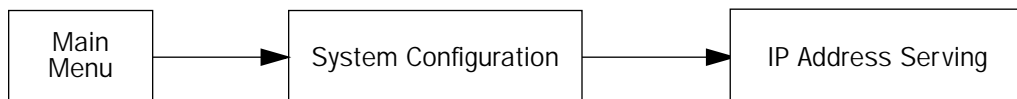
Toggling from **Yes** to **No** makes the router ready to be configured. If you toggle from **No** to **Yes** after any configuration changes have been entered (and confirm the reboot), your changes are committed and the router comes up using the newly created configuration.

User-definable DHCP Lease Times

The firmware supports user-definable served IP address DHCP lease times.

The default DHCP Lease time is one hour. This may be unnecessarily brief in your network environment. Consequently, the DHCP lease time is now configurable in the IP Address Serving screen.

From the Main Menu navigate to **System Configuration** and then **IP Address Serving**.



The IP Address Serving screen offers a new field **DHCP Lease Time (Hours)** allowing you to modify the router's default lease time of one hour as shown below:

IP Address Serving	
IP Address Serving Mode...	DHCP Server
Number of Client IP Addresses:	100
1st Client Address:	192.168.1.100
Client Default Gateway...	192.168.1.1
Serve DHCP Clients:	Yes
DHCP Lease Time (Hours):	1
DHCP NetBIOS Options...	
Serve BOOTP Clients:	Yes
Serve Dynamic WAN Clients	Yes

Configure Address Serving (DHCP, BOOTP, etc.) here.

You can enter any number up to and including 168 (one week) for the DHCP lease.

RFC1973 LMI Support

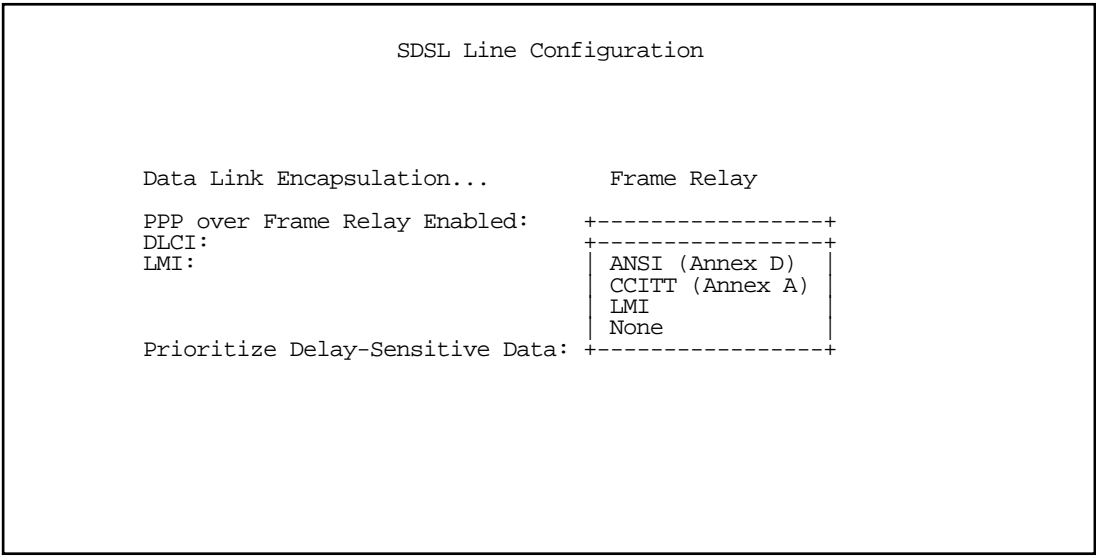
Introduced in version 4.8, the firmware provides RFC 1973 Local Management Interface (LMI) support. LMI is a set of enhancements to the basic Frame Relay specification that includes support for:

- a keep-alive mechanism, which verifies that data is flowing
- a multicast mechanism, which provides the network server with its local DLCI and the multicast DLCI
- global addressing, which gives DLCIs global rather than local significance in Frame Relay networks
- a status mechanism, which provides an on-going status report on the DLCIs known to the switch

RFC1973 LMI support applies to all routers that support RFC1973 (R3000-series and R7100-series routers).

The console menu contains new pop-up menus that permit you to configure the LMI when you choose RFC1973 encapsulation, as shown in the following example screen.

Note: The example is an R7100 Easy Setup screen, but the same applies for the R3000-series and corresponding Advanced Configuration screens.



When you choose **Frame Relay** as the data link encapsulation method and **PPP over Frame Relay Enabled** is set to **On**, the LMI option becomes available in the pop-up menu.

Copper Mountain DHCP Server Support

Introduced in version 4.8, the firmware offers Dynamic Host Configuration Protocol (DHCP) client support for the Copper Mountain proprietary operation mode necessary to interoperate with a Copper Mountain Networks Copper Edge 200 DSLAM-based DHCP server. This operation mode supplements but does not replace the existing standards-based mode of operation.

You set the DHCP operation mode for each Connection Profile either by modifying the default setting in the Easy Setup Profile or by adding a new Connection Profile through the WAN Configuration menus and specifying the mode in the appropriate IP Profile Parameters screen.

Overview

Netopia firmware version 4.1 introduced support for the frame-based R7100 SDSL Router compatible with the CE200 DSLAM. This release included the ability to automatically configure the SDSL WAN interface via DHCP when the data link encapsulation was set to RFC1483 MAC-Encapsulated Routing (MER) and no local WAN IP address was configured. This implementation was a standards-based implementation that conformed in all respects with the Dynamic Host Configuration Protocol specification in RFC 2131.

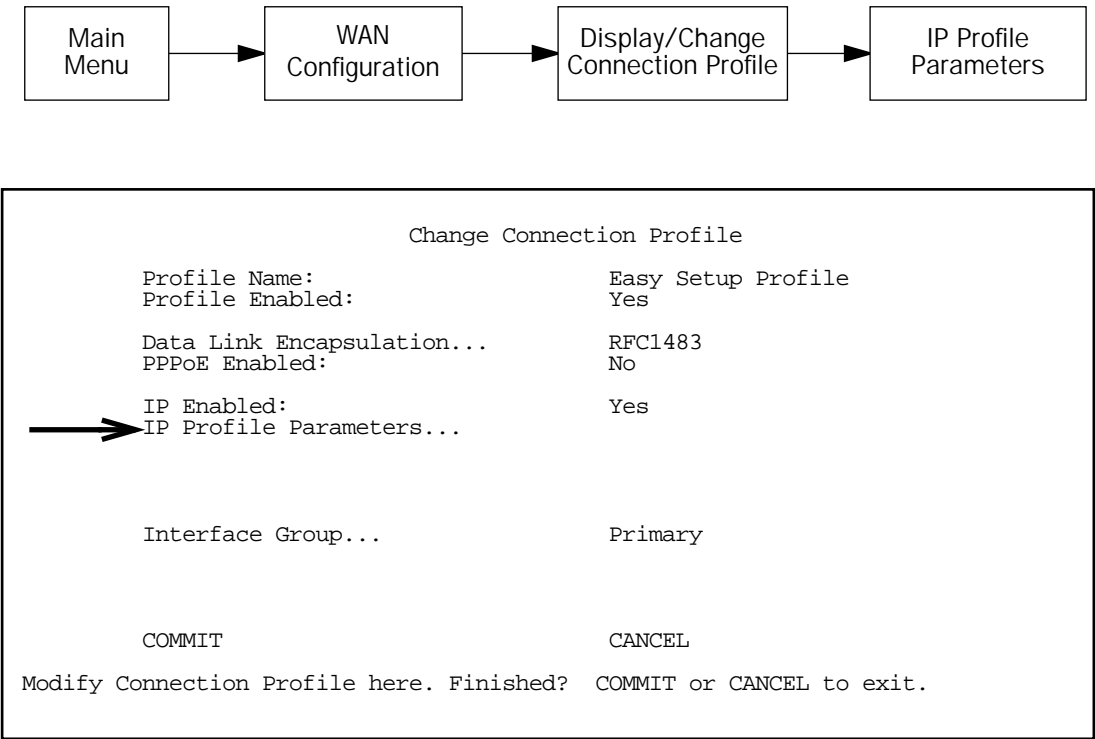
Beginning with CE200 firmware release 2.1, Copper Mountain added the ability for the DSLAM itself to act as a DHCP server. In this mode, the CE200 DSLAM intercepts and responds to DHCP requests from CPE routers.

Prior to Netopia version 4.8 firmware, the Netopia router DHCP client implementation did not interoperate with the CE200-based DHCP server. The 4.8 firmware release added support for the Copper Mountain proprietary mode of operation necessary to interoperate with a CE200-based DHCP server.

Configuration

You configure a Connection Profile's DHCP mode in the [IP Profile Parameters](#) screen or the [IP Parameters \(Default Profile\)](#) screen.

You access the IP Profile Parameters screen for a Connection Profile through the WAN Configuration menus.



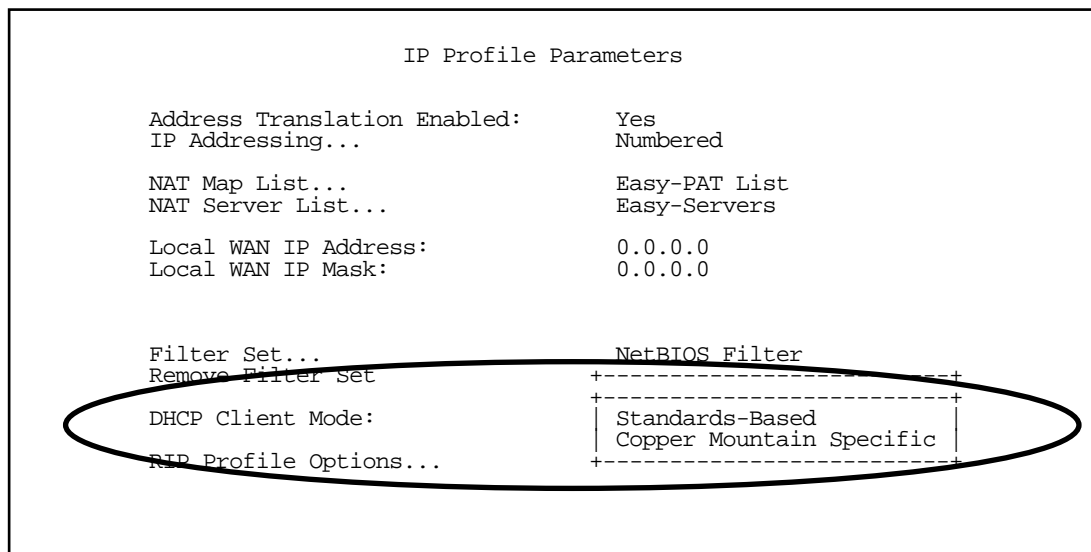
Set **Data Link Encapsulation** to **RFC1483** and select **IP Profile Parameters**.

IP Profile Parameters

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Filter Set... NetBIOS Filter	
Remove Filter Set	+-----+-----+
DHCP Client Mode:	Standards-Based Copper Mountain Specific
IP Profile Options...	+-----+-----+



The **Local WAN IP Address** must be set to acquire an IP address from the DHCP server; that is, it must be 0.0.0.0.

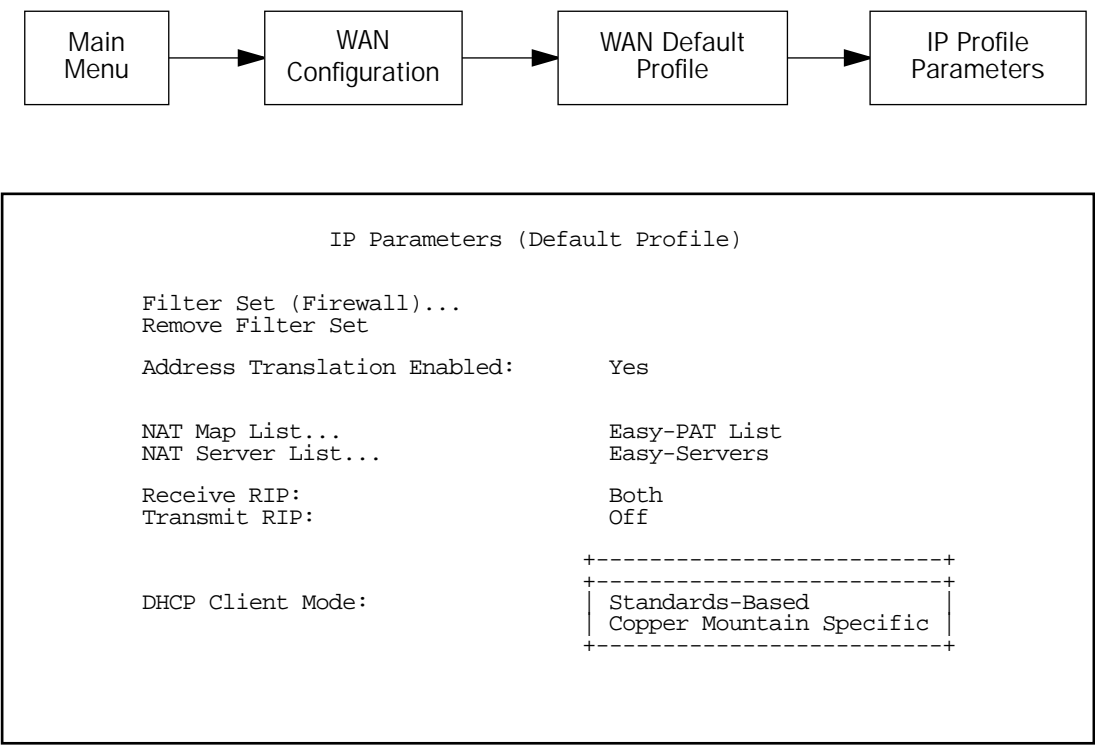
By selecting **DHCP Client Mode**, you can choose either Standards-Based (the default) or Copper Mountain Specific.

DHCP Client Mode is visible for RFC1483 MAC-Encapsulated Routing (MER) Connection Profiles configured to act as a DHCP client; that is, no Local WAN IP Address is configured.

- **Standards-Based** selects the DHCP client behavior specified by RFC 2131.
- **Copper Mountain Specific** selects the Copper Mountain proprietary DHCP client behavior.

IP Parameters (Default Profile)

You configure the DHCP mode for the WAN Default Profile in an analogous manner on the IP Parameters (Default Profile) screen of the WAN Default Profile menu.

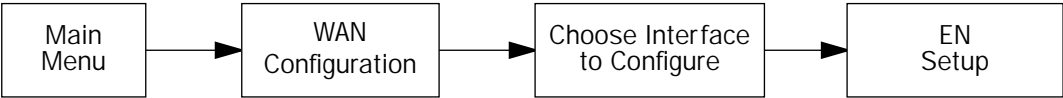


By selecting **DHCP Client Mode**, you can choose either Standards-Based (the default) or Copper Mountain Specific.

Note: The **Local WAN IP Address** must be set to acquire an IP address from the DHCP server; that is, it must be 0.0.0.0. DHCP Client Mode is visible for RFC1483 MAC-Encapsulated Routing (MER) Connection Profiles configured to act as a DHCP client; that is, no Local WAN IP Address is configured.

WAN Ethernet Configuration

For an R9100 Ethernet-to-Ethernet router, you configure the DHCP mode for the WAN Ethernet Configuration on the WAN Ethernet Configuration screen.



WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set...	
Remove Filter Set	
Enable PPP over Ethernet:	On
Wan Ethernet MAC Address:	00:00:c5:78:5d:12
DHCP Client Mode:	<div>Standards-Based</div> <div>Copper Mountain Specific</div>
RIP Options...	

PPP Ethernet LAN Reconfiguration

Introduced in version 4.8, the firmware adds the ability for PPP to reconfigure the router's Ethernet LAN when establishing an unnumbered, non-NAT connection.

In firmware versions earlier than 4.8, when establishing an unnumbered, non-NAT connection, PPP would not request or accept a different IP address from the PPP peer. When establishing a numbered connection, PPP does request an IP Address for the WAN interface if no local WAN IP address was configured.

The version 4.8 firmware allows a central site router to supply an entire IP subnet, rather than a single IP address, for use by a Netopia router. If the applicable Connection Profile specifies an unnumbered, non-NAT connection and Negotiate LAN IP Addr/Mask is set to On, PPP will attempt to negotiate both an IP Address and subnet mask.

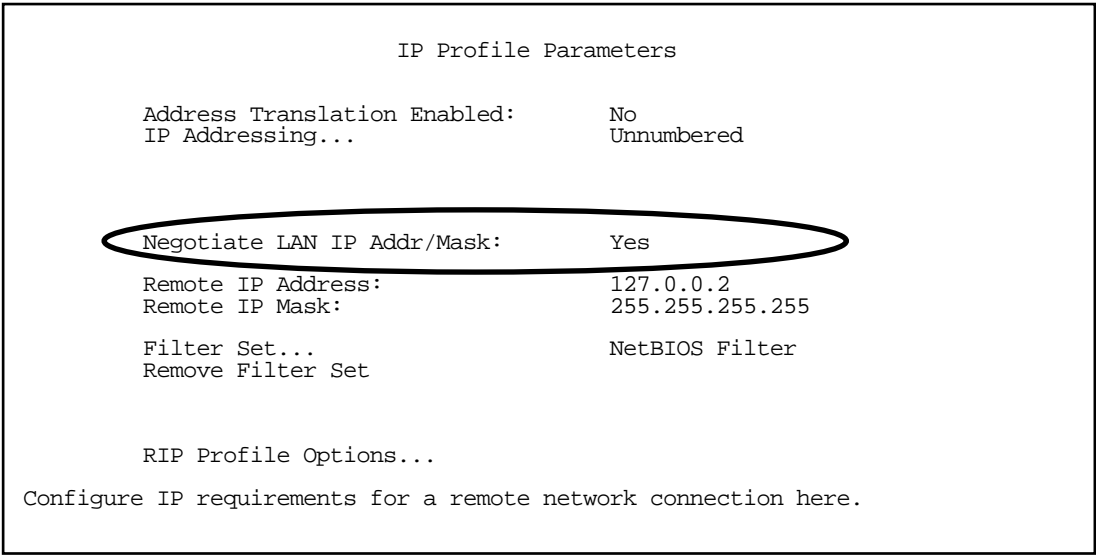
Note: Once the router has reconfigured the address serving pool only to conform to the negotiated subnet, you can adjust the base or extent of the pool and reboot the router. Your adjustments will not be overwritten when the connection is next renegotiated because the router only reconfigures the address serving pool if it lies outside the negotiated subnet.

The router does not adjust any address serving parameters other than the base and extent of the address serving pool. This allows you to otherwise configure address serving as you please using the normal address serving configuration items. For example, if you disable address serving, the router will not enable address serving when it reconfigures the address serving pool.

Configuration

To enable PPP Ethernet LAN configuration, navigate to the IP Profile Parameters screen of the Connection Profile you want to use. This can be either the Easy Setup Profile or any other Connection Profile you have added.

The IP Profile Parameters screen for a Connection Profile displays a Negotiate LAN IP Addr/Mask toggle:



- This toggle is visible only if the profile’s Data Link Encapsulation is set to **PPP**, the Address Translation Enabled toggle is set to **No** and IP Addressing is set to **Unnumbered**. The default value is **No**.
- RIP Profile Options is not visible if Negotiate LAN IP Addr/Mask is set to **Yes** and the Remote IP Mask is set to **0.0.0.0**. See “RIP Profile Options” on page 10-17 for more information.

Quick View

The Quick View screen (as shown below) displays both Primary and Secondary DNS Server addresses. This is useful because both may be served via PPP.

Quick View

8/8/2000 10:46:14 AM

Default IP Gateway: 163.176.12.1

CPU Load: 6%

Unused Memory: 232 KB

Primary DNS Server: 163.176.4.31

WAN Interface Group -- EN

Secondary DNS Server: 163.176.4.10

Domain Name: isp.com

-----MAC Address-----IP Address-----

Ethernet Hub: 00-00-c5-78-5d-10 192.168.1.1

Ethernet WAN1: 00-00-c5-78-5d-12 0.0.0.0

Current WAN Connection Status

Profile Name-----Rate--%Use-Remote Address-----Est.-More Info-----

VPN QuickView

LED Status

PWR+-----WAN1-----+-----CON--AUX-----+-----EN--+-----LEDS-----

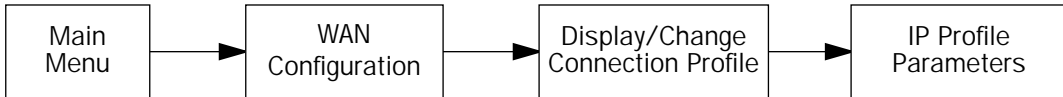
LNK RDY CH1 CH2 LNK LNK DATA | '-'= Off 'G'= Green

G - G - - Y - - | 'R'= Red 'Y'= Yellow

RIP Profile Options

Introduced in version 4.8, the firmware changes the IP Profile Parameters RIP Profile Parameters screen for Connection Profiles.

The three Routing Information Protocol (RIP) options, Receive RIP, Transmit RIP, and TX RIP Policy, have been moved to a new RIP Profile Parameters screen. To access the RIP Profile Parameters screen you navigate from the Main Menu to WAN Configuration, Display/Change Connection Profile, and IP Profile Parameters.



You access the RIP Profile Parameters screen via the **RIP Profile Options** item on the IP Profile Parameters screen.

IP Profile Parameters	
Address Translation Enabled: IP Addressing...	No Unnumbered
Negotiate LAN IP Addr/Mask:	Yes
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	NetBIOS Filter
Remove Filter Set	
RIP Profile Options...	
Configure IP requirements for a remote network connection here.	

When you select **RIP Profile Options** and press Return, the RIP Profile Parameters screen appears.

RIP Profile Parameters	
Receive RIP:	Both
Transmit RIP:	v2 (multicast)
TX RIP Policy...	Poison Reverse

For detailed information on these RIP options, see the chapter on "IP Setup" in the *User's Reference Guide*.

Connection Profile Changes Require COMMIT

In order to ensure that Connection Profile configurations can be changed without immediately affecting your connection, the Add/Change Connection Profile menus now operate on an internal *copy* of the profile until you press **COMMIT**. If you change your mind and decide not to make the changes as you have entered them, press **CANCEL** and your changes are discarded.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
Interface Group...	Primary
COMMIT	CANCEL

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

47-Character PPP Authentication String Support

PPP authentication strings for username and password (PAP) and hostname and secret (CHAP) may now be up to 47 characters.

Chapter 11

DSL Bonding

Introduced in version 4.6, the firmware incorporates DSL Bonding technology for increased bandwidth supported on new Internet equipment and upgrade options.

Introduced in firmware version 4.7.1 is the ability to bond up to four IDSL or leased ISDN circuits using Multilink PPP to provide bandwidth of up to 576 Kbps at distances of up to 36,000 feet from a Central Office. By using PPP, IP service providers can aggregate the bandwidth of multiple IDSL or ISDN circuits without regard to the manufacturer or configuration of the local loop carrier's equipment.

The version 4.8 firmware offers Multilink PPP-based DSL Bonding support for new R6161 ADSL and R7272 SDSL routers. R7171 routers gain Multilink PPP DSL Bonding support as well. This requires that PVCs be set on a per-WAN interface basis.

This chapter covers the following topics:

- [“About DSL Bonding” on page 11-1](#)
- [“Bonded DSL Configuration” on page 11-3](#)
- [“Multilink PPP for Bonded IDSL and Leased ISDN Routers” on page 11-6](#)
- [“Multilink PPP Configuration” on page 11-7](#)
- [“Monitoring” on page 11-12](#)
- [“Multilink PPP-based DSL Bonding Support for ADSL and SDSL Routers” on page 11-14](#)

About DSL Bonding

DSL Bonding, also called inverse multiplexing or IMUX, technology combines the bandwidth of multiple DSL (Digital Subscriber Line) circuits into a single virtual data pipe.

Before DSL Bonding was developed, the maximum speed of a DSL connection was dependent on the customer's distance from the central office. DSL Bonding allows customers who are located at greater distances from the central office to aggregate DSL circuits, in order to achieve two or more times the speed otherwise available to them with a single line.

The premise behind DSL Bonding is to provide a cost-effective means of bridging the bandwidth gap between relatively low network speeds and much higher rates, thereby allowing high-speed applications to use bandwidth up to 3 Mbps.

Netopia's DSL routers and DSUs with bonding allow users with 1.5 Mbps SDSL connections to enjoy speeds of over 3 Mbps, twice as fast as T1. They also allow customers who, because of line quality problems, were previously limited to a 144 Kbps IDSL connection, to enjoy speeds of up to 576 Kbps.

Supported equipment

Netopia Internet equipment incorporating DSL Bonding includes:

- The Netopia R7171 SDSL Router and the Netopia D7171 SDSL DSU, which support two SDSL circuits for

speeds of over 3 Mbps.

- The Netopia R3232 IDSL Router and Netopia D3232 IDSL DSU, which support up to four BRI circuits for speeds of up to 576 Kbps

If you want to take advantage of DSL Bonding you can upgrade your existing Netopia router or DSU with the following new add-on WAN modules:

- Netopia TER/71 SDSL, which adds a second SDSL WAN interface module to a Netopia R7100 Router or D7100 DSU
- Netopia TER/32 IDSL, which adds two more IDSL connections to a Netopia R3100-I IDSL Router

Netopia's DSL Bonding products are designed to work with Copper Mountain's family of CopperEdge DSL concentrators.

What DSL Bonding does

DSL Bonding is the opposite, or inverse, of traditional multiplexing:

- The concept of multiplexing applies when a number of relatively small data streams are combined into a single line with greater bandwidth, in order to increase the efficiency and maximize utilization of a higher speed WAN connection. An example of multiplexing would be the combination of multiple DS0 links in a single T1 or E1 circuit.
- DSL Bonding takes a single high-speed data stream and spreads it across several lower speed physical links, which logically form a single aggregated channel or group. Multiple SDSL or IDSL lines are combined to create a single logical data channel that is the aggregate of the individual lines' bandwidths, minus a small amount used for overhead. A packet of information from a LAN, video conferencing session, or other data application is broken down into individual bits or cells which are transmitted in a round robin fashion across two SDSL or IDSL circuits. At the other end of the link, the bits or cells are reassembled in the same order in which they were transmitted, and the reconstructed packet is sent on to the recipient's networking equipment.

From the point of view of the routers or other devices connected to the inverse multiplexers, they are communicating via a single high-speed WAN channel at some multiple of the SDSL or IDSL rate. This is especially important when an application's bandwidth requirements are high. But a high bandwidth service is either difficult to obtain or too expensive. Some examples include: a university offering remote educational services, or distance learning, may require very high bandwidth across the WAN in order to maintain acceptable quality for its classroom video. Bringing together relatively less expensive, lower speed SDSL or IDSL circuits to form a single high-speed link often saves a company a significant amount money. The savings can pay for the inverse multiplexer in a few months.

Netopia DSL Bonding

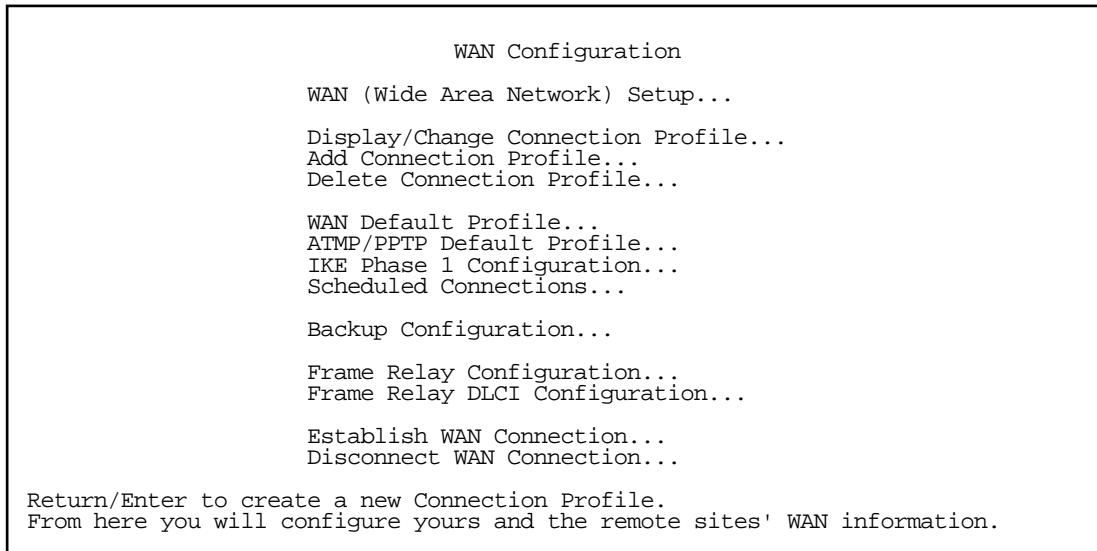
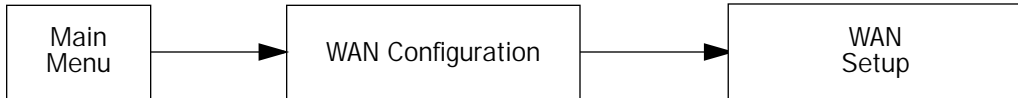
Netopia's DSL Bonding implementation is based on a technique used in Copper Mountain Networks CopperEdge DSL Access Concentrators. Copper Mountain's approach conforms with the Multi-link Frame Relay (MFR) protocol. However, where DML operates between the CPE and DSLAM, MFR would more likely operate between the CPE and Frame Relay terminator (potentially the ISP's router).

The Copper Mountain approach allows the bonding of multiple physical DSL links into a single logical channel. The logical channel may use RFC1483 FUNI, RFC1490 and/or Q.922 Frame Relay, or RFC1661/1662 PPP data link encapsulations. In addition, the physical links support Copper Mountain's control protocol (CMCP).

Bonded DSL Configuration

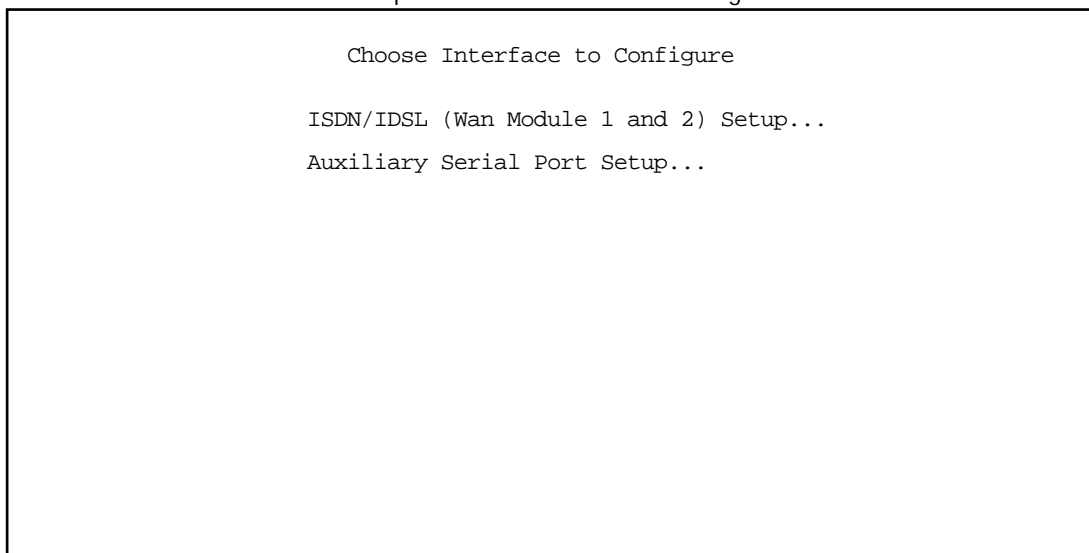
Configuring a bonded DSL link is the same as configuring a single link. The firmware auto-senses the presence of bondable WAN interface modules and aggregates the channels based on whatever hardware you have installed in the router or DSU.

Beginning with firmware version 4.5, you have access to configuration options for the external WAN interfaces of the router or DSU from a single screen under the WAN Configuration menu. Navigate to **WAN Setup** under the WAN Configuration menu and press **Return**.

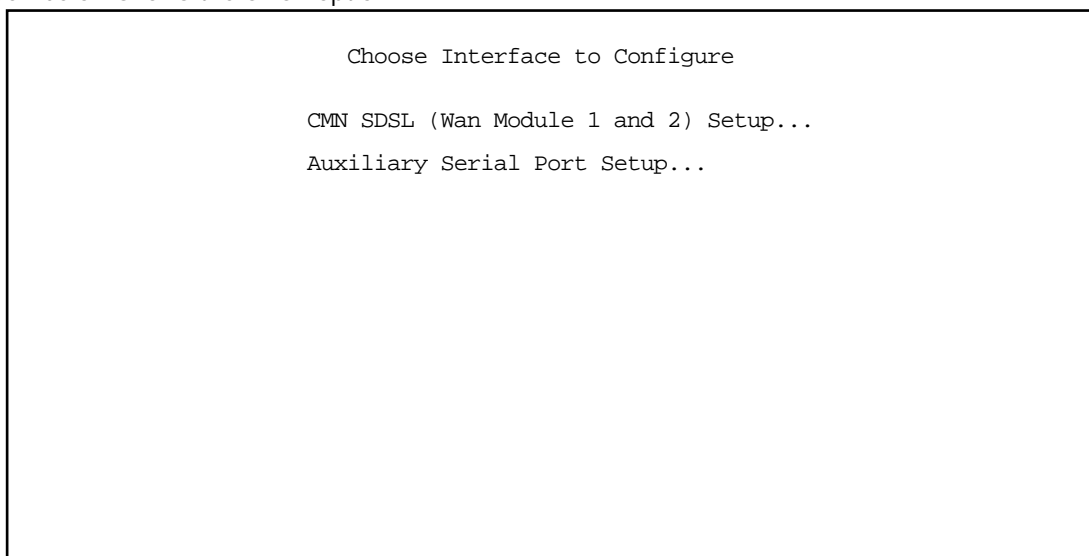


The **Choose Interface to Configure** screen appears.

The screen below shows the ISDN/IDSL option for the WAN to be configured.



The screen below shows the SDSL option.



Both screens show the dual WAN interfaces as a single bonded interface, and you configure them together by selecting **(Wan Module 1 and 2) Setup...** and pressing **Return**.

The Line Configuration screen appears, either **SDSL Line Configuration**,

SDSL Line Configuration	
Clock Source...	Network
Data Link Encapsulation...	RFC1483
Prioritize Delay-Sensitive Data:	No

Enter Information supplied to you by your telephone company.

or **ISDN Line Configuration**, depending on your hardware.

ISDN Line Configuration	
Data Link Encapsulation...	Frame Relay

Enter information supplied to you by your ISDN phone company.

Follow the configuration instructions in the *User's Reference Guide* on your Netopia CD appropriate to your hardware. For example, for an SDSL router, you use the R7100 *User's Reference Guide*. For an ISDL router you use the R3100 *User's Reference Guide*.

Multilink PPP for Bonded IDSL and Leased ISDN Routers

DSL Bonding, also called inverse multiplexing or IMUX, technology combines the bandwidth of multiple DSL (Digital Subscriber Line) circuits into a single virtual data pipe.

Before DSL Bonding was developed, the maximum speed of a DSL connection was dependent on the customer's distance from the central office. DSL Bonding allows customers who are located at greater distances from the central office to aggregate DSL circuits, in order to achieve two or more times the speed otherwise available to them with a single line.

Netopia's Bonded IDSL and leased ISDN routers, which support up to four BRI circuits, allow customers who, because of line quality problems, were previously limited to a 144 Kbps IDSL connection, to enjoy speeds of up to 576 Kbps.

Many service providers require the capability of encapsulating PPP information via the bonded link, sometimes also requiring User Name and Password information to allow you to connect. Firmware version 4.7.1 offers Multilink PPP (MLPPP) support for the Netopia Bonded IDSL and leased ISDN routers, R3131 and R3232. This permits user authentication via PPP over the bonded WAN link. Firmware version 4.7.1 also interoperates with the Cisco and Redback routers.

By default, the system initiates MLPPP to its peer as long as the Data Link Encapsulation is set to PPP on the WAN and its associated connection profile. MLPPP is also supported in conjunction with RFC1973 (PPP over ISDN).

To use PPP over bonded IDSL or leased ISDN, first enable PPP as the Data Link Encapsulation method on the WAN link and MLPPP as the IMUX Mode. Next, create a corresponding Connection Profile. Finally, provide your authentication information in that Connection Profile.

This can be done in either:

- the series of Easy Setup console screens (see ["Easy Setup method" on page 11-7](#))
- or, for advanced users, who need more than one Connection Profile or additional features,
- in the WAN Configuration screens (see ["Advanced WAN Configuration method" on page 11-9](#))

Note: In the examples that follow, the configuration screens shown are for a Netopia R3232-I IDSL router. For other R-series router models, your screens may show variations appropriate to your specific model.

Multilink PPP Configuration

Easy Setup method

In the Easy Setup screens you first enable PPP on the WAN interface, using the ISDN Easy Setup screen, then enable MLPPP as the IMUX Mode, as follows:

From the Main Menu, select **Easy Setup** and press **Return**.

The **ISDN Easy Setup** screen appears (in this example, for the **IDSL, CMN** circuit type).

ISDN Easy Setup	
Circuit Type...	IDSL, CMN
Data Link Encapsulation...	PPP
IMUX Mode...	MLPPP
TO MAIN MENU	NEXT SCREEN
Enter information supplied to you by your ISDN phone company.	

- Select **PPP** from the **Data Link Encapsulation** pop-up menu, **MLPPP** from the **IMUX Mode** pop-up menu, and press **Return**.

Note: For Circuit Types that can support either DML or MLPPP, the IMUX Mode pop-up menu permits choosing between DML and MLPPP. This menu item is only visible when there are two ISDN WAN interface modules installed in the router, and then only if an appropriate circuit type is chosen. Also, the Data Link Encapsulation must be set to PPP or PPP over Frame Relay. For Circuit Types that do not support both DML and MLPPP, the IMUX Mode pop-up menu item does not appear because MLPPP is the only option, and will be enabled.

- Select **NEXT SCREEN** and press **Return**.

The **Easy Setup Profile** screen appears.

Connection Profile 1: Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

206.25.23.12

Local WAN IP Mask:

255.255.255.0

Remote IP Address:

127.0.0.2

Remote IP Mask:

255.255.255.255

PPP Authentication...

PAP

Send User Name:

michaelt

Send Password:

PREVIOUS SCREEN

NEXT SCREEN

Return/Enter takes you back to previous screen.

- From the **PPP Authentication** pop-up menu, select your authentication type: None, PAP, CHAP, PAP-TOKEN, or CACHE-TOKEN. The default is None. If you select any value other than None, the **Send User Name** and **Send Password** fields appear.
- Using the **Down** arrow key, select **Send User Name**. Type the user name that identifies you to your service provider. Press **Return**.
- Select **Send Password** and type the password that authenticates you to your service provider. Press **Return**.
- Select **NEXT SCREEN** and press **Return**. When you exit the Easy Setup profile screens, a Connection Profile is created that contains the information that you have entered.

If you need to change any of the other parameters in the Easy Setup screens, you can do so by accessing Easy Setup from the Main Menu. For more information on Easy Setup and Connection Profiles, see the respective sections in the on-line *User's Reference Guide* on your Netopia CD.

Advanced WAN Configuration method

In the WAN Configuration screens you first enable PPP on the WAN interface, using the Line Configuration screen, then add a PPP Connection Profile, using the Add Connection Profile screens, as follows:

From the Main Menu, select **WAN Configuration** then **WAN Setup** and press **Return**.

The **Choose Interface to Configure** screen appears.

```

Choose Interface to Configure

ISDN/IDSL (Wan Module 1 and 2) Setup...
Auxiliary Serial Port Setup...
Configuration Changes Reset WAN Connection:      Yes
  
```

Select **[WAN_Interface_Type] (Wan Module 1 and 2) Setup** and press **Return**.

The **Line Configuration** screen appears (in this example, the **ISDN Line Configuration** screen).

```

ISDN Line Configuration

Circuit Type...          IDSL, CMN

Data Link Encapsulation...  PPP

IMUX Mode...             MLPPP

Enter information supplied to you by your ISDN phone company.
  
```

- Select **PPP** from the **Data Link Encapsulation** pop-up menu, **MLPPP** from the **IMUX Mode** pop-up menu, and press **Return**.

Note: For Circuit Types that can support either DML or MLPPP, the IMUX Mode pop-up menu permits choosing between DML and MLPPP. This menu item is only visible when there are two ISDN WAN interface modules installed in the router, and then only if an appropriate circuit type is chosen. Also, the Data Link Encapsulation must be set to PPP or PPP over Frame Relay. For Circuit Types that do not support both DML and MLPPP, the IMUX Mode popup menu item does not appear because MLPPP is the only option, and will be enabled.

- Press **Escape** twice to return to the WAN Configuration screen. Select **Add Connection Profile** and press **Return**.

The **Add Connection Profile** screen appears.

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
IPX Enabled:	No
Interface Group...	Primary
<div style="display: flex; justify-content: space-around; width: 100%;"> ADD PROFILE NOW CANCEL </div>	

Configure a new Conn. Profile. Finished? ADD or CANCEL to exit.

- Select **PPP** from the **Data Link Encapsulation** pop-up menu, then select **Data Link Options** and press **Return**.

The **Datalink (PPP/MP) Options** screen appears.

Datalink (PPP/MP) Options

Data Compression...	Standard LZS
Send Authentication...	PAP
Send User Name:	michaelt
Send Password:	*****
Receive User Name:	
Receive Password:	
Maximum Packet Size:	1500

In this Screen you will configure the PPP/MP specific connection params.

- Select **Send User Name** and type the user name that identifies you to your service provider. Press **Return**.
- Select **Send Password** and type the password that authenticates you to your service provider. Press **Return**.
- Press **Escape** to return to the **Add Connection Profile** screen. Select **ADD PROFILE NOW** and press **Return**.

When you exit the screen, a Connection Profile is created that contains the information that you have entered. For more information on WAN Configuration and Connection Profiles, see the respective sections in the on-line *User's Reference Guide* on your Netopia CD.

Monitoring

Quick View

The **Quick View** screen now displays status of the Bonded DSL WAN interface.

```

                                Quick View                                11/5/1999 12:42:24 PM

Default IP Gateway:  0.0.0.0          CPU Load: 10%   Unused Memory: 228 KB
Domain Name Server:  0.0.0.0          WAN Interface Group -- ISDN/IDSL
Domain Name: None Provided

-----MAC Address-----IP Address-----IPX Address-----
Ethernet Hub: 00-00-c5-70-03-48  192.168.1.1
DSL Bond: 00-00-c5-70-03-4a  0.0.0.0

                                Current Frame Relay Status
--DLCIs In Use--Bytes Rx---Bytes Tx---Frames Rx---Frames Tx---FECNs+BECNs---
      0              0      0      0      0      0      0

VPN QuickView

                                LED Status
PWR+-----WAN1-----+---CON---AUX---+-----WAN2-----+---EN---+-----LEDS-----
   LNK RDY CH1 CH2   LNK  LNK   LNK RDY CH1 CH2  DATA | '-'= Off 'G'= Green
   G   -   R   -   -   Y   -   -   R   -   -   -   | 'R'= Red 'Y'= Yellow
```

System Information

The **System Information** screen now displays whether or not IMUX support is installed.

```

                                System Information

Serial Number              70-03-48 (7340872)
Firmware Version           4.6

Processor Speed (MHz)      33
Flash ROM Capacity (MBytes) 1
DRAM Capacity (MBytes)     4

Ethernet                   8 Port 10Base-T
Auxiliary Serial Port      Switched Async
WAN 1 Interface             CMN SDSL, fw v1.40.13
WAN 2 Interface             CMN SDSL, fw v1.40.13

AppleTalk Feature Set      Not Installed
Analog Dial-In Kit         Installed

IMUX Support               Installed
```

WAN Event History

The **WAN Event History** screen now displays events related to the multiple WAN links. The log reports the connection of each separate DSL link as DML-1, DML-2, DML-3, and DML-4.

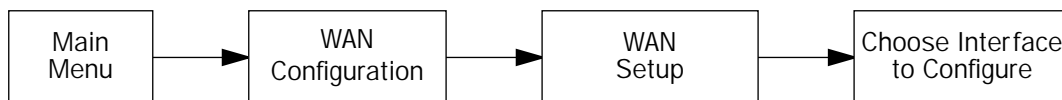
```

                                WAN Event History
                                Current Date -- 11/5/99
11:48:19 AM
-Date-----Time-----Event-----
-----SCROLL UP-----
11/04/99 17:46:21   RFC1483: IP up, channel 2, gateway: 163.176.107.1
11/04/99 17:46:17   RFC1483-2 rate set to 576 Kbps
11/04/99 17:46:17   DML-4 up
11/04/99 17:46:17   RFC1483-2 rate set to 432 Kbps
11/04/99 17:46:17   RFC1483-2 rate set to 432 Kbps
11/04/99 17:46:17   DML-3 up
11/04/99 17:46:17   DML-1 up
11/04/99 17:46:17   DML-2 up
11/04/99 17:46:15 >>WAN: Data link activated at 144 Kbps
11/04/99 17:46:15 >>WAN: Data link activated at 144 Kbps
11/04/99 17:46:15 >>WAN: Data link activated at 144 Kbps
11/04/99 17:46:15   RFC1483-2 rate set to 144 Kbps
11/04/99 17:46:15   RFC1483: Channel 2 up
11/04/99 17:46:15 >>WAN: Data link activated at 144 Kbps
-----SCROLL DOWN-----
Clear History...

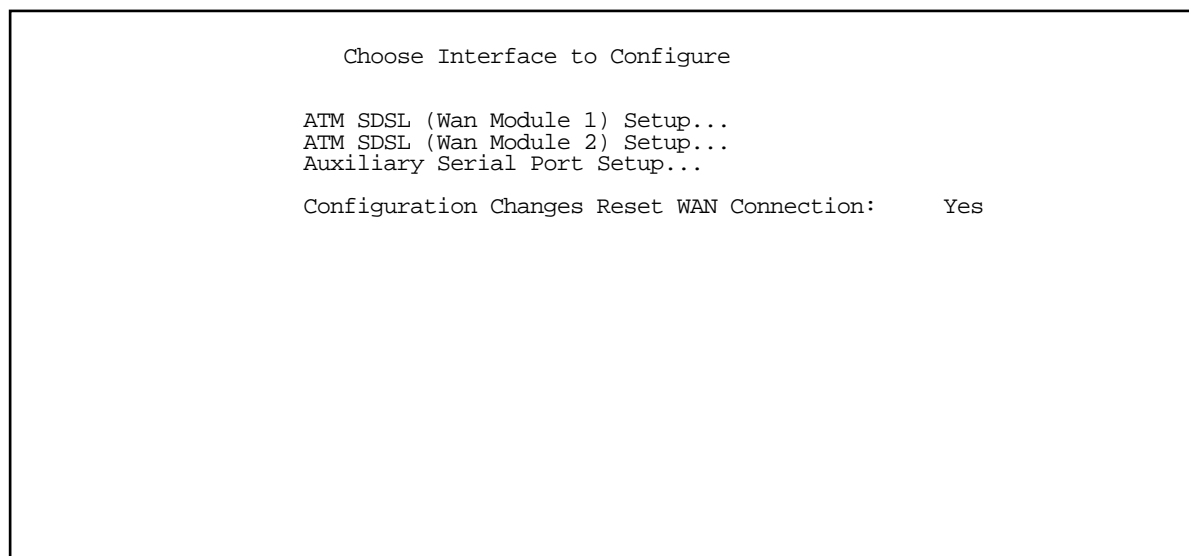
Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.
```

Multilink PPP-based DSL Bonding Support for ADSL and SDSL Routers

Introduced in version 4.8, the firmware offers Multilink PPP-based DSL Bonding support for R6161 ADSL and R7272 SDSL routers. R7171 routers gain Multilink PPP DSL Bonding support as well. This requires that PVCs be set on a per-WAN interface basis. You access this feature in the Choose Interface to Configure screen under the WAN Setup menu.



When there are two ADSL or SDSL WAN interface modules installed in the router, the Choose Interface to Configure screen changes to the following:



The second WAN module configuration screen, and the menu that takes you to it, are accessible when:

- both WAN modules are the same
- both WAN modules are capable of Multilink PPP
- both WAN modules make use of ATM PVCs.

This currently includes the R6161 and R7272.

When you select **ATM SDSL (Wan Module 2) Setup** above and press Return, the secondary WAN module screen appears.

SDSL Line 2 Configuration

Display/Change Circuit...
Add Circuit...
Delete Circuit...

Enter Information supplied to you by your telephone company.

This is because the only configuration that is allowed is the configuration of PVCs. See [“Multiple ATM Permanent Virtual Circuit Support” in Chapter 5](#) for more information.

Chapter 12

DSL and Leased Line Backup

The firmware offers dial backup functionality in the event of a line failure on a DSL, Ethernet, or leased-line primary WAN link. The firmware now supports backup to an external modem connected to the Auxiliary port or an internal V.90 modem via a V.90 modem WAN module or an ISDN interface via an ISDN WAN interface module in the second WAN slot.

This chapter covers the following topics:

- [WAN Configuration on page 12-3](#)
- [IP Setup screen on page 12-8](#)
- [Connection Profiles on page 12-9](#)
- [Using Scheduled Connections with Backup on page 12-9](#)
- [Management/Statistics on page 12-11](#)
- [QuickView on page 12-13](#)
- [Event Logs on page 12-13](#)
- [SNMP Support on page 12-13](#)
- [Backup Enhancements on page 12-14](#)

The purpose of line backup is to provide a recovery mechanism in the event that the primary connection fails. A failure can be either line loss, for example by central site switch failure or physical cable breakage, or in the case of Frame Relay (with LMI) or PPP, loss of end-to-end connectivity. Detection of one of these failures causes the router to switch from using the primary WAN port to using the auxiliary port to which a modem has been attached or to an internal asynchronous modem or ISDN WAN module if one is installed. The port used for backup is determined by whether or not a second WAN module is installed in the router. If there is only one WAN module installed then the Auxiliary port is the backup port. If an asynchronous modem or ISDN WAN module is installed in the second slot, then that is the backup port.

In the event of a loss of primary connectivity you have the option of switching back to the primary port automatically once it has recovered its connection.

The supported backup ports are the Auxiliary port or an asynchronous V.90 modem or ISDN WAN module in Switched Asynchronous mode with PPP as the data link encapsulation.

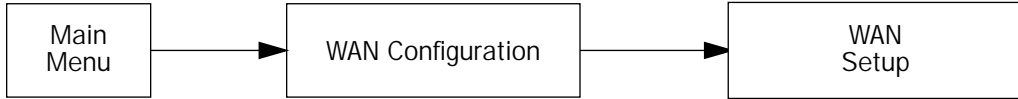
Leased line Backup supports the following Netopia R-Series Routers:

V.90 Backup	ISDN Backup
R3120 ISDN (leased mode) and R3120-I IDSL with V.90 backup **	–
R5120 Serial with V.90 backup **	R5131 SA with ISDN backup **
R5220 DDS with V.90 backup *	–
R5320 T-1 with V.90 backup *	R5331 T-1 with ISDN backup *
R7120 SDSL with V.90 backup *	R7131 SDSL with ISDN backup *
R7220 SDSL with V.90 backup *	R7231 SDSL with ISDN backup *
R9120 Ethernet with V.90 backup **	R9131 Ethernet with ISDN backup **
<p>* May be purchased as an assembled unit. ** Requires addition of an upgrade WAN module daughter card. You can upgrade a base-model router to dial backup, for example an R7100 to either an R7120 or R7131, by adding either of two upgrade kits which enable the addition of internal dial backup modules to current Netopia routers:</p>	
TER/20: V.90 WAN module	TER/31: ISDN WAN module

Note: Installation of the TER/20 V.90 WAN module in an R3100 router disables the switched ISDN capability on the primary WAN interface. The router can then be used only in leased ISDN mode. Also, you cannot install switched ISDN as a backup to an R3100 in leased line or IDSL mode.

WAN Configuration

To configure Line Backup, from the Main Menu select **WAN Configuration** and then **WAN Setup**.



```

                                WAN Configuration

WAN (Wide Area Network) Setup...

Display/Change Connection Profile...
Add Connection Profile...
Delete Connection Profile...

WAN Default Profile...
ATMP/PPTP Default Profile...
IKE Phase 1 Configuration...
Scheduled Connections...

Backup Configuration...

Frame Relay Configuration...
Frame Relay DLCI Configuration...

Establish WAN Connection...
Disconnect WAN Connection...

Return/Enter to create a new Connection Profile.
From here you will configure yours and the remote sites' WAN information.
```

The **Choose Interface to Configure** screen appears.

```

                                Choose Interface to Configure

CMN SDSL (Wan Module 1) Setup...
MODEM (Wan Module 2) Setup...
Auxiliary Serial Port Setup...
```

The router senses what type of WAN interface modules are installed in the WAN interface slots. For example, if you have an ISDN daughter card installed in slot 2, the screen will say **ISDN (Wan Module 2) Setup...**

Choose the interface you want to configure for backup, either **Motherboard Auxiliary Setup...** or **(Wan Module 2) Setup...**

- If you select **Motherboard Auxiliary Setup...**, the following screen appears:

Auxiliary Port Configuration

Aux Serial Port...	Async Modem
Data Rate (kbps)...	57.6
Aux Modem Init String:	AT&F&C1&D2E0S0=1
Aux Modem Directory Number:	

- Options for the **Aux Serial Port** are Async Modem or Unused.
- If you select **Async Modem**, you can select its **Data Rate** from a pop-up menu, edit the **Aux Modem Init String**, if necessary, and enter the **Aux Modem Directory Number** to dial to connect to your ISP.
- Press **Escape** twice to return to the **WAN Configuration** screen, and select **Backup Configuration** (shown on [page 12-7](#)).

- If you select **(Wan Module 2) Setup...** and have a V.90 modem card in slot 2, the following screen appears:

Internal Modem Setup

Modem Dialing Prefix:	ATDT
PBX Dialing Prefix:	
Answer on Ring Type...	Any
Speaker On...	Until Carrier
Speaker Volume...	2-Medium

Enter Information supplied to you by your telephone company.

- You can edit the **Modem Dialing Prefix**, if necessary, add a **PBX Dialing Prefix** (such as "9" for an outside line), set the conditions for whether the modem will **Answer on Ring Type** incoming calls, adjust the conditions for when the **Speaker** is **On**, and adjust the **Speaker Volume**, from the pop-up menus.
- The default **Modem Dialing Prefix** is ATDT. You can edit it if you need to.
- You can enter a PBX Dialing Prefix such as "9" if you are on a PBX or Centrex phone system and must dial a prefix for an outside line.
- You may choose to selectively answer inbound calls, based on a distinctive ring pattern, using **Answer on Ring Type...** This permits you to set up a party line configuration where a fax machine or other device shares the line, but uses a different telephone number and ring pattern. Supported options are:

Ring Type:	Description:
Any	(the default) any pattern
Ring A	2.0 sec ON, 4.0 sec OFF (normal North American ring pattern)
Ring B	0.8 sec ON, 0.4 sec OFF, 0.8 sec ON, 4.0 sec OFF
Ring C	0.4 sec ON, 0.2 sec OFF, 0.4 sec ON, 0.2 sec OFF, 0.8 sec ON, 4.0 sec OFF
Never	the line will not answer to any ring pattern

- You may choose when the Netopia R-Series Routers's modem connection tones are audible in the

Speaker On... field. Supported options are:

Selection:	Behavior:
Never	Turns off all speaker activity and hides the Speaker Volume control.
Until Carrier	The default. Allows call placement and handshaking tones to be heard.
During Answer	Same as above, but blocks dialing tones.
Always	Allows carrier tones to be heard, as well.

- When the modem speaker is on, you can adjust the volume in the **Speaker Volume...** field.
- Press **Escape** twice to return to the **WAN Configuration** screen, and select **Backup Configuration** (shown on [page 12-7](#)).
- If you select **(Wan Module 2) Setup...** and have an ISDN card in slot 2, the following screen appears:

ISDN Line Configuration

Switch Type...Auto-Detect

Directory Number 1:
SPID 1:
Directory Number 2:
SPID 2:

PBX Prefix:

Enter information supplied to you by your ISDN phone company.

The router will attempt to auto-detect all of your ISDN parameters. If it cannot do so, you can edit them manually in the **ISDN Line Configuration** screen. You can select the **Switch Type** that your ISP or corporate site uses from the pop-up menu. Enter your **Directory Number(s)** and **SPID(s)** as required, and a **PBX Prefix**, such as “9” for an outside line, if you need one.

Press **Escape** twice to return to the **WAN Configuration** screen, and select **Backup Configuration** (shown on [page 12-7](#)).

Backup Configuration screen

This screen is used to configure the conditions under which backup will occur, if it will recover, and how the Auxiliary port is configured.

For an internal V.90 modem or an external modem connected to the Auxiliary port, the Backup Configuration screen appears as follows (variations for ISDN are described below):

Backup Configuration

Backup Parameters	
Backup to Internal Modem...	Automatic
Requires Data Link Failure of...	2 Min
Ping Host Name or IP Address:	
Recovery to CMN SDSL...	Automatic
Requires Recovery of...	30 Sec
Auto-Recovery on loss of Layer 2:	No
Data Link Encapsulation is	Async PPP

Enter Information supplied to you by your telephone company.

- Select **Backup to Auxiliary Port**, **Backup to Internal Modem**, or **Backup to ISDN** and press Return. The system automatically senses whether you have an internal modem or ISDN card installed in the second slot. If you do not, this menu item will be Auxiliary Port; if you do, this item will be Internal Modem or ISDN. A pop-up menu allows you to select Disabled, Manual, or Automatic. You enable line backup by selecting either Manual or Automatic. If you enable backup, the subsequent menu items become visible.
- Select **Requires Data Link Failure of...** and press Return. A pop-up menu allows you to choose among 30 Sec(onds), 1 Min(ute), 2 Min(utes), 5 Min(utes), 10 Min(utes), or 15 Min(utes) to determine how long you want the system to wait before the backup port becomes enabled in the event of primary line failure. This allows you to be sure that the primary WAN connection is not merely briefly interrupted before the router switches to backup mode.
- Select **Ping Host Name or IP Address** and enter an IP address or resolvable DNS name that the router will ping. This is an optional item that is particularly useful for testing if the remote end of a VPN connection has gone down. Should this address become unreachable the router will treat this as a loss of connectivity and begin the backup timer. This loss is a Layer 2 loss.
- Select **Recovery to "WAN_name"** (where *WAN_name* is the type of WAN connection you have, e.g., SDSL) and press Return. Choose either Manual or Automatic to determine how the system will return to the primary WAN link when it becomes available again. If you choose Automatic, the next two menu items become visible.

Note: Automatic recovery only works upon loss of primary WAN connectivity.

- If you chose Automatic Recovery, select **Requires Recovery of...** and press Return. A pop-up menu

allows you to choose among 30 Sec(onds), 1 Min(ute), 2 Min(utes), 5 Min(utes), 10 Min(utes), or 15 Min(utes). This allows you to be sure that the primary WAN connection is well re-established before the router switches back to it from the backup mode.

- You can toggle **Auto-Recovery on loss of Layer 2** to Yes or No (the default). This setting determines whether the router should try to Auto-Recover when the backup is invoked because of a Layer 2 loss, for example, a no valid Connection Profile. (Layer 1 is still available, and this is what recovery checks.) Use this setting with caution. Setting it to Yes may induce alternating switching between Backup and Recovery Mode. This field will determine the recovery behavior of a Manual backup and Ping failure backup. These two failures are treated as Layer 2 failures.
- **Data Link Encapsulation** is set to Async PPP. This field is not editable.

IP Setup screen

The IP Setup screen now permits entry of a backup IP gateway address. This field is always visible, even if the **Default IP Gateway** field is not filled out, as in the case of a DHCP-acquired IP address and default gateway on the primary WAN interface.

IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP:	Both
Transmit RIP:	Off
Static Routes...	
IP Address Serving...	
Network Address Translation (NAT)...	
Filter Sets...	

Set up the basic IP attributes of your Netopia in this screen.

For more information on IP Setup see the *User's Reference Guide*.

Connection Profiles

The line backup feature allows you to configure a complete Connection Profile for the backup port, just as you do for your primary WAN connection. In this way profiles are associated with a particular interface. The profile should reflect the port it is associated with. It should have switched characteristics for the backup port.

Add Connection Profile

Profile Name:	Backup
Profile Enabled:	Yes
Data Link Encapsulation is	PPP
Data Link Options...	
IP Enabled:	Yes
IP Profile Parameters...	
IPX Enabled:	No
Interface Group...	Backup
Telco Options...	
<div style="display: flex; justify-content: space-around;"> ADD PROFILE NOW CANCEL </div>	

Return/Enter to discard changes you have made. Profile will not be added.
Configure a new Conn. Profile. Finished? ADD or CANCEL to exit.

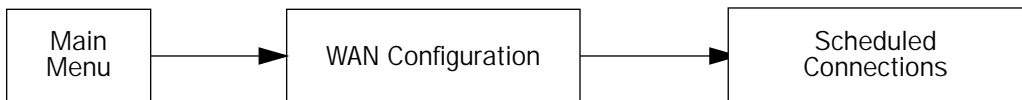
For instructions on creating a Connection Profile see the *User's Reference Guide*.

To associate this Connection Profile with your backup port interface, choose **Backup** from the Interface Port pop-up menu and press Return.

Using Scheduled Connections with Backup

The backup link is a PPP dial-up connection and only connects to the Internet service provider when traffic is initiated from the LAN. If you want to use the backup link to provide redundancy for services, such as a Web service that you provide to the outside world, you must force the connection to stay up. You do this by creating a scheduled connection entry that will be a permanent “forced up” connection for the backup port. The backup port will be activated upon primary WAN link failure and remain active until primary WAN link recovery.

To configure a Scheduled Connection, from the Main Menu select WAN Configuration and then Scheduled Connections.



The Scheduled Connections screen appears.

Scheduled Connections

Display/Change Scheduled Connection...

Add Scheduled Connection...

Delete Scheduled Connection...

Return/Enter to add a Scheduled Connection.
Navigate from here to add/modify/change/delete Scheduled Connections.

- Select **Add Scheduled Connection** and press Return. The Add Scheduled Connection screen appears.

Add Scheduled Connection

Scheduled Connection Enable: On

How Often... Weekly

Schedule Type... Forced Up

Set Weekly Schedule...

Use Connection Profile...

ADD SCHEDULED CONNECTION CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
Scheduled Connections dial remote Networks on a Weekly or Once-Only basis.

- Toggle **Scheduled Connection Enable** to **On**.
- From the **How Often** pop-up menu, select **Weekly** and press Return.
- From the **Schedule Type** pop-up menu, accept the default **Forced Up** and press Return.
- Select **Set Weekly Schedule**, and press Return. The Set Weekly Schedule screen appears.

Set Weekly Schedule

Monday:	Yes
Tuesday:	Yes
Wednesday:	Yes
Thursday:	Yes
Friday:	Yes
Saturday:	Yes
Sunday:	Yes
Scheduled Window Start Time:	11:27
AM or PM:	AM
Scheduled Window Duration Per Day: 24:00	

Return/Enter accepts * Tab toggles * ESC cancels.

- Toggle all the days of the week to **Yes**, and set the **Scheduled Window Duration Per Day** to **24:00**. This guarantees a 24X7 connection. Press Escape to return to the Add Scheduled Connection screen.
- Select **Use Connection Profile**, and press Return. A screen displays all of your Connection Profiles. Select the one you want to apply this scheduled connection to and press Return. Your selection becomes effective.

Now, if your primary WAN link fails, the backup link will become active and remain active until the primary link recovers.

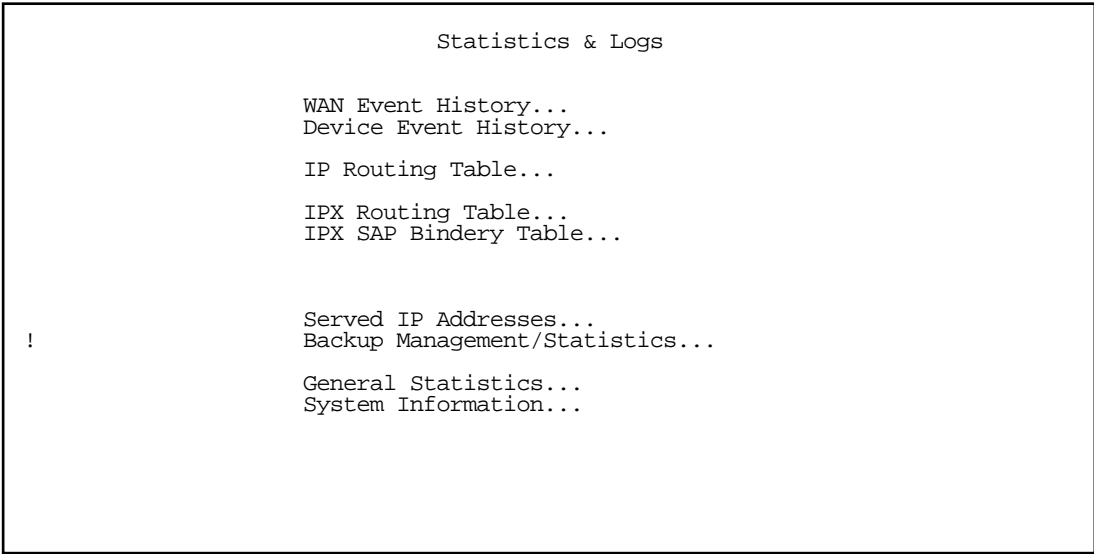
For more information on Scheduled Connections, see the *User's Reference Guide*.

Management/Statistics

The Statistics & Logs menu offers a Backup Management/Statistics option.

To view the Backup Management/Statistics, from the Main Menu select Statistics & Logs.

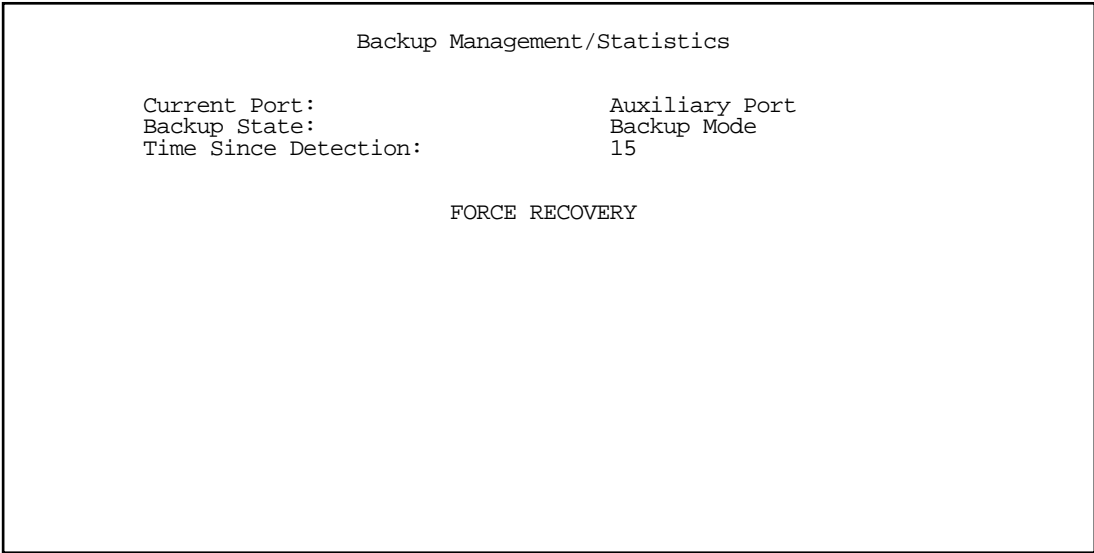




Select **Backup Management/Statistics** and press Return.

Note: This option is only visible if backup is not Disabled.

The Backup Management/Statistics screen appears.



- **Current Port** is a display-only field that shows which port is currently in operation.
- **Backup State** is a display-only field that shows the current state of Backup or Recovery.
- **Time Since Detection** is a display-only field that is only visible if backup or recovery is in progress. It displays the elapsed time since detection of either primary WAN line failure or re-establishment of the

connection.

- The **FORCE BACKUP/FORCE RECOVERY** option is a selectable option that, depending on the current state of backup, will force the switching of ports. If you are currently in backup mode, the option will be **FORCE RECOVERY**. If you are currently in normal WAN link mode, the option will be **FORCE BACKUP**. Selecting either one and pressing Return will force the link to switch to the other mode.

QuickView

QuickView now has an information element to indicate which port is in use.

```

                                Quick View
Default IP Gateway:  0.0.0.0      CPU Load: 4%      Unused Memory: 387 KB
Domain Name Server:  0.0.0.0      Current WAN Port: Auxiliary Port
Domain Name: happyinternet.com

```

Event Logs

When a backup or recovery occurs an event is logged in the WAN Event History.

```

                                WAN Event History
                                Current Date --  4/17/99 10:57:12 AM
-Date-----Time-----Event-----
                                SCROLL UP
04/17/99 10:39:37 * Line Failure: Switching to backup port
04/17/99 10:38:51 * Line Recovery: Switching to primary port
04/17/99 10:37:42 * Line Failure: Switching to backup port
04/17/99 10:35:53 --Device restarted-----
04/17/99 10:04:48 --Device restarted-----
04/17/99 10:04:13 --Device restarted-----
04/17/99 08:59:01 --Device restarted-----
04/14/99 09:12:09 --Device restarted-----
04/13/99 10:31:08 --Device restarted-----
04/13/99 09:47:57 >>WAN: SDSL 1 deactivated
04/13/99 09:47:56 >>WAN: SDSL 1 activated at 10000 Kbps
04/13/99 09:42:07 --Device restarted-----
04/13/99 09:29:45 --Device restarted-----
04/12/99 11:29:44 --Device restarted-----
                                SCROLL DOWN
Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.

```

SNMP Support

The router supports objects for determining the state of backup, as well as providing traps for the backup and recovery events. No objects support configuration of backup or recovery.

Backup Enhancements

Beginning with firmware version 4.8, Backup and Recovery timers now allow you to enter your own values in minutes. The value zero is not permitted for these fields. If you are upgrading from 4.7.x or earlier your previous settings will be preserved; however a value of 30 seconds is rounded up to 1 minute.

By setting **Clear Backup Call only if idle** to **Yes** you can access **Requires idle time of**. You enter this value in seconds. When in backup mode and the primary interface comes up, the router waits the specified time entered in the Recovery timer field. In earlier firmware versions, after this expires the router would normally switch back to the Primary interface (depending on various settings). Starting with firmware version 4.8, if you want a backup call to be cleared only when idle, the router will wait until the call has been idle for the time you specified. After this expires the router will tear down the call and switch to the Primary interface.

Note: Backup and Recovery have resolutions of five seconds. This is how often the router evaluates the state of the connections and makes decisions.

Chapter 13

IP Address Serving Enhancements

Overview

The current firmware includes enhancements to the Netopia Router's built-in DHCP IP address server. These enhancements include:

- The ability to exclude one or more IP addresses from the address serving pool so the addresses will not be served to clients.
- The ability to reserve a particular IP address for a client with a particular Ethernet MAC address.
- The ability to view the host name associated with a client to which the router has leased an IP address.
- The ability for the router's Ethernet IP address(es) to overlap the DHCP address serving pool(s).
- The ability to serve as a DHCP Relay Agent.

Beginning with version 4.6, the firmware supports reserving an IP address only for a type 1 client identifier (i.e., an Ethernet hardware address). It does not support reserving an IP address for an arbitrary client identifier. (For more information on client identifiers, see RFC 2131, section 9.14.)

Configuring the IP Address Server

To access the enhanced DHCP server functions, from the Main Menu navigate to **Statistics & Logs** and then **Served IP Addresses**.



The following example shows the Served IP Addresses screen after three clients have leased IP addresses. The first client did not provide a Host Name in its DHCP messages; the second and third clients did.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103	DHCP	00:59	EN: 00-00-C5-70-00-04
192.168.1.104	DHCP	00:59	Bill's Pentium
192.168.1.105	DHCP	00:45	Steve's Power Mac
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

Beginning with the version 4.5 firmware release, the rightmost column displays the host name supplied by the client if one was provided; otherwise it displays the client identifier. (If a host name is displayed, the client identifier is still accessible in a Details pop-up menu. See below.)

Note: The server does not query the client for its host name. Macintosh computers running versions of MacOS prior to MacOS version 8.5 (OT 2.0.1, TCP/IP 2.0.1) do not supply a host name option in their DHCP messages, so no host name will appear in the Served IP Addresses list.

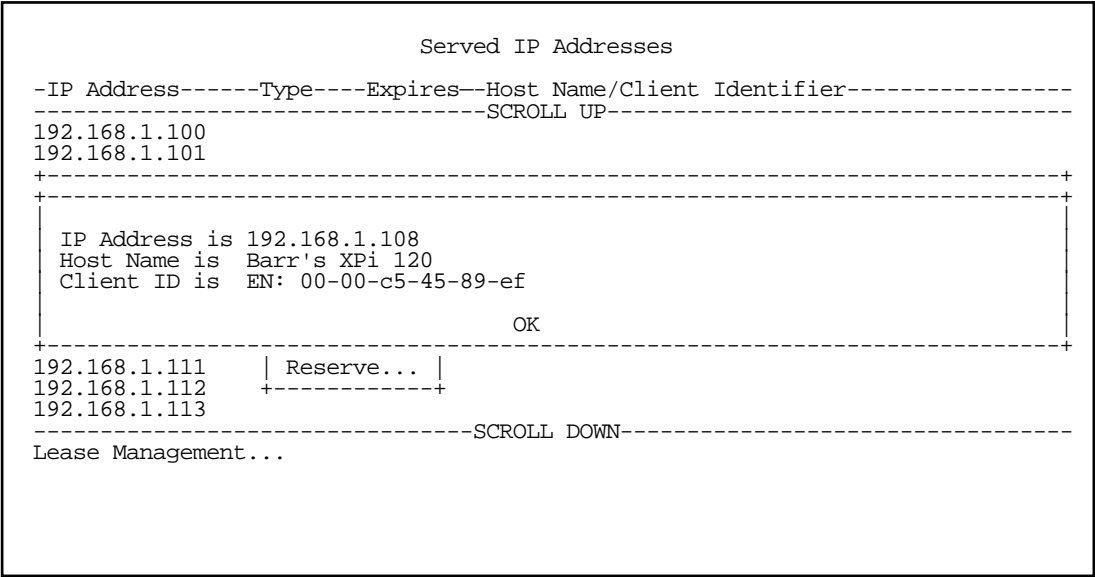
You can select the entries in the Served IP Addresses screen. Use the up- and down-arrow keys to move the selection to one of the entries in the list of served IP addresses. (You cannot select IP addresses in the MacIP static range, as well as the router's Ethernet IP address(es) that have been automatically excluded on startup, since you cannot perform any operations on these addresses.)

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

Once you select an entry, pressing Return displays an action pop-up menu that lists operations that can be performed on that entry. Possible operations are: **Details...**, **Exclude**, **Include**, **Release**, and **Reserve...** The action popup is context-sensitive, and lists only those operations that apply to the selected IP address in its current lease state.

- **Details...** is displayed if the entry is associated with both a host name and a client identifier.

Selecting **Details...** displays a pop-up menu that provides additional information associated with the IP address. The pop-up menu includes the IP address as well as the host name and client identifier supplied by the client to which the address is leased.



- **Exclude** is displayed if the entry is not already excluded.

Selecting **Exclude** excludes the IP address from the address serving pool so the address will not be served to a client. If the IP address is currently leased to or reserved for a client, you will be presented with a warning dialog asking you to confirm the operation.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.1+	-----+-----		
192.1+	-----+-----		
192.1	You are about to make changes that will affect an address		
192.1	that is currently in use. Are you sure you want to do this?		
192.1			
192.1	CANCEL		OK
192.1	-----+-----		
192.1+	-----+-----		
192.168.1.111	Reserve...		
192.168.1.112	+-----+		
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

- **Include** is displayed if the entry is either excluded or declined.

An IP address is marked declined when a client to whom the DHCP server offers the address declines the address. A client declines an address if it determines that a leased address is already in use by another device.

Selecting **Include** restores the selected IP address to the address serving pool so that the IP address is once again eligible to be served to a client.

- **Release** is displayed if the entry is currently offered, leased, or reserved.

Selecting **Release** puts the selected entry in the available state. You will be presented with a warning dialog asking you to confirm the operation since the IP address is in use. There is no mechanism to notify the client to whom the address is leased that the lease has been terminated. Thus, the client will continue to use the address until the next time it attempts to renew its lease. In the interim, the server may lease the same IP address to a different client, thereby creating an address conflict. For this reason, releasing an address that is actively being used by a client is generally not recommended.

- **Reserve...** is displayed if the entry is available, declined, excluded, leased, offered, or reserved.

Reserving an IP address for a client with a particular Ethernet MAC address guarantees that a client with the specified MAC address will be offered or leased the specified IP address. Moreover, it prevents the specified IP address from being offered or leased to any other client.

Selecting **Reserve...** displays a pop-up dialog box that displays the IP address and editable item in which you can enter an Ethernet MAC address. The pop-up dialog box includes **OK** and **CANCEL** buttons for confirming or cancelling the operation. If the IP address is currently offered or leased to, or reserved for, a client, you will be presented with a warning dialog asking you to confirm the operation. Reserving an IP address guarantees that the IP address will only be leased.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

The router's Ethernet IP address(es) will be automatically excluded from the address serving pool(s) on startup. Entries in the served IP address list corresponding to the router's Ethernet IP address(es) that have been automatically excluded on startup are not selectable.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.1	Excluded for the router's IP address		
192.168.1.2	Excluded		
192.168.1.3	DHCP	00:24	Barr's XPi 120
192.168.1.4			
192.168.1.5			
192.168.1.6			
192.168.1.7			
192.168.1.8			
192.168.1.9			
192.168.1.10			
192.168.1.11			
192.168.1.12			
192.168.1.13			
192.168.1.14			
-----SCROLL DOWN-----			
Lease Management...			
Hit RETURN/ENTER for available operations.			

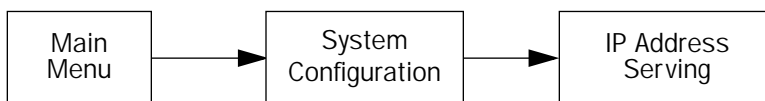
DHCP Relay Agent

Introduced in version 4.4, the firmware now offers DHCP Relay Agent functionality, as defined in RFC1542. A DHCP relay agent is a computer system or a router that is configured to forward DHCP requests from clients on the LAN to a remote DHCP server, and to pass the replies back to the requesting client systems.

When a DHCP client starts up, it has no IP address, nor does it know the IP address of a DHCP server. Therefore, it uses an IP broadcast to communicate with one or more DHCP servers. These broadcasts are normally limited to the network segment on which the client is located, and do not pass through routers such as the Netopia Router. If the Netopia Router is configured to act as a DHCP server, it will assign the client an address from an address pool configured locally in the Netopia Router and respond to the client's request itself.

However, if the Netopia Router is configured to act as a DHCP relay agent, it does not satisfy the DHCP request itself, but instead forwards the request to one or more remote DHCP servers. These servers process the request, assign an address from an address pool configured on the remote server, and forward the response back to the Netopia Router for delivery back to the client. The agent then sends the response to the client on behalf of the DHCP server. This process is transparent to the client, which doesn't know that it is communicating through an intermediary rather than directly to a local server. Using DHCP relay, it is possible to centralize the configuration information for the host computers at many remote sites at single location, easing the burden of administering configuration management for remote sites.

To configure the Netopia Router to act as a DHCP relay agent, from the Main Menu navigate to the System Configuration menu.



13-8 Firmware Version 4.10 Addendum

Select **IP Address Serving** and press Return. The IP Address Serving screen appears.

```

                                IP Address Serving
                                +-----+
                                |         |
IP Address Serving Mode...    | Disabled |
                                | DHCP Server |
Number of Client IP Addresses: | DHCP Relay Agent |
1st Client Address:           |         |
Client Default Gateway...     | 192.168.1.1 |
                                +-----+

Serve DHCP Clients:           Yes
DHCP NetBIOS Options...

Serve BOOTP Clients:          Yes

```

Select **IP Address Serving Mode**. The pop-up menu offers the choices of Disabled, DHCP Server (the default), and DHCP Relay Agent.

If you select **DHCP Relay Agent** and press Return, the screen changes as shown below.

```

                                IP Address Serving

IP Address Serving Mode...    DHCP Relay Agent

Relay Server #1:              10.1.1.1
Relay Server #2:              20.1.1.1
Relay Server #3:              30.1.1.1

Configure Address Serving (DHCP, BOOTP, etc.) here.

```

Now you can enter the IP address(es) of your remote DHCP server(s), such as might be located in your company's corporate headquarters. Each time you enter an IP address and press Return, an additional field appears. You can enter up to four DHCP server addresses.

In the example above, DHCP requests from clients on the LAN will be relayed to the DHCP servers at IP addresses 10.1.1.1, 20.1.1.1, and 30.1.1.1.

Notes: The remote DHCP server(s) to which the Netopia Router is relaying DHCP requests must be capable of servicing relayed requests. Not all DHCP servers support this feature. For example, the DHCP server in the Netopia Router does *not*.

The DHCP server(s) to which the Netopia Router is relaying DHCP requests must be configured with one or more address pools that are within the Netopia Router's primary Ethernet LAN subnet. (There is no mechanism for DHCP clients to receive an address on a secondary subnet via a relayed DHCP request.)

Chapter 14

Virtual Private Networks (VPNs)

Introduced in version 4.6, the firmware offers both PPTP and ATMP tunneling support for Virtual Private Networks (VPN).

The version 4.8 firmware adds IPsec support. See [“Internet Key Exchange \(IKE\) IPsec Key Management” on page 15-1](#) for more information.

The following topics are covered in this chapter:

- [“Overview” on page 14-1](#)
- [“About PPTP Tunnels” on page 14-4](#)
- [“PPTP Tunnel Configuration for Windows NT” on page 14-7](#)
- [“Encryption Support” on page 14-8](#)
- [“VPN Default Answer Profile” on page 14-10](#)
- [“VPN QuickView” on page 14-11](#)
- [“Dial-Up Networking for VPN” on page 14-12](#)
- [“Installing the VPN Client” on page 14-16](#)
- [“About ATMP Tunnels” on page 14-18](#)
- [“Allowing VPNs through a Firewall” on page 14-22](#)
- [“Windows Networking Broadcasts” on page 14-28](#)

Overview

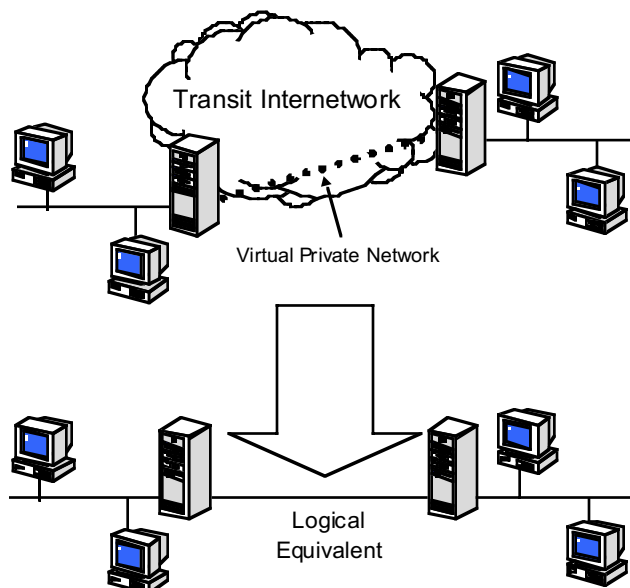
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation, and exchange information about the happenings on opposite sides of the state, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with Netopia Routers running the version 4.7.1 firmware, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

The Netopia Router can be used in VPNs either to initiate the connection or to answer it. When used in this way, the routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look "virtually" like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Two such protocols are in common use for tunnelling, Point-to-Point Tunnelling Protocol (PPTP) and Ascend Tunnel Management Protocol (ATMP). The Netopia Router can use either one.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia's PPTP implementation is compatible with Microsoft's and can function as either the client (PAC) or the server (PNS). As a client, a Netopia R-series router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia R-series router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see ["Dial-Up Networking for VPN" on page 14-12](#)) utility built into Windows 95, 98, or NT, no additional client software is required.
- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend routers. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE)

protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Netopia Router is called a *PPTP Access Concentrator (PAC)*, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia Router is called a *PPTP Network Server (PNS)*, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia Router wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

Configuring the Netopia Router for use with either of the two protocols is done through the console-based menu screens. Each type is described in its own section:

- [“About PPTP Tunnels” on page 14-4](#)
- [“About ATMP Tunnels” on page 14-18](#)

Your configuration depends on which protocol you (and the router at the other end of your tunnel) will use, and whether or not you will be using the VPN client software in a standalone remote connection.

Note: You must choose which protocol you will be using, since you cannot both export PPTP and use ATMP, or vice versa, at the same time.

Having both an ATMP tunnel and a PPTP export is not possible because functions require GRE and the router's PPTP export/server does not distinguish the GRE packets it forwards. Since it processes all of them, ATMP tunneling is impaired. For example, you cannot run an ATMP tunnel between two routers and also have PPTP exported on one side.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia Router) can exchange data with remote networks that are also connected to a VPN-capable router.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers. The feature is built around two key technologies: PPTP and ATMP.

About PPTP Tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

PPTP configuration

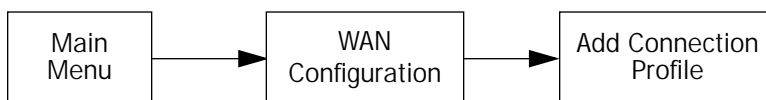
To set up the router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See [“VPN Default Answer Profile” on page 14-10](#) for more information.

PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation. See the *User’s Reference Guide* for information on creating Connection Profiles.

Note: As of firmware version 4.4, the R9100 Ethernet-to-Ethernet Router now has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed you cannot use PPP as a datalink encapsulation, and you will have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.



Add Connection Profile	
Profile Name:	Profile 2
Profile Enabled:	+-----+
Data Link Encapsulation...	+-----+
Data Link Options...	PPP
	Frame Relay
	ATM FUNI
	ATMP
	PPTP
	+-----+
IP Enabled:	
IP Profile Parameters...	
ADD PROFILE NOW	CANCEL

When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.

PPTP Tunnel Options	
PPTP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Data Compression...	None
Authentication...	CHAP
Send Host name:	tony
Send Secret:	*****
Receive Host name:	kimba
Receive Secret:	*****
Initiate Connections:	Yes
On Demand:	Yes
Idle Timeout (seconds):	300
Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.	
In this Screen you will configure the GRE/PPTP specific connection params.	

Note: Profiles using PPTP do not offer a Telco Options screen.

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.

If you do not specify the PPTP Partner IP Address the gateway cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).

- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the gateway partner is reached.

If you do not specify the PPTP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.

- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.

Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.

- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.
- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not itself a compression protocol.

Note: The version 4.6 firmware supports 128-bit ("strong") encryption. Unlike MS-CHAP version 1, which supports one-way authentication, MS-CHAP version 2 supports mutual authentication between connected routers and is incompatible with MS-CHAP version 1 (MS-CHAP-V1). When you choose MS-CHAP as the authentication method for the PPTP tunnel, the Netopia router will start negotiating MS-CHAP-V2. If the router you are connecting to does not support MS-CHAP-V2, it will fall back to MS-CHAP-V1, or, if the router you are connecting to does not support MPPE at all, the PPP session will be dropped.

- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Secret** (the CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Secret**, used for authenticating the remote PPTP client.
- You can specify that this router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established via the call management screens or may be scheduled using the scheduled connections feature. See "Scheduled Connections" in the *User's Reference Guide*.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is

torn down, use of the Idle Timeout is strongly encouraged.

An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile. The method works the same way as creating a forced up scheduled connection for the line backup feature. See [“Using Scheduled Connections with Backup” on page 12-9](#).

- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
Receive RIP:	Both

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a PAC has NAT applied to a Connection Profile set for PPTP data link encapsulation, the PNS and devices behind it, cannot Ping the PAC’s tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

PPTP Tunnel Configuration for Windows NT

Some networks that use Microsoft Windows NT PPTP Network Servers require additional authentication information, called *Windows NT Domain Name*, when answering PPTP tunnel connection requests. Not all Windows NT installations require this information, since not all such installations use this authentication feature. The Windows NT Domain Name is not the same as the Internet domain name, but is the name of a group of servers that share common security policy and user account databases. Your PPTP tunnel partner’s administrator will supply this Windows NT Domain Name if it is required.

When you create your Connection Profile for a PPTP tunnel, the PPTP Tunnel Options menu now offers an **Optional Windows NT Domain Name** field as shown below.

PPTP Tunnel Options

PPTP Partner IP Address:	173.167.8.134
Authentication...	PAP
Data Compression...	None
Send Host Name:	
Send Password:	
Receive Host Name:	
Receive Password:	
Initiate Connections:	Yes
On Demand:	Yes
Optional Windows NT Domain Name:	
Idle Timeout (seconds):	300

In this Screen you will configure the GRE/PPTP specific connection params.

If you configure your Netopia equipment to initiate PPTP tunnel connections by toggling **Initiate Connections** to **Yes**, the **Optional Windows NT Domain Name** field appears. Enter the domain name your network administrator has supplied.

Encryption Support

Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

Netopia's ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia routers. The encryption option, none or DES, is a selectable option in the ATMP Tunnel Options screen.

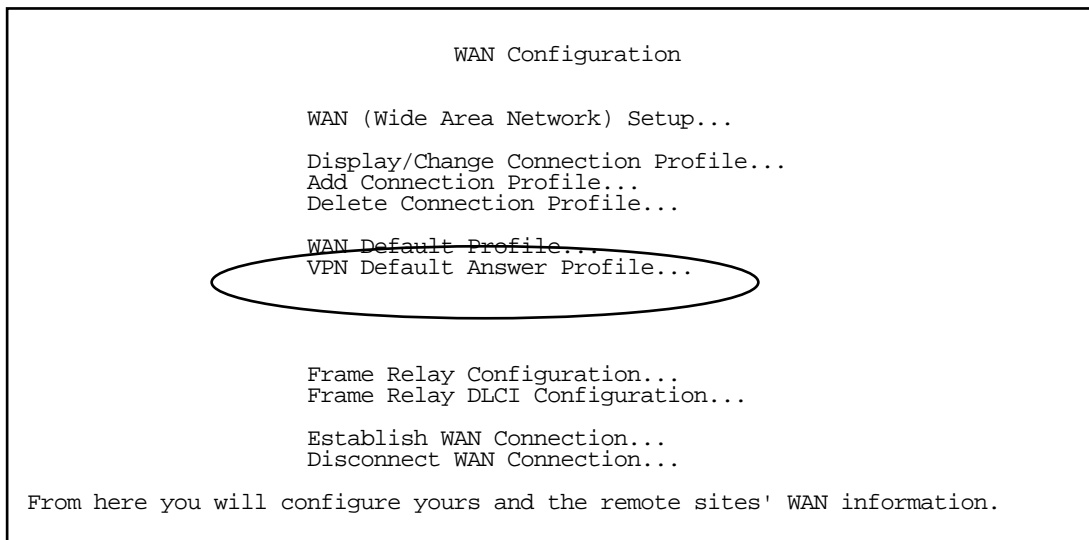
MS-CHAP V2 and 128-bit strong encryption

Notes:

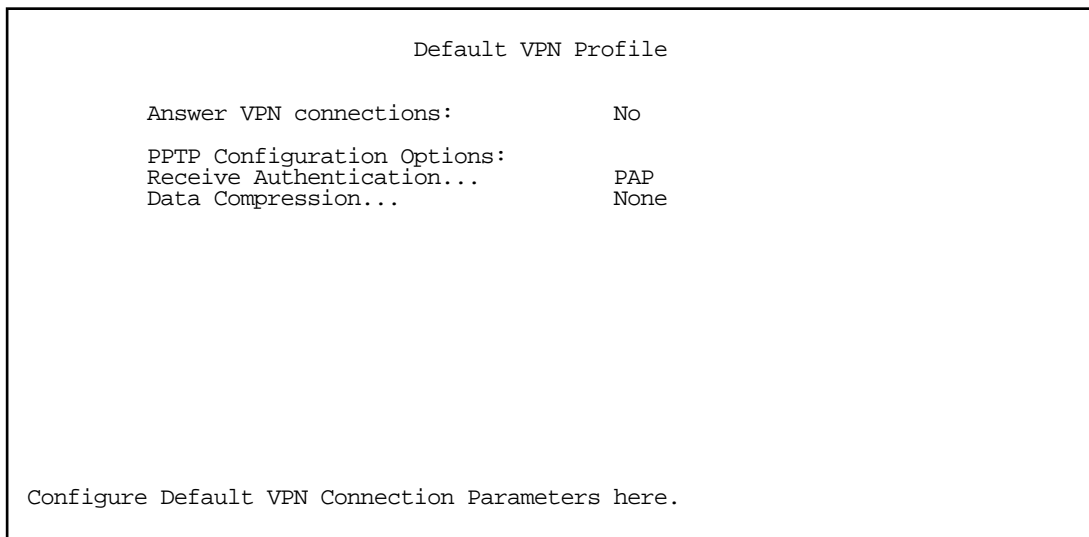
- Beginning with firmware version 4.6, the Netopia Router supports 128-bit (“strong”) encryption.
US encryption regulations changed mid-February, 2000 making it possible to include this new encryption feature as a standard part of the firmware. This means that all R-Series models (worldwide) that support VPN also support 128-bit encryption for free, when using PPTP tunnels.
ATMP does not have an option of using 128-bit MPPE. If you are using ATMP between two Netopia routers you can optionally set 56-bit DES encryption.
- When you choose MS-CHAP as the authentication method for a PPTP tunnel, the Netopia router will start negotiating MS-CHAPv2. If the router or VPN adapter client you are connecting to does not support MS-CHAPv2, the Netopia router will fall back to MS-CHAPv1, or, if the router or VPN adapter client you are connecting to does not support MPPE at all, the PPP session will be dropped. This is done automatically and transparently.

VPN Default Answer Profile

The WAN Configuration menu offers a VPN Default Answer Profile option. Use this selection when your router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The VPN Default Answer Profile determines the way the attempted tunnel connection is answered.



To set the parameters under which the router will answer attempted VPN connections, select **VPN Default Answer Profile** and press Return. The Default VPN Profile screen appears.



- Toggle **Answer VPN Connections** to **Yes** if you want the router to accept VPN connections or **No** (the

default) if you do not. This applies to both ATMP and PPTP connections.

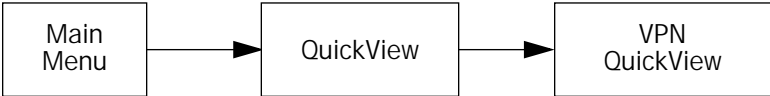
- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.



The VPN QuickView screen appears.

VPN Quick View						
Profile Name-----	Type--	Rx Pckts--	Tx Pckts--	Est.-	Partner	Address-----
HA <-> FA1 (Jony Fon	ATMP	99	99	Rmt	173.166.82.8	
HA <-> FA3 (Sleve M.	ATMP	13	14	Rmt	63.193.117.91	

Profile Name: Lists the name of the Connection Profile being used, if any.

Type: Shows the data link encapsulation method (PPTP or ATMP).

Rx Pckts: Shows the number of packets received via the VPN tunnel.

Tx Pckts: Shows the number of packets transmitted via the VPN tunnel.

Est: Indicates whether the connection was locally ("Lcl") or remotely ("Rmt") established.

Partner Address: Shows the tunnel partner's IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote standalone workstation to establish a VPN tunnel to a PPTP server such as a Netopia Router located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia Router initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia router.

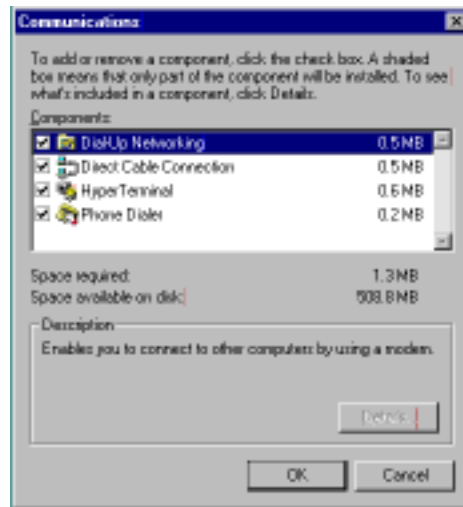
Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at <http://www.netopia.com> and, for the latest software and release notes, the Microsoft website at <http://www.microsoft.com>.

Installing Dial-Up Networking

Check to see if Dial-Up Networking is already installed on your PC. Open your My Computer (or whatever you have named it) icon on your desktop. If there is a folder named Dial-Up Networking, you don't have to install it. If there is no such folder, you must install it from your system disks or CDROM. Do the following:

1. From the **Start** menu, select **Settings** and then **Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.
The Add/Remove Programs Properties window appears.
3. Click the **Windows Setup** tab.
4. Double-click **Communications**.

The Communications window appears.



5. In the Communications window, select **Dial-Up Networking** and click the **OK** button.
This returns you to the Windows Setup screen. Click the **OK** button.
6. Respond to the prompts to install Dial-Up Networking from the system disks or CDROM.
7. When prompted, reboot your PC.

Creating a new Dial-Up Networking profile

A Dial-Up Networking profile is like an address book entry that contains the information and parameters you need for a secure private connection. You can create this profile by using either the Internet Connection Wizard or the Make New Connection feature of Dial-Up Networking. The following instructions tell you how to create the profile with the Make New Connection feature. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.
Open the Dial-Up Networking folder, and then double-click **Make New Connection**. The Make New Connection wizard window appears.
2. Type a name for this connection (such as the name of your company, or the computer you are dialing into).
From the pull-down menu, select the device you intend to use for the virtual private network connection. This can be any device you have installed or connected to your PC. Click the **Next** button. A screen appears with fields for you to enter telephone numbers for the computer you want to connect to.
3. Type the directory number or the **Virtual Circuit Identifier** number.
This number is provided by your ISP or corporate administrator. Depending on the type of device you are using, the number may or may not resemble an ordinary telephone directory number.
4. Click the **Next** button.
The final window will give you a chance to accept or change the name you have entered for this profile. If you are satisfied with it, click the **Finish** button. Your profile is complete.

Configuring a Dial-Up Networking profile

Once you have created your Dial-Up Networking profile, you configure it for TCP/IP networking to allow you to connect to the Internet through your Internet connection device. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.
Open the Dial-Up Networking folder. You will see the icon for the profile you created in the previous section.
2. Right-click the icon and from the pop-up menu select **Properties**.
3. In the Properties window click the **Server Type** button.

From the Type of Dial-up Server pull-down menu select the appropriate type of server for your system version:

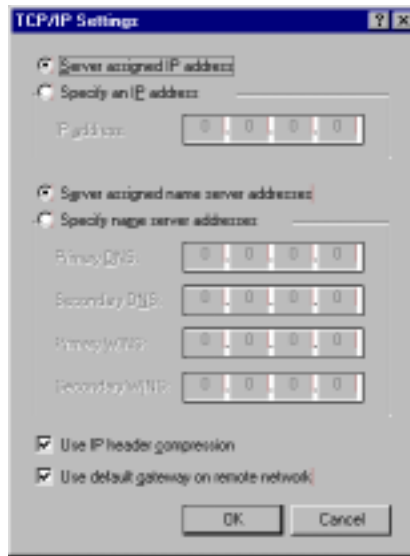


- Windows 95 users select **PPP: Windows 95, Windows NT 3.5, Internet**
- Windows 98 users select **PPP: Windows 98, Windows NT Server, Internet**

In the Allowed network protocols area check **TCP/IP** and uncheck all of the other checkboxes.

Note: Netopia's PPTP implementation does not currently support tunnelling of IPX and NetBEUI protocols.

4. Click the **TCP/IP Settings** button.



- If your ISP uses dynamic IP addressing (DHCP), select the Server assigned IP address radio button.
 - If your ISP uses static IP addressing, select the Specify an IP address radio button and enter your assigned IP address in the fields provided. Also enter the IP address in the Primary and Secondary DNS fields.
5. Click the **OK** button in this window and the next two windows.

Installing the VPN Client

Before Installing the VPN Client you must have TCP/IP installed and have an established Internet connection.

Windows 95 VPN installation

1. From your Internet browser navigate to the following URL:
<http://www.microsoft.com/NTServer/nts/downloads/recommended/dunl3win95/releasenotes.aso>
Download the Microsoft Windows 95 VPN patch dun 1.3 to the Windows 95 computer you intend to use as a VPN client with PPTP. Follow the installation instructions.
2. From the Windows 95 **Start** menu select **Settings**, then **Control Panel** and click once.
The Control Panel screen appears.
3. Double-click **Add/Remove Programs**.
The Add/Remove Programs screen appears.
4. Click the **Windows Setup** tab.
The Windows Setup screen will be displayed within the top center box.
5. Highlight **Communications** and double-click.
This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.
6. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.
7. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.
8. Double-click the **My Computer** icon (normally at the left upper corner of the screen).
This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.
9. Double click **Make New Connection**.
This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.
Click the **Next** button at the bottom of the screen
This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Windows 98 VPN installation

1. From the Windows 98 **Start** menu select **Settings**, then **Control Panel** and click once.
The Control Panel screen appears.
2. Double-click **Add/Remove Programs**.
The Add/Remove Programs screen appears.

3. Click the **Windows Setup** tab.

The Windows Setup screen will be displayed within the top center box.

4. Double-click **Communications**.

This displays a list of possible selections for the communications option. Active components will have a check in the checkboxes to their left.

5. Check **Dial Up Networking** at the top of the list and **Virtual Private Networking** at the bottom of the list.

6. Click **OK** at the bottom right on each screen until you return to the Control Panel. Close the Control Panel by clicking the upper right corner X.

7. Double-click the **My Computer** icon (normally at the left upper corner of the screen).

This will display the devices within My Computer. Scroll down the list to **Dial-Up Networking** and double-click it.

8. Double click **Make New Connection**.

This displays the Make New Connection installation screen. In this screen you will see a box labelled **Select a device**. From the pull-down menu to the right, select **Microsoft VPN Adapter**.

Click the **Next** button at the bottom of the screen

This displays the **VPN Host** screen. In the box to the top center of the screen enter your VPN server's IP address (for example, 192.168.xxx.xxx. This is not a proper Internet address)

Connecting using Dial-Up Networking

A Dial-Up Networking connection will be automatically launched whenever you run a TCP/IP application, such as a web browser or email client. When you first run the application a Connect To dialog box appears in which you enter your User name and Password. If you check the Save password checkbox, the system will remember your User name and Password, and you won't be prompted for them again.

About ATMP Tunnels

To set up an ATMP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote ATMP partner. ATMP uses the terminology of a *foreign agent* that initiates tunnels and a *home agent* that terminates them. You use the same procedure to initiate or terminate an ATMP tunnel. Used in this way, the terms *initiate* and *terminate* mean the beginning and end of the tunnel; they do not mean *activate* and *deactivate*.

ATMP is a tunneling protocol, with two basic aspects. Tunnels are created and torn down using a session protocol that is UDP-based. User (or client) data is transferred across the tunnel by encapsulating the client data within Generic Routing Encapsulation (GRE). The GRE data is then routed using standard methods.

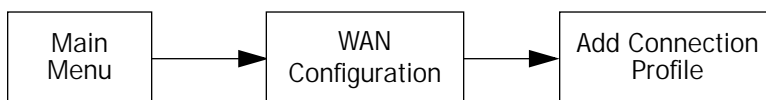
ATMP configuration

ATMP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, since ATMP is not a native encapsulation. The Easy Setup Profile does not offer ATMP datalink encapsulation. See the *User's Reference Guide* for information on creating Connection Profiles.

Note: The R9100 Ethernet-to-Ethernet Router now has access to Connection Profiles for tunnelling purposes. If the PPP dialup kit is not installed you cannot use PPP as a datalink encapsulation, and have access only to ATMP and PPTP. If the kit is installed you also have access to PPP.

The WAN Event History screens will report VPN tunnel events, such as connections and disconnections, as Channel 4 (and higher) events.

To define an ATMP tunnel, navigate to the **Add Connection Profile** menu from the Main Menu.



Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	+-----+
Data Link Encapsulation...	+-----+
Data Link Options...	PPP
	Frame Relay
	ATM FUNI
IP Enabled:	ATMP
IP Profile Parameters...	PPTP
	+-----+

ADD PROFILE NOW

CANCEL

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.

ATMP Tunnel Options

ATMP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Network Name:	sam.net
Password:	****
Data Encryption...	DES
Key String:	
Initiate Connections:	Yes
On Demand:	Yes
Idle Timeout (seconds):	300

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
In this Screen you will configure the GRE/ATMP specific connection params.

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

Note: Profiles using ATMP do not offer a Telco Options screen.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the gateway can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel

requests as a home agent.

- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the gateway partner is reached. If you do not specify the ATMP Partner IP Address, the router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- You can specify a **Network Name**. When the tunnel partner is another Netopia router, this name may be used to match against a Connection Profile. When the partner is an Ascend router in Gateway mode, then **Network Name** is used by the Ascend router to match a gateway profile. When the partner is an Ascend router in Router mode, leave this field blank.

- You must specify a **Password**, used for authenticating the tunnel.

Note: The Password entry will be the same for both ends of the tunnel.

- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.

Note: Ascend does not support DES encryption for ATMP tunnels.

- You must specify an 8-byte **Key String** when DES is selected. When encryption is None, this field is invisible.
- You can specify that this router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.

An alternate way to force a tunnel to stay up is to define a forced up scheduled connection for the profile. The method works the same way as creating a forced up scheduled connection for the line backup feature. See [“Using Scheduled Connections with Backup” on page 12-9](#).

- Return to the Connection Profile screen by pressing Escape.

- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
Receive RIP:	Both

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Note: A peculiarity associated with VPNs is that when a foreign agent has NAT applied to a Connection Profile set for ATMP data link encapsulation, the home agent and devices behind it, cannot Ping the foreign agent's tunnel end-point IP address. This is because ICMP packets have no port association, and thus will be discarded rather than being processed by NAT.

Ordinarily, Ping is an excellent troubleshooting tool, but it will not be effective in this circumstance. Instead, use another TCP- or UDP-based network service for troubleshooting. Since the Netopia Router is capable of serving Telnet and HTTP, we recommend using these services instead of Ping.

Allowing VPNs through a Firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

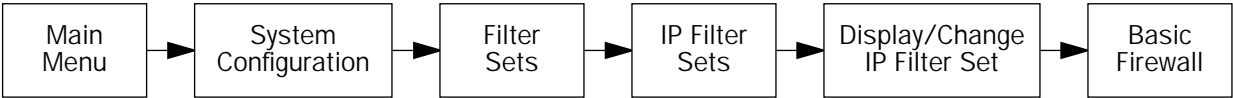
- [“PPTP example” on page 14-23](#)
- [“ATMP example” on page 14-26](#)

Make your own appropriate substitutions. For more information on filters and firewalls, see the *User's Reference Guide*.

PPTP example

To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+-#----Source IP Addr----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+								
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes	
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes	

For Input Filter 1 set the Destination Port information as shown below.

Change Input Filter 1

Enabled:

Forward:

Source IP Address:

Source IP Address Mask:

Dest. IP Address:

Dest. IP Address Mask:

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Established TCP Conns. Only:

Yes

Yes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

TCP

No Compare

0

Equal

1723

No

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

Change Input Filter 2

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

GRE

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+--#-----Source IP Addr-----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+								
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes	
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes	

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

TCP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

Equal

Dest. Port ID:

1723

Established TCP Conns. Only:

No

For Output Filter 2 set the Protocol Type to allow GRE as shown below.

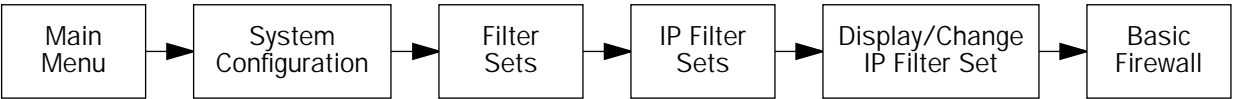
Change Output Filter 2

Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	GRE

ATMP example

To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+--#----Source IP Addr----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+								
+-----+-----+-----+-----+-----+-----+-----+-----+-----+								
1	0.0.0.0	0.0.0.0	UDP	NC	=5150	Yes	Yes	
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes	

For Input Filter 1 set the Destination Port information as shown below.

Change Input Filter 1

Enabled:

Forward:

Yes

Yes

Source IP Address:

Source IP Address Mask:

0.0.0.0

0.0.0.0

Dest. IP Address:

Dest. IP Address Mask:

0.0.0.0

0.0.0.0

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Established TCP Conns. Only:

TCP

No Compare

0

Equal

1723

No

For Input Filter 2 set the Protocol Type to allow GRE as shown below.

Change Input Filter 2

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

GRE

In the Display/Change IP Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+---#-----Source IP Addr-----Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd--+								
1	0.0.0.0	0.0.0.0	UDP	NC	NC	Yes	Yes	
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes	

For Output Filter 1 set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

UDP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

No Compare

Dest. Port ID:

5150

For Output Filter 2 set the Protocol Type to allow GRE as shown below.

Change Output Filter 2

Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	GRE

Windows Networking Broadcasts

The version 4.10 firmware introduces the ability to forward Windows Networking NetBIOS broadcasts. This is useful for, for example, a Virtual Private Network, in which you want to be able to browse the remote network to which you are tunnelling, as part of your Windows Network Neighborhood.

Routed connections, such as VPNs, can not use NetBEUI to carry the Network Neighborhood information. They need to use NetBIOS, because NetBEUI cannot be routed. This feature will allow browsing the Network Neighborhood without any additional workstation configuration.

You enable this feature in the IP Profile Parameters screen of your Connection Profile. The IP Profile Parameters screen varies slightly, depending on whether your model router connects directly to the Internet, or if it connects via an Ethernet connection through a cable or DSL modem. The enabling feature is the same for both:

Direct Connection

IP Profile Parameters	
Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	
Remove Filter Set	
NetBIOS Proxy Enabled	Yes
RIP Profile Options...	

TAB to enable/disable forwarding NetBIOS broadcasts through this profile
Configure IP requirements for a remote network connection here.

WAN Ethernet Connection

WAN Ethernet Configuration	
Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set...	
Remove Filter Set	
NetBIOS Proxy Enabled:	Yes
Enable PPP over Ethernet:	Off
Wan Ethernet MAC Address:	00:00:c5:78:91:9a
DHCP Client Mode:	Standards-Based
RIP Options...	

Using the Tab key, toggle **NetBIOS Proxy Enabled** from the default **No** to **Yes**, and press Return. Your remote Network Neighborhood becomes accessible from your Windows desktop.

Note: Microsoft Network browsing is available with or without a Windows Internet Name Service (WINS) server. Shared volumes on the remote network are accessible with or without a WINS server. Local LAN shared volumes that have Port Address Translation (PAT) applied to them are *not* available to hosts on the remote LAN. For tunnelled traffic, NAT on the WAN has no effect on the Microsoft Networking traffic.

Chapter 15

Internet Key Exchange (IKE) IPsec Key Management

IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). See “[Virtual Private Networks \(VPNs\)](#)” in [Chapter 14](#) for more information.

The version 4.10 firmware supports Internet Key Exchange (IKE) for secure encrypted communication over a VPN tunnel.

Overview

IPsec supports two encapsulation modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. Netopia Routers support Tunnel mode.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. Netopia Routers running firmware version 4.8 or higher offer IPsec DES encryption over the VPN tunnel. Beginning with firmware version 4.10, Netopia Routers offer IPsec 3DES (triple DES) encryption as a standard option. The optional VPN Accelerator (TER/XL) accelerates IPsec encryption and authentication, adds IPComp (LZS compression), and also accelerates PPTP MPPE, ATMP DES, and PPP LZS.

Internet Key Exchange (IKE), introduced in firmware version 4.9, is an authentication and encryption key management protocol used in conjunction with the IPsec standard.

IKE is a two-phase protocol for key exchange.

- Phase 1 authenticates the security gateways and establishes the *Security Parameters* (SPs) they will use to negotiate on behalf of the clients. *Security Associations* (SAs) are sets of information values that allow the two devices on the Internet to communicate securely.
- Phase 2 establishes the tunnel and provides for secure transport of data.

IPsec can be configured without IKE, but IKE offers additional features, flexibility, and ease of configuration. Key exchange between your local router and a remote point can be configured either manually or by using the key exchange protocol.

The advantage of using IKE is that it automatically negotiates IPsec Security Associations and enables IPsec secure communications without having to manually enter the lengthy encryption keys at both ends of the connection. You enter a human-readable pass phrase or shared secret English sentence, like “my dog has fleas” on each end once. This pass phrase is used to authenticate each end to the other. Thereafter, the two ends periodically use a public key encryption method called Diffie-Hellman to exchange key material and then securely generate new authentication and encryption keys. The keys are automatically and continually changing, making the data exchanged using the keys inherently secure.

It also allows you to specify a lifetime for the IPsec Security Association and allows encryption keys to change periodically during IPsec sessions. You can set this period for key generation to as often as your security requirements dictate.

A *Security Policy Database (SPD)* now defines the security requirements. This is a significant change from earlier firmware implementations of IPsec. Traffic with a source IP address that falls within the local member specification of an IPsec tunnel and that is addressed to a destination IP address that falls within the remote member specification of that tunnel is not routed using the normal routing table. Instead it is forwarded using the security policy database to the remote security gateway (remote tunnel endpoint) specified in the IPsec tunnel configuration. It is not possible to send traffic outside the tunnel by bypassing the tunnel and the remote security gateway.

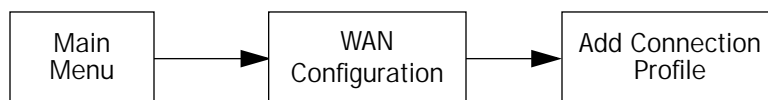
Note: To fully protect against IP address “spoofing” of local member addresses requires firewall rules to be installed on the WAN interface. These must prevent packets coming in through that interface with local member source addresses, since local member source addresses should only originate from the LAN. Otherwise it is theoretically possible for a malicious hacker to send packets through the tunnel by impersonating local member IP addresses. See the chapter “Security” in the *User’s Reference Guide* on your Netopia CD for more information.

Traffic originating from local member LAN addresses that is not addressed to remote member addresses, as well as traffic originating from local LAN IP addresses that do not match any local member specifications, is routed using the normal routing table. This means that if you want to restrict traffic from local members from going out to the Internet and force it all to go through one or more tunnels you need to specify remote members of 0.0.0.0 - 255.255.255.255 or 0.0.0.0/0. Traffic originating from the router, for example, telnet, ping, DNS queries, will not use the default VPN definition even if the source addresses match. Traffic to and from the router is included in specific VPNs.

Internet Key Exchange (IKE) Configuration

IPsec tunnels are defined in the same manner as PPTP tunnels. (See “[PPTP configuration](#)” on page 14-4.) You configure the Connection Profile as follows.

From the Main Menu navigate to WAN Configuration and then Add Connection Profile.



The Add Connection Profile screen appears.

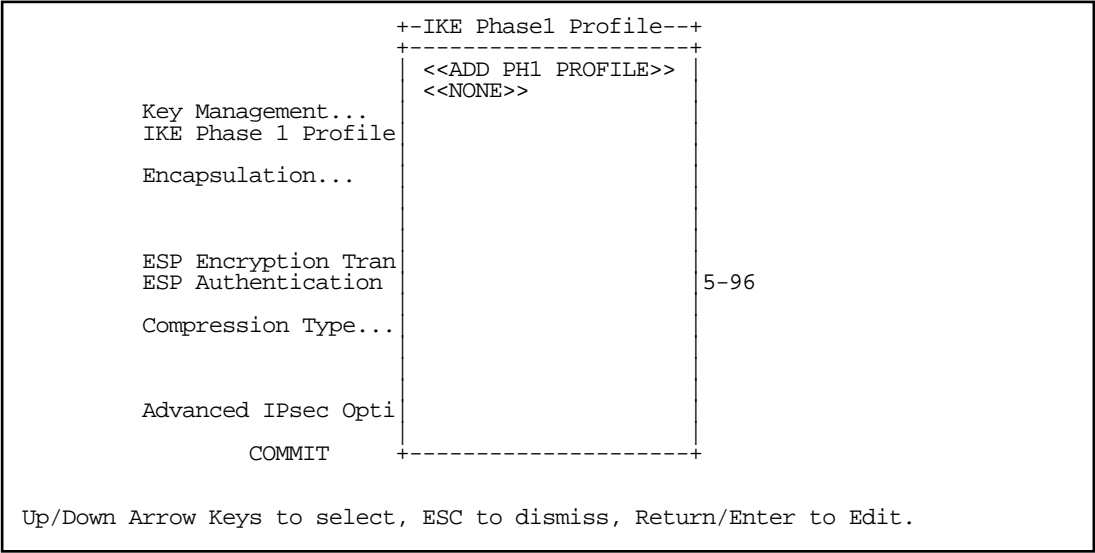
Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	<input checked="" type="checkbox"/>
Encapsulation Type...	PPP
Encapsulation Options...	HDL
	Frame Relay
	RFC1483
	ATMP
	PPTP
	IPsec
IP Profile Parameters...	
Interface Group...	Primary
COMMIT	CANCEL

- From the **Encapsulation Type** pop-up menu select **IPsec**.
- Then select **Encapsulation Options**. The IPsec Tunnel Options screen appears.

IPsec Tunnel Options	
Key Management...	IKE
IKE Phase 1 Profile...	
Encapsulation...	ESP
ESP Encryption Transform...	DES
ESP Authentication Transform...	HMAC-MD5-96
Compression Type...	None
Advanced IPsec Options...	
COMMIT	CANCEL

For **Key Management** you can use either **IKE** or **Manual**. If you choose Manual, skip to “[IPsec Manual Key Entry](#)” on page 15-16. If you choose IKE (the default) continue below.

- Select **IKE Phase 1 Profile** and press Return.



- A pop-up window displays a list of IKE Phase 1 Profiles that you have configured. If you have not previously configured an IKE Phase 1 Profile, the selection **ADD PH1 PROFILE** allows you to do that now.

Adding an IKE Phase 1 Profile

IKE Phase 1 Profiles contain the information that the two ends of a tunnel use to authenticate each other and the parameters that govern the public key cryptography exchanges that are required to generate new keys periodically. Make sure to add an IKE Phase 1 Profile. If an IKE Phase 1 Profile is not assigned to an IKE Connection Profile, all VPN traffic for that profile will be discarded.

Select **ADD PH1 PROFILE**. The Add IKE Phase 1 Profile screen appears.

Add IKE Phase 1 Profile	
Profile Name:	IKE Profile 1
Mode...	Aggressive Mode
Local Identity Type...	IPv4 Address
Local Identity Value:	0.0.0.0
Remote Identity Type...	IPv4 Address
Remote Identity Value:	0.0.0.0
Authentication Method...	Shared Secret
Shared Secret:	*****
Encryption Algorithm...	des
Hash Algorithm...	md5
Diffie-Hellman Group...	Group 2 (1024 bits)
Advanced IKE Phase 1 Options...	
ADD IKE PHASE 1 PROFILE	CANCEL

- The **Profile Name** field accepts any name of up to 16 characters. Sixteen IKE Phase 1 profiles are supported, since each of the potential sixteen Connection Profiles may be associated with a separate IKE Phase 1 profile.
- The **Mode** pop-up menu allows you to choose between Main Mode (the default) and Aggressive Mode.
- In **Main Mode** the router hides the **Local** and **Remote Identity Type** and **Value** fields, defaults to the host address, and always uses the IPV4 Address and the local and remote tunnel endpoint address.
- In **Aggressive Mode** the **Local** and **Remote Identity Type** pop-up menus allow you to choose the type of Identity value to use: IPv4 Address, IPv4 Subnet, IPv4 Range, Host Name, E-Mail Address, Key ID (ASCII), and Key ID (HEX). The **Local** and **Remote Identity Type** and **Value** menus allow you to specify one of the following, based on what Local Identity Type you selected in the previous pop-up menu:

IPv4 Address: A single IPv4 address in the familiar dotted-quad notation (a.b.c.d).

IPv4 Subnet: A single IPv4 network address in dotted-quad notation (a.b.c.d) followed by a mask specified *either* by a slash and a bit-count between 0 and 32 OR by a second dotted-quad.

IPv4 Range: Two IPv4 addresses in dotted quad notation (a.b.c.d) separated by a space.

Host Name: A fully-qualified domain name (FQDN).

E-Mail Address: An RFC 822 e-mail address in the form *user@hostname*.

Key ID (ASCII): An opaque string consisting of printable ASCII characters represented as a sequence of printable ASCII characters.

Key ID (HEX): An opaque string consisting of arbitrary 8-bit ASCII values represented as a sequence of hexadecimal digits, each of which corresponds to one nibble of the string value.
- The **Authentication Method** pop-up menu specifies the IKE Phase 1 authentication method. The only currently supported authentication method is Shared Secret. Other methods may be supported in future firmware releases.
- The **Shared Secret** field allows you to enter a shared secret phrase (between 1 and 48 characters long)

that will be used to generate key material for IKE Phase 1.

- The **Encryption Algorithm** pop-up menu specifies the IKE Phase 1 encryption algorithm, and may be either DES (the default) or 3DES.
- The **Hash Algorithm** pop-up menu specifies the IKE Phase 1 hash algorithm, and may be either SHA1 (the default) or MD5.
- The **Diffie-Hellman Group** pop-up menu specifies the IKE Phase 1 Diffie-Hellman key exchange size, and may be either Group 1 (768 bits), Group 2 (1024 bits) (the default), or Group 5 (1536 bits).
- If you select **Advanced IKE Phase 1 Options** the Advanced IKE Phase 1 Options screen appears.

Advanced IKE Phase 1 Options

Negotiation...	Normal
SA Use Policy...	Newest SAs Immediately
Allow Dangling Phase 2 SAs:	Yes
Phase 1 SA Lifetime (seconds):	28800
Phase 1 SA Lifetime (Kbytes):	0
Send Initial Contact Message:	Yes
Include Vendor ID Payload:	Yes
Independent Phase 2 Re-keys:	Yes
Strict Port Policy:	No

Return/Enter accepts * Tab toggles * ESC cancels.

Normally it is not necessary to change the settings of the items on the Advanced IKE Phase 1 Options screen. Most of these settings exist for ensuring compatibility with remote IKE implementations that may have certain limitations.

- The **Negotiation** pop-up menu allows you to specify the way the device will respond to a connection attempt. Normal (the default) is a two-way mode; Initiate Only or Respond Only permit limiting the connection to one-way only.
- The **SA Use Policy** pop-up menu specifies the policy that the router will use to determine which Phase 1 SAs to use when multiple valid Phase 1 SAs are available for transmitting traffic on an IPsec tunnel.

Because the router normally re-keys prior to the expiration of the current Phase 1 SAs, multiple valid Phase 1 SAs may exist during the period of time after the router has re-keyed and established new Phase 1 SAs and the time at which the old Phase 1 SAs expire.

- If you select **Newest SAs Immediately**, the router will begin using the newly created Phase 1 SAs immediately after they are negotiated.
- If you select **Old SAs Until Expired**, the router will continue using the old Phase 1 SAs until they expire and will begin using the newly created Phase 1 SAs only after the old ones are no longer valid.
- **Allow Dangling Phase 2 SAs** toggles whether or not Phase 2 SAs are permitted to survive the expiration of

the Phase 1 SAs under which they were created. Phase 2 SAs “dangle” when the Phase 1 SA under which they were created expires before they do. There is no requirement that the Phase 1 SA exist for the duration of the Phase 2 SA’s lifetime, but it is convenient because a Delete message may be sent.

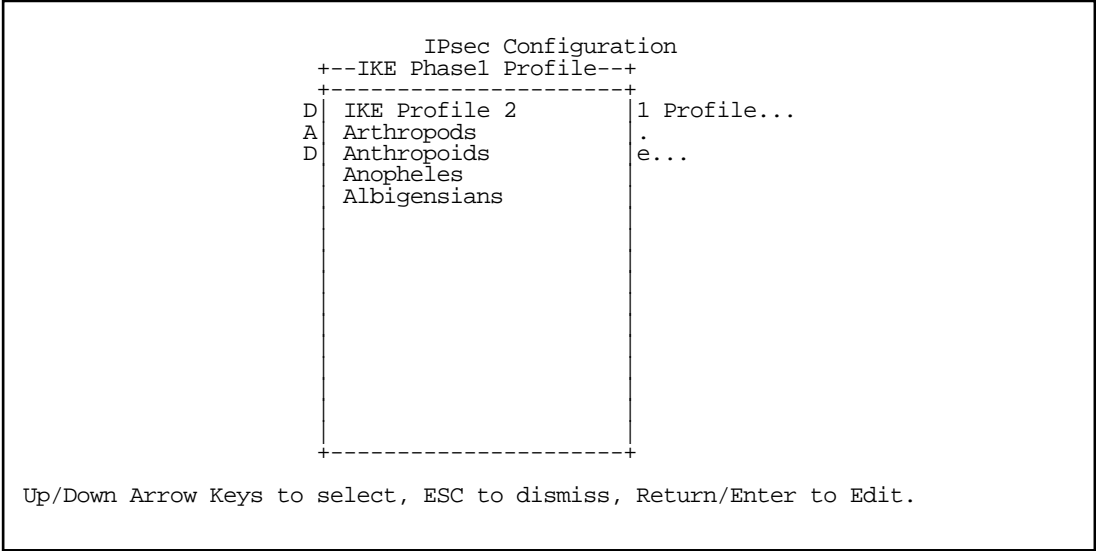
- The two SA Lifetime items specify the lifetime associated with each Phase 1 SA and control when the SA will expire and become invalid.
 - **Phase 1 SA Lifetime (seconds)** specifies the duration in seconds for which the SA will remain valid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 28,800 seconds. The value zero specifies the default.
 - **Phase 1 SA Lifetime (Kbytes)** specifies the maximum number of kilobytes of data that may be secured (encrypted/decrypted or authenticated) using the SA before it expires and becomes invalid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 0 Kilobytes. The value zero specifies the absence of a secured data lifetime.

Note: It is invalid to set both lifetime values to zero. This condition is not enforced by the console (in order to avoid order dependencies when configuring the items), but will set defaults at runtime.

- **Send Initial Contact Message** toggles whether or not the IKE negotiation process begins by sending an initial contact message. The default is **Yes**.
- **Include Vendor-ID Payload** toggles whether or not the router includes the vendor-ID payload in its IKE Phase 1 messages.
- **Independent Phase 2 Re-keys** toggles whether or not a Phase 2 re-keys requires a Phase 1 re-key. If this item is set to Yes (the default), Phase 2 re-keys will be performed independently when necessary without requiring a Phase 1 re-key. If this item is set to No, each Phase 2 re-key will be preceded by a Phase 1 re-key. This item should normally be set to Yes unless the device is communicating with a non-compliant remote IPsec peer that requires that a Phase 1 re-key precede each Phase 2 re-key.
- **Strict Port Policy** toggles whether or not IKE requires packets to originate from the IANA IKE port (500). Set to **Yes**, the router will listen only to port 500 and source its packets from port 500. Set to **No**, the router will return traffic to whatever port originated it.

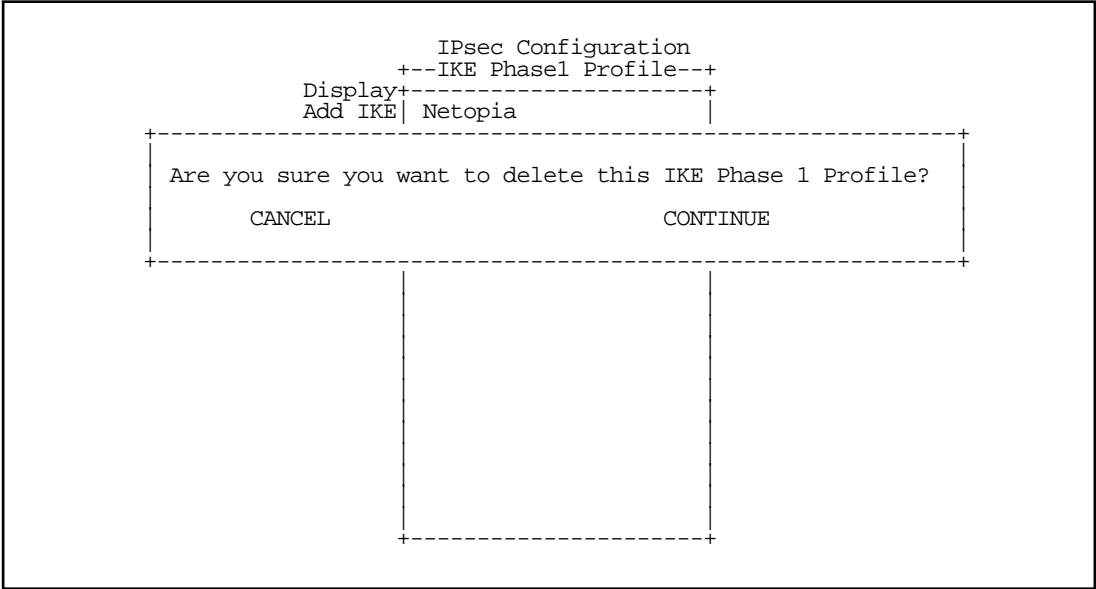
Changing an IKE Phase 1 Profile

Selecting **Display/Change IKE Phase 1 Profile** or **Delete IKE Phase 1 Profile** displays an IKE Phase 1 profile pop-up menu listing the names of all currently defined IKE Phase 1 profiles:



Selecting **Display/Change IKE Phase 1 Profile** and choosing an IKE phase 1 profile name from the pop-up list displays the Change IKE Phase 1 Profile screen. This screen is identical to the Add IKE Phase 1 Profile screen shown above.

Selecting **Delete IKE Phase 1 Profile** and choosing an IKE phase 1 profile name from the pop-up list displays a confirmation alert asking you to confirm that you really want to delete the specified IKE phase 1 profile:



Key Management

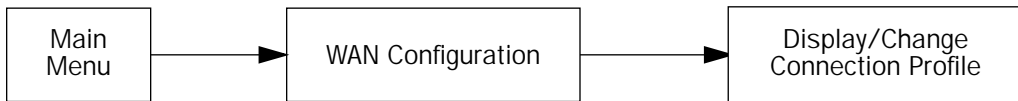
You specify your IKE key management on a per-Connection Profile basis. You can do this in one of three ways:

- You can create your IKE Phase 1 Profile first, and then associate it with an existing Connection Profile
- You can create a Connection Profile and then modify it to associate it with an existing IKE Phase 1 Profile
- You can create a new Connection Profile and add a new IKE Phase 1 Profile as you go

You can do this WAN Configuration menus.

Refer to your *User's Reference Guide* for instructions on creating a Connection Profile if you don't already know how to do that.

You can access the Key Management menus from the Change Connection Profile menu under the WAN Configuration screen for a Connection Profile you have already created,



or you can create a new Connection Profile with your IKE settings included, as you go.

The IKE Key management settings are part of the Data Link Options that you specify in the Add Connection Profile or Change Connection Profile menus. In this description, it is assumed that you are changing an existing Connection Profile.

A Change Connection Profile screen is shown below.

Change Connection Profile

Profile Name:	Easy Setup Profile
Profile Enabled:	+-----+
Encapsulation Type...	+-----+
Encapsulation Options...	PPP
	ATMP
	PPTP
	IPsec
IP Profile Parameters...	+-----+
Telco Options...	
COMMIT	CANCEL

Note: The Change Connection Profile screen will offer different options, depending on the model of router you are using. For a router with the Dial Backup feature, you can associate an IPsec profile with the Primary, the Backup, or choose to apply it to Any Port of the WAN interface by choosing the interface from the Interface Group pop-up menu as shown below.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	Yes
Encapsulation Type...	IPsec
Encapsulation Options...	
IP Profile Parameters...	
Interface Group...	<div>+-----+ +-----+ Primary Backup Any Port +-----+ +-----+</div>
COMMIT	CANCEL

From the Encapsulation Type pop-up menu, select **IPsec**. Then select **Encapsulation Options** and press Return. The IPsec Tunnel Options screen appears.

IPsec Tunnel Options	
Key Management...	IKE
IKE Phase 1 Profile...	
Encapsulation...	ESP
ESP Encryption Transform...	DES
ESP Authentication Transform...	HMAC-MD5-96
Advanced IPsec Options...	
COMMIT	CANCEL

The **Key Management** pop-up menu at the top of the IPsec Tunnel Options screen allows you to choose between IKE key management (the default for a new IPsec profile beginning with firmware version 4.9) and Manual key management.

If you select **Manual**, the IKE Phase 1 Profile option does not display, and you must enter your IPsec Manual Keys under the IPsec Manual Keys screen. See “IPsec Manual Key Entry” on page 16.

- The **IKE Phase 1 Profile** pop-up menu allows you to associate an IKE Phase 1 Profile with the IPsec tunnel. An IKE Phase 1 Profile specifies the set of parameters that will be used for the IKE Phase 1 exchange. IKE Phase 1 Profiles may be shared by multiple IPsec tunnels. The pop-up menu item displays the name of the currently associated IKE Phase 1 Profile, if any, or is blank if no IKE Phase 1 profile is associated with the tunnel.

The pop-up menu lists the names of all currently defined IKE Phase 1 Profiles. The pop-up menu also includes an <<ADD PH1 PROFILE>> item to allow you to define a new IKE Phase 1 Profile directly without first going to the IPsec Configuration screen, and a <<NONE>> item to allow you to dissociate an existing IKE Phase 1 Profile from the IPsec tunnel.

The remainder of the screen allows you to configure the IKE Phase 2 parameters that control the contents of the single IKE Phase 2 proposal sent by the router. These same items specify the values that must be offered by one of the remote peer’s proposals.

- The **Encapsulation** pop-up menu allows you to select what IPsec encapsulations will be used: ESP only (the default), AH only, or AH+ESP (both AH and ESP).
- An **AH Authentication Transform** pop-up menu (which is visible only if you have selected AH or AH+ESP encapsulation) allows you to specify the type of AH authentication: HMAC-MD5-96 or HMAC-SHA1-96.
- The **ESP Encryption Transform** pop-up menu (which is visible only if you have selected ESP or AH+ESP encapsulation) allows you to specify the type of ESP encryption: DES, 3DES, or NULL (no encryption).
- The **ESP Authentication Transform** pop-up menu (which is visible only if you have selected ESP or AH+ESP encapsulation) allows you to specify the type of ESP authentication: None, HMAC-MD5-96, or HMAC-SHA1-96.

If you select **Advanced IPsec Options**, the Advanced IPsec Options screen appears.

Advanced IPsec Options	
SA Lifetime seconds:	28800
SA Lifetime Kbytes:	0
Perfect Forward Secrecy:	Yes
Dead Peer Detection:	No

This screen allows you to specify the lifetime associated with each IPsec Security Association (SA) and control when the SA will expire and become invalid.

- **SA Lifetime (seconds)** specifies the duration in seconds for which the SA will remain valid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 28,800 seconds (1 hour). The value zero specifies the absence of an elapsed time lifetime.
- **SA Lifetime (Kilobytes)** specifies the maximum number of kilobytes of data that may be secured (encrypted/decrypted or authenticated) using the SA before it expires and becomes invalid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 0 Kilobytes. The value zero specifies the absence of a secured data lifetime.

Note: It is invalid to set both lifetime values to zero! This condition is not enforced by the console (in order to avoid order dependencies when configuring the items), but rather is enforced at runtime and will cause the IPsec profile to assume the defaults.

- **Perfect Forward Secrecy** toggles whether or not Perfect Forward Secrecy will be used. Enabling Perfect Forward Secrecy (the default) causes IKE to perform a new Diffie-Hellman exchange with each Phase 2 re-key. Because the additional Diffie-Hellman exchanges required for Perfect Forward Secrecy introduce additional overhead, it may be good to disable Perfect Forward Secrecy when security does not require it.
- **Dead Peer Detection** toggles whether or not the router will detect a remote peer being offline. Dead peer detection counts the outbound packets on a tunnel. If 256 packets go out without a single packet coming in, the tunnel SAs are expired and a rekey is started. Rekeying is first attempted on the previous Phase 1 SA. If the Phase 1 request times out, then the Phase 1 SA is expired and Phase 1 rekeying is begun over again.

Press Escape to return to the Add or Change Connection Profile screen, and select **IP Profile Parameters**.

If you enable IKE key management the IP Profile Parameters screen appears.

IP Profile Parameters	
Remote Tunnel Endpoint:	0.0.0.0
Remote Member Format...	Subnet
Remote Member Address:	0.0.0.0
Remote Member Mask:	255.255.255.255
Local Member Format...	Subnet
Local Member Address:	0.0.0.0
Local Member Mask:	0.0.0.0
Address Translation Enabled:	Yes
NAT Map List...	<<None>>
NAT Server List...	<<None>>
PAT IP Address:	0.0.0.0
Filter Set...	<<None>>
Remove Filter Set	
Advanced IP Profile Options...	
COMMIT	CANCEL

- The **Remote Tunnel Endpoint** field accepts either an IP address in the familiar dotted-quad notation a.b.c.d or a hostname to be resolved using the Domain Name System (DNS).
- The **Remote Member Format** pop-up menu allows you to select Subnet (the default), Range, or Host Address. This indicates the type of Remote member specification. The Address and Mask items change to 1st Address and Last Address when the Format is set to Range. Selecting Host Address allows you to specify a single host address for the Member ID.

Note: Many IKE implementations do not accept ranges; they will only accept subnets.

- The **Remote Member Address** accepts either a network address or a host address. You can specify the format Subnet, and enter a host address and a host (all-ones) mask, or you can specify a format Range and enter the single address as both the first and last address in the range.
- The **Local Member Format** pop-up menu allows you to select Subnet (the default), Range, or Host Address. This indicates the type of Local member specification. The Address and Mask items change to 1st Address and Last Address when the Format is set to Range. Selecting Host Address allows you to specify a single host address for the Member ID.
- **Local Member Address** and **Local Member Mask** apply only to IKE or Manual key management.

- Specifying IKE key management alters the **Advanced IP Profile Options** screen as follows:

Advanced IP Profile Options

Local Tunnel Endpoint Address:	0.0.0.0
Next Hop Gateway:	0.0.0.0
Idle Timeout (seconds):	300

- You can specify a **Local Tunnel Endpoint Address**. If not 0.0.0.0, this value must be one of the assigned interface addresses, either WAN or LAN. This is used as the source address of all IPsec traffic.
- You can specify a **Next Hop Gateway**. If you specify the Remote Tunnel Endpoint Address, and the address is in the same subnet as the Remote Members Network you specified in the IP Profile Parameters, the **Next Hop Gateway** option allows you to enter the address by which the gateway partner is reached.

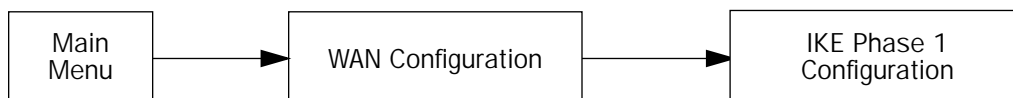
If you do not specify the Remote Tunnel Endpoint Address, the router will use the default gateway to reach the partner. If the partner should be reached via an alternate port (for example, the LAN instead of the WAN), the **Next Hop Gateway** field allows this path to be resolved.

- You can specify an **Idle Timeout (seconds)** value. The idle timeout tells the router that if no traffic passes through the tunnel for the specified number of seconds, no automatic SA re-key should be performed. When new traffic does pass through the tunnel, the idle timeout interval resets again when the current SAs expire.

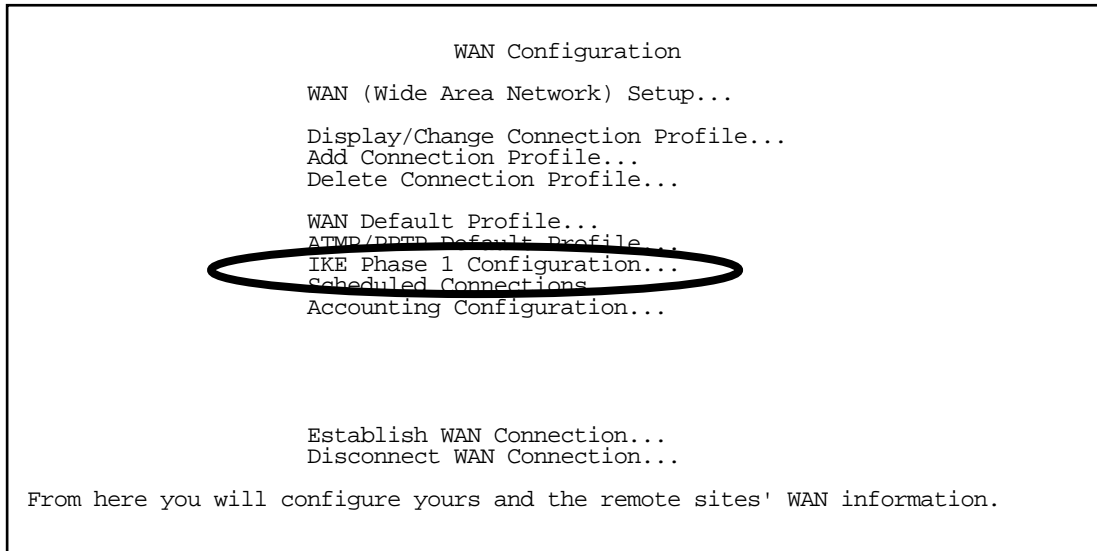
If you set the value to zero, the router will re-key the SA whenever the SA Lifetime interval specifies, regardless of whether traffic is passing through it or not. This will effectively “nail up” the tunnel.

IPsec WAN Configuration Screens

You can also configure IKE Phase 1 Profiles in the WAN Configuration menus.

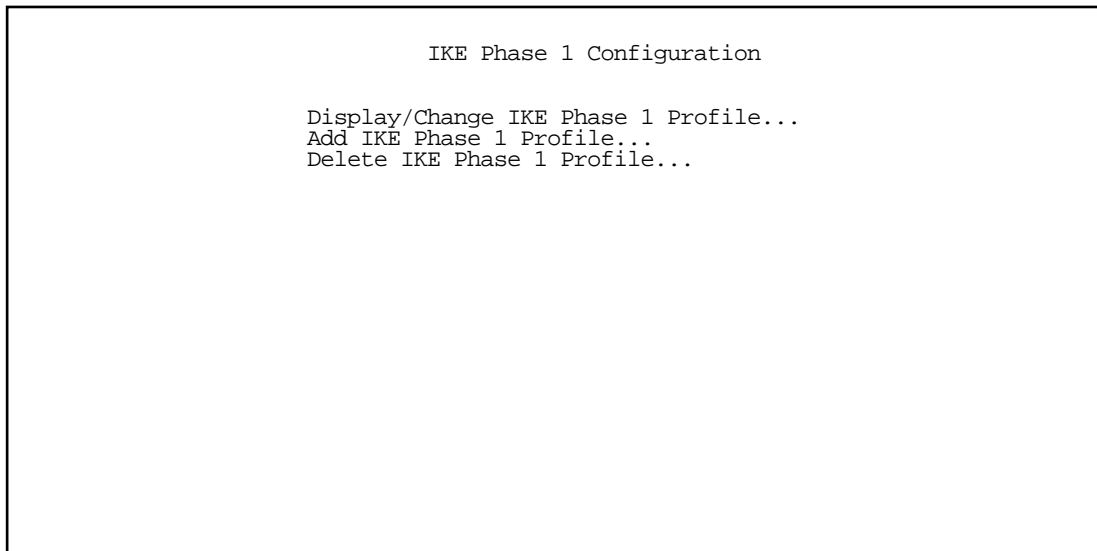


The WAN Configuration screen now includes IKE Phase 1 Configuration as shown:



Select **IKE Phase 1 Configuration** and press Return.

The IKE Phase 1 Configuration screen appears.



The IKE Phase 1 Configuration screen allows configuration of global (non-connection-profile-specific) IPsec parameters. This screen allows you to Display, Change, Add, or Delete an IKE Phase 1 profile.

IPsec Manual Key Entry

The version 4.10 firmware has a redesigned layout and additional options for manual key entry. If you selected Manual Key Management in the IPsec Tunnel Options screen, you will need to enter your encryption keys in the IPsec Manual Keys screen.

IPsec Tunnel Options	
Key Management...	Manual
Encapsulation...	ESP
ESP Encryption Transform...	DES
ESP Authentication Transform...	HMAC-MD5-96
IPsec Manual Keys...	
COMMIT	CANCEL

Select **IPsec Manual Keys** and press Return.

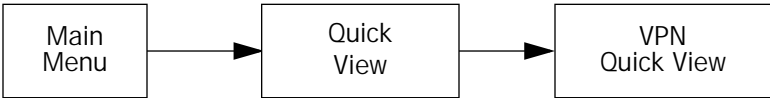
IPsec Manual Keys	
SHA1 ESP Auth. Key:	
SHA1 AH Auth. Key:	

Depending on your selections of Encapsulation, Encryption Transform, and Authentication Transform in the IPsec Tunnel Options screen, the IPsec Manual Keys screen will display differing entry fields to enter authorization keys and encryption keys.

With Manual Keys, you must manually configure identical authentication and encryption keys at both ends of the tunnel. The authentication keys are either 32 (for MD5) or 40 (for SHA1) ascii hex characters, while the encryption keys are 16 (for DES) or 48 (for triple-DES) ascii-hex characters.

VPN Quickview

Statistics are displayed on the VPN Quick View screen.



The VPN Quick View screen has been modified slightly in firmware version 4.10.

VPN Quick View					
Profile Name-----	Type--	Rx Pckts--	Tx Pckts--	Discard--	Remote Address--
HA <-> FA1 (Jony Fon	ATMP	99	99		173.166.82.8
HA <-> FA3 (Sleve M.	ATMP	13	14		63.193.117.91
My IPsec Tunnel	IPsec	23	12		0.0.0.0
Bangalore	PPTP	45	35		1.1.1.1

If the remote tunnel end point is a hostname (or "0.0.0.0") 0.0.0.0 is displayed until a Security Association is established. Previously the remote members network was displayed.

WAN Event History Error Reporting

The following events are logged and displayed in the WAN Event History screen:

Event message:	Meaning:
IKE: no ph1 preferences assigned	An attempt was made to use an IPsec profile with no IKE profile attached to it.
IKE: DNS lookup failure	The DNS lookup of the remote tunnel end point has failed.
IKE: no matching ph1 profile	An IKE phase 1 request was received and did not match any of the profiles stored in the local router.
IKE: no matching proposal	An IKE phase 1 request was received and the proposal did not match an allowed parameter, or else the remote rejected the local router's proposal.
IKE: phase 1 auth failure	The phase 1 remote authentication failed.
IKE: phase 1 resend timeout	The attempt to resend the phase 1 remote authentication timed out.
IKE: phase 1 complete	The phase 1 negotiation completed successfully.
IKE: phase 2 hash failure	The phase-2 hash failed because the data received is out of date or has been tampered with.
IKE: no matching ph2 proposal	Either the local router rejected the proposals of the remote or the remote rejected the local router's.
IKE: ph2 resend timeout	The attempt to resend the phase 2 authentication timed out.
IKE: phase 2 complete	The phase 2 negotiation completed successfully.

Chapter 16

Multiple Network Address Translation (MultiNAT)

Beginning with version 4.6, the firmware offers enhanced Network Address Translation functionality.

This chapter covers the following topics:

- [Overview on page 16-2](#)
- [MultiNAT Configuration on page 16-7](#)
- [Basic configuration – Easy Setup Profile on page 16-7](#)
- [Advanced configuration – Server Lists and Dynamic NAT on page 16-8](#)
- [Adding Server Lists on page 16-18](#)
- [Binding Map Lists and Server Lists on page 16-24](#)
- [NAT Associations on page 16-31](#)
- [MultiNAT Configuration Example on page 16-33](#)
- [Firmware Upgrades and NAT on page 16-37](#)

Introduced in version 4.4, 4.5, 4.6, and 4.8 MultiNAT supports the following features:

- **NetBIOS Datagram service**
NetBIOS datagram service is transparently mapped so that the domain login service will be available. It is possible to browse a remote network from behind NAT if the remote network has an NT server and domain login. The resources of the host behind NAT will not be available to the remote network.
- **Arbitrary IP protocol pass-through for Static and Dynamic NAT addresses**
All IP protocols are passed through the Static and Dynamic NAT mappings.
- **Unmapped IP address support**
IP addresses can be passed through the router unmapped. The (un)mapping is indicated by a Static map with the Public range and Private map addresses equal to each other. The unmapped addresses function as though they are routed without NAT applied.
- **QuickTime 4 (RTP and RTSP) support**
Transparent support for QuickTime 4 and RealAudio native streaming protocols has been added. Multiple streams and multiple hosts are supported.
- **Transparent NetMeeting Gateway**
A single NetMeeting session at a time can be supported.
- **Default service export is no longer necessary**
Although the Easy Servers list is created by default, it does not contain any entries. Creating a server list no longer adds a default entry for the router. Additionally, all such entries are removed by the upgrade to version 4.8.

The service exports are added to the end of the list (similar to NAT rules) rather than to the beginning as in firmware versions earlier than 4.8.

You should read this chapter completely before attempting to configure any of the advanced NAT features available.

Overview

NAT (Network Address Translation) is a means of mapping one or more IP addresses and/or IP service ports into different values. This *mapping* serves two functions:

- It allows the addresses of many computers on a LAN to be represented to the public Internet by only one or a few addresses, saving you money.
- It can be used as a security feature by obscuring the true addresses of important machines from potential hackers on the Internet.

To help you understand some of the concepts discussed here, it may be helpful to introduce some NAT terminology.

The term *mapping* refers to rules that associate one or more private addresses on the Netopia Router's LAN to one or more public addresses on the Netopia Router's WAN interface (typically the Internet).

The terms *private* and *internal* refer to addresses on the Netopia Router's LAN. These addresses are considered private because they are protected or obscured by NAT and cannot be directly accessed from the WAN (or Internet) side of the Netopia Router unless specifically configured otherwise.

The terms *public* and *external* refer to the WAN (or Internet) side of the Netopia Router.

Features

MultiNAT features can be divided into several categories that can be used simultaneously in different combinations on a per-Connection Profile basis.

The following is a general description of these features:

Port Address Translation

The simplest form of classic Network Address Translation is *PAT* (Port Address Translation). PAT allows a group of computers on a LAN, such as might be found in a home or small office, to share a single Internet connection using one IP address. The computers on the LAN can surf the web, read email, download files, etc., but their individual IP addresses are never exposed to the public network. Instead, a single IP address, the IP address of the router, acts as the source IP address of traffic originating from the LAN. The Netopia allows you to define multiple PAT mappings, which can be individually mapped to different public IP addresses. This offers more control over the access permitted to users on the LAN.

A limitation of PAT is that communication must be initiated from the internal network. A user on the external side can not access a machine behind a PAT connection. A PAT enhancement introduced in firmware version 4.4 is the ability to define multiple PAT mappings. Each of these can optionally map to a section or *range* of IP addresses of the internal network. PAT mapping allows only internal users to initiate traffic flow between the internal and external networks.

Server lists

Server lists, previously known as exported services, make it possible to provide access from the public network to hosts on the LAN. Server Lists allow you to define particular services, such as web, ftp, or e-mail, which are available via a public IP address. You define the type of service you would like to make available, and the internal IP address to which you would like to provide access. You may also define a specific public IP address to use for this service if you want to use an IP other than the WAN IP address of the Netopia Router.

Static mapping

If you want to host your own website or provide other Internet services to the public, you need more than classic NAT. The reason is noted above – external users cannot initiate traffic to computers on your LAN because external users can never see the real addresses of the computers on your LAN. If you want users outside your LAN to have access, for example, to a web or FTP server that you host, you need to make a representation of the real IP addresses of those servers public.

Static mappings are a way to make one or more private IP addresses fully accessible from the public network via corresponding public IP addresses. Some applications may negotiate multiple TCP connections in the process of communication, which often does not work with traditional PAT. Static mapping offers the ability to use these applications through NAT. Each private IP address is mapped, on a one-to-one basis, to a public IP address that can be accessed from the Internet or public network. As with PAT mappings, you may have multiple Static mappings to map a range of private IP addresses to a range of public IP addresses if desired.

Dynamic mapping

New in firmware 4.5, *Dynamic mapping*, often referred to as Many-to-Few, offer an extension to the advantages provided by Static mapping. Instead of requiring a one to one association of public addresses and private addresses, as is required in Static mapping, Dynamic mapping uses a group of public IP addresses to dynamically allocate static mappings to private hosts that are communicating with the public network. If a host on the private network initiates a connection to the Internet, for example, the Netopia router automatically sets up a one-to-one mapping of that host's private IP address to one of the public IP addresses allocated to be used for Dynamic NAT. As long as this host is communicating with the Internet, it will be able to use that address. When traffic from that host ceases, and no traffic is passed from that host for five minutes, the public address is made available again for other private hosts to use as necessary.

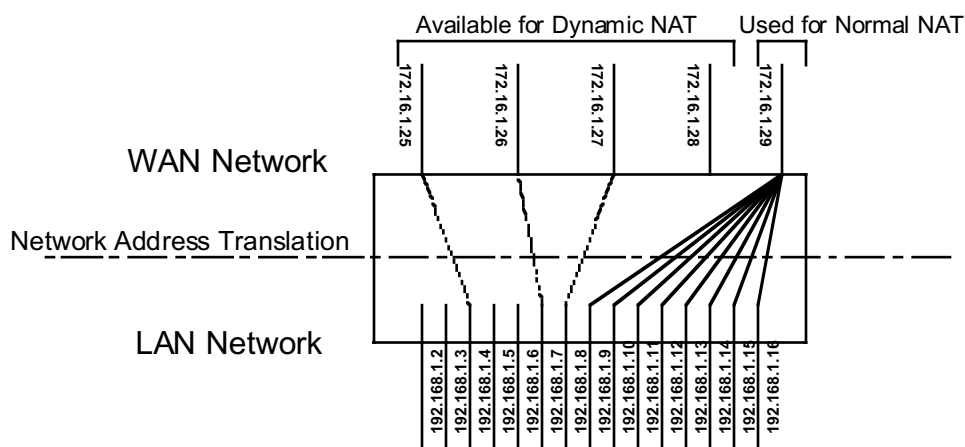
When addresses are returned to the group of available addresses, they are returned to the head of the group, being the most recently used. If that same host requests a connection an hour later, and the same public address is still available, then it will be mapped to the same private host. If a new host, which has not previously requested a connection, initiates a connection it is allocated the last, or oldest, public address available.

Dynamic NAT is a way of sharing a range of public, or exterior, NAT addresses among one or more *groups* of private, or interior, hosts. It is generally referred to as *Many-to-Few* mapping. This is intended to provide superior support for applications that traditionally have difficulty communicating through NAT. Dynamic NAT is intended to provide functionality beyond Many-to-One and One-to-One translation. The 4.4 firmware release made it possible to have a static mapping of one public address to one private address, thus allowing applications such as NetMeeting to work by assuring that any traffic sent back to the source IP address is forwarded through to the internal machine.

Static One-to-One mapping works well if you have enough IP addresses for all the workstations on your LAN. If you do not, Dynamic NAT allows machines to make full use of the publicly routable IP addresses provided by the ISP as necessary, on demand. When these public IP addresses are no longer being used by a particular workstation, they are returned to a pool of available addresses for other workstations to use.

A common example is a DSL customer's application. Most DSL ISPs only provide customers with a few IP addresses for use on their network. For networks with more than four or five machines it is usually mandatory to use NAT. A customer may have 15 workstations on the LAN, all of which need Internet access. The customer is only provided five IP addresses by their ISP. The customer has eight hosts, which only need to use email and have web access, but another seven hosts, which use NetMeeting to communicate with clients once or twice a day. NetMeeting will not work unless a static One-to-One mapping exists for the machine running NetMeeting to use for communication. The customer does not have enough IP addresses to create a One-to-One mapping for each of the seven users. This is where Dynamic NAT applies.

The customer can configure four of these addresses to be used for Dynamic NAT. The fifth address is then used for the eight other machines that do not need One-to-One mappings. As each machine configured to use addresses from the dynamic pool tries to connect to the Internet it is allocated a public IP address to use temporarily. Once the communication has been terminated, that IP address is freed for one of the other six hosts to use.



Exterior addresses are allocated to internal hosts on a demand, or as-needed, basis and then made available when traffic from that host ceases. Once an internal host has been allocated an address, it will use that address for all traffic. Five minutes after all traffic ceases – no pings, all tcp connections closed, no DNS requests, etc. – the address is put at the head of an *available* list. If an interior host needs an exterior address an hour later, and the previously used address is still available, it will acquire the same address. If an interior host that has not previously been allocated an exterior address needs one, it will be allocated the last, hence the oldest, exterior address on the available list.

All NAT configurations are *rule-based*. This means that traffic passed through NAT from either the public or the private network is compared to the rules and mappings configured in the Netopia Router in a particular order. The first rule that applies to the traffic being initiated is used.

For example, if a connection is initiated from the public network and is destined for a public IP address configured on the Netopia router, the following comparisons are made in this order.

- The Netopia router first checks its internal NAT cache to see if the data is part of a previously initiated connection, if not...
- The Netopia router checks the configured Server Lists to see if this traffic is intended to be forwarded to an

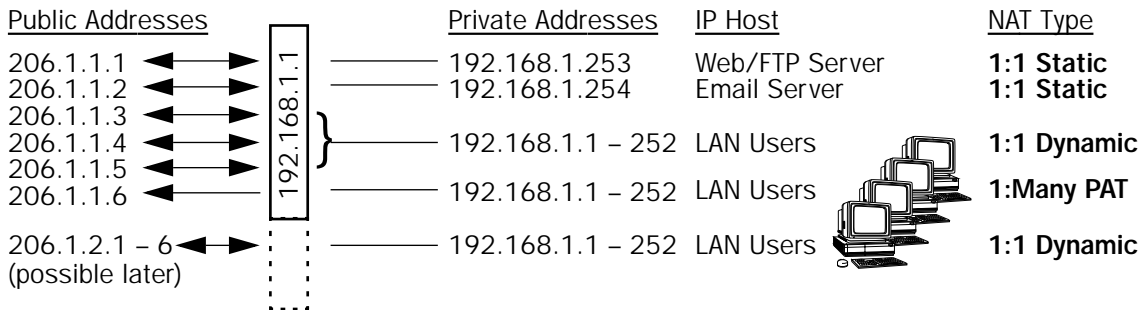
internal host based on the type of service.

- The Netopia router then checks to see if there is a Static, Dynamic, or PAT mapping for the public IP address that the connection is being initiated to.
- The Netopia router answers the request itself if the data is destined for the Netopia's WAN interface IP address. Otherwise the data is discarded.

Complex maps

Map Lists and Server Lists are completely independent of each other. A Connection Profile can use one or the other or both.

MultiNAT allows complex mapping and requires more complex configuration than in firmware versions earlier than 4.5. Multiple mapped interior subnets are supported, and the rules for mapping each of the subnets may be different. The figure below illustrates a possible multiNAT configuration.



In order to support this type of mapping, you define two address ranges. First, you define a public range which contains the first and last public address to be used and the way in which these addresses should be used (PAT, static, or dynamic). You then configure an address map which defines the private IP address or addresses to be used and which public range they should be mapped to. You add the address map to the list of address maps which are configured, creating a Map List. The mappings in the Map List are order-dependent and are compared in order from the top of the list to the bottom. If a particular resource is not available, subordinate mappings can be defined that will redirect traffic.

Enhancements

In firmware versions previous to version 4.4, NAT had a single public IP address that was always associated with the Connection Profile's WAN IP address. This was always the PAT public address and the exported services public address. Beginning with firmware version 4.5, this association is no longer required. beginning with version 4.6 you are allowed multiple public addresses, none of which have to be the same as the Connection Profile WAN IP address. Any public addresses not associated with the Connection Profile WAN IP address must have a static route pointing to it from a router on the public network if public users are expected to be able to access the NATed machines or services. The multiple NAT feature enhancements include the following:

- Default behavior consistent with previous firmware versions, including PAT to a DHCP- or PPP-assigned address.
- A feature of NAT in firmware version 4.5 is 1:1 Dynamically Assigned NAT Mapping. This allows internal

addresses to be temporarily assigned a public IP address to use for NAT. When the private host is finished communicating, the public IP address is made available for use by other internal hosts again.

- 1-to-1 static NAT mapping.

An internal private address is permanently mapped to an external address. TCP and UDP port addresses are not altered.

- Multiple Many-to-1 PAT mappings on a single interface.

PAT addresses may be assigned to specific private address subnets. Unlike pre-4.4 NAT, not all internal machines need to be included on a PAT mapping list.

- Coexistent mapped and unmapped traffic on a public interface.

If the router's IP address is not included in a NAT list, it will be invisible to the external network.

- Mapped services (exports) may use multiple public addresses.

- NAT maps per WAN interface, similar to the filter rules.

Supported traffic

MultiNat supports the following IP protocols:

- PAT: TCP/UDP traffic which does not carry source or destination IP addresses or ports in the data stream (i.e., HTTP, telnet, 'r' commands, tftp, NFS, NTP, SMTP, NNTP, etc.).
- Static NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.
- Dynamic NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.

MultiNAT Configuration

You configure the MultiNAT features through the console menu:

- For a simple 1-to-many NAT configuration (classic NAT), use the [Basic configuration – Easy Setup Profile](#), described below.
- For the more advanced features, such as Server Lists and Dynamic NAT, follow the instructions in:
 - [IP setup](#), described on [page 16-9](#)
 - [IP profile parameters](#), described on [page 16-24](#)

Basic configuration – Easy Setup Profile

The screen below is an example. Depending on the type of router you are using, fields displayed in this screen may vary.

Connection Profile 1: Easy Setup Profile

Number to Dial:	2125551212
Address Translation Enabled:	Yes
IP Addressing...	Unnumbered
Local WAN IP Address:	206.1.1.6
Local WAN IP Mask:	0.0.0.0
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
PPP Authentication...	PAP
Send User Name:	tony
Send Password:	*****

PREVIOUS SCREEN
NEXT SCREEN

Enter the directory number for the remote network connection.
Enter basic information about your WAN connection with this screen.

The **Local WAN IP Address** is used to configure a NAT public address range consisting of the Local WAN IP Address and all its ports. The public address map list is named *Easy-PAT List* and the port map list is named *Easy-Servers*.

When you exit this screen the two map lists, Easy-PAT List and Easy-Servers, are created by default and NAT configuration becomes effective. This will map all your private addresses (0.0.0.0 through 255.255.255.255) to your public address. These map lists are bound to the Easy Setup Profile. See [Binding Map Lists and Server Lists on page 16-24](#).

This is all you need to do if you want to continue to use a single PAT, or 1-to-many, NAT configuration.

Advanced configuration – Server Lists and Dynamic NAT

You use the advanced NAT feature sets by first defining a series of mapping rules and then grouping them into a *list*. There are two kinds of lists -- *Map Lists*, made up of Dynamic, PAT and Static mapping rules, and *Server Lists*, a list of internal services to be presented to the external world. Creating these lists is a four-step process:

1. **Define the public range** of addresses that external computers should use to get to the NAT internal machines. These are the addresses that someone on the Internet would see.
2. **Create a List name** that will act as a rule or server holder.
3. **Create a map or rule** that specifies the internal range of NATed addresses and the external range they are to be associated with.
4. **Associate the Map or Server List to your WAN interface** via a Connection Profile or the Default Profile.

The three NAT features all operate completely independently of each other, although they can be used simultaneously on the same Connection Profile.

You can configure a simple 1-to-many PAT (often referred to simply as NAT) mapping using Easy Setup. More complex setups require configuration using the **Network Address Translation** item on the IP Setup screen.

An example MultiNAT configuration at the end of this chapter describes some applications for these features. See [MultiNAT Configuration Example on page 16-33](#).

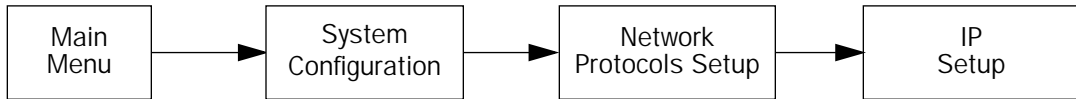
In order to configure the router to make servers on your LAN visible to the Internet, you use advanced features in the System Configuration screens, described in [IP setup on page 16-9](#).

Note: There is no implicit binding between the WAN IP interface address and NAT, as in earlier firmware versions, so you cannot disallow configuration of NAT simply because the interface is numbered or disallow configuration of the addressing type (numbered or unnumbered) simply because NAT is enabled.

If the router has a numbered interface, then it is addressable by the IP address. In firmware versions earlier than 4.4, when NAT was enabled the interface would be marked unnumbered and the IP address subsumed by NAT. However, NAT would allow traffic directed to that IP address to be delivered to the router. This effectively made the interface a numbered interface. MultiNAT adds the option of true unnumbered NAT. Traffic delivered to the router on an unnumbered interface which cannot be processed by NAT is dropped.

IP setup

To access the NAT configuration screens, from the Main Menu navigate to IP Setup:



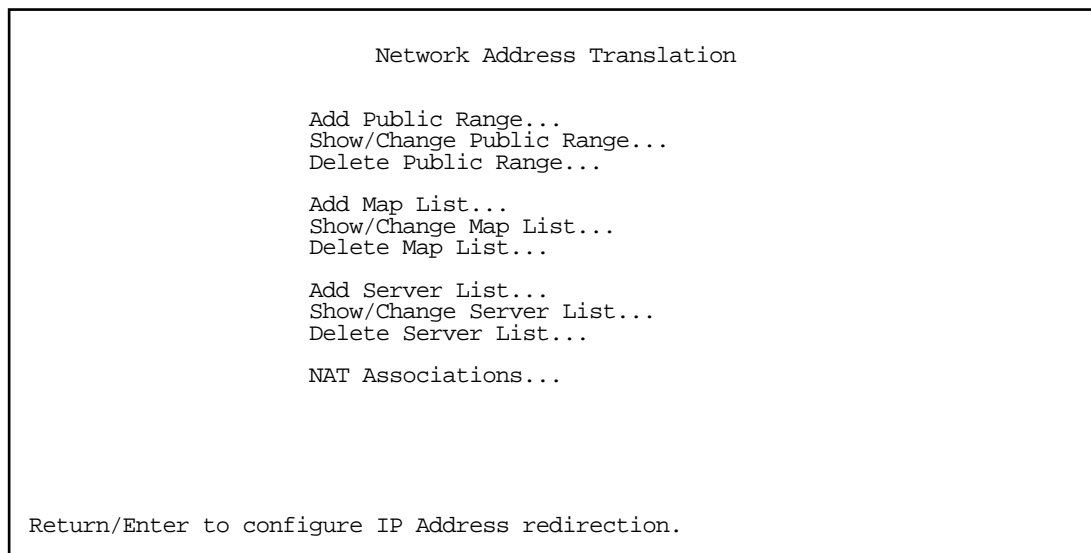
IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Domain Name:	isp.com
Receive RIP:	Both
Transmit RIP:	Off
Static Routes...	
IP Address Serving Setup Network Address Translation (NAT)... Filter Sets...	

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
 Set up the basic IP attributes of your Netopia in this screen.

Select **Network Address Translation (NAT)** and press Return.

The Network Address Translation screen appears.



Public Range: defines an external address range and indicates what type of mapping to apply when using this range. The types of mapping available are *dynamic*, *static* and *pat*.

Map Lists: define collections of mapping rules. A rule maps interior range addresses to exterior range addresses by the mapping techniques defined in the map list.

Server Lists: bind internal IP addresses and ports to external IP addresses and ports so that connections initiated from the outside can access an interior server.

NAT rules

The following rules apply to assigning NAT ranges and server lists:

- Static public address ranges must not overlap other static, PAT, public addresses or the public address assigned to the router's WAN interface.
- A PAT public address must not overlap any static address ranges. It may be the same as another PAT address or server list address, but the port range must not overlap.

You configure the ranges of exterior addresses by first adding public ranges.

Select **Add Public Range** and press Return.

The Add NAT Public Range screen appears.

Add NAT Public Range

Range Name:	my_first_range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535

ADD NAT PUBLIC RANGE
CANCEL

- Select **Range Name** and give a descriptive name to this range.
- Select **Type** and from the pop-up menu, assign its type. Options are static, dynamic, or pat (the default).
 - If you choose *pat* as the range type, select **Public Address** and enter the exterior IP address in the range you want to assign. Select **First** and **Last Public Port** and enter the first and last exterior ports in the range. These are the ports that will be used for traffic initiated from the private LAN to the outside world.

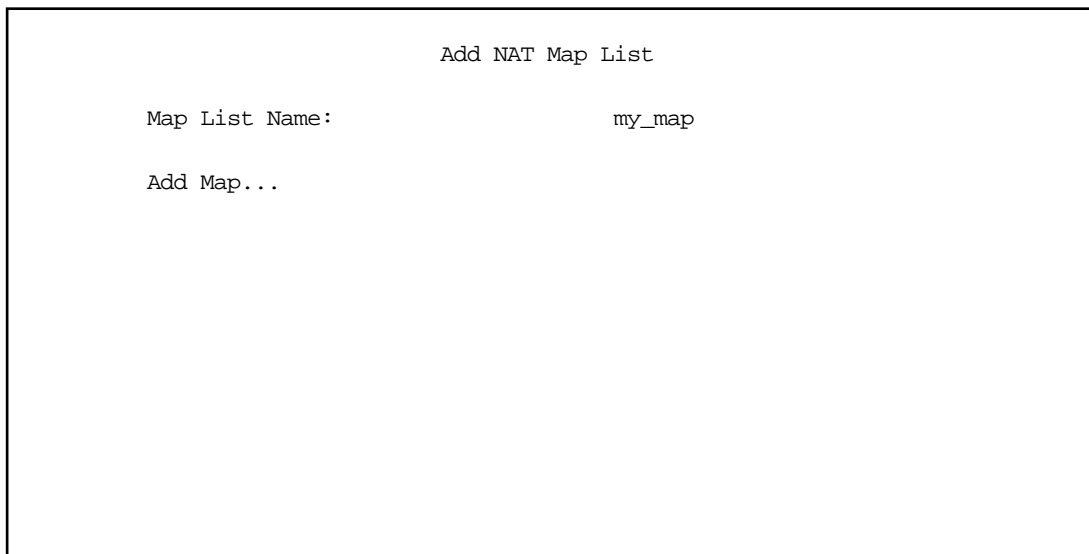
Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.

- If you choose *dynamic* as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.
- If you choose *static* as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.
- Select **ADD NAT PUBLIC RANGE** and press Return. The range will be added to your list and you will be returned to the Network Address Translation screen.

Once the public ranges have been assigned, the next step is to bind interior addresses to them. Because these bindings occur in ordered lists, called *map lists*, you must first define the list, then add mappings to it.

From the Network Address Translation screen select **Add Map List** and press Return.

The Add NAT Map List screen appears.

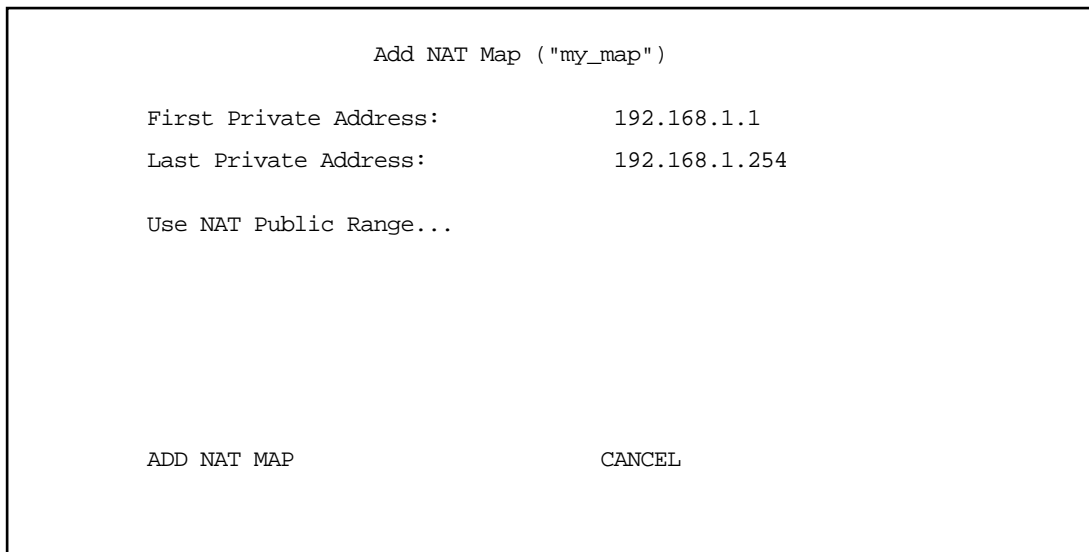


Add NAT Map List

Map List Name: my_map

Add Map...

- Select **Map List Name** and enter a descriptive name for this map list. A new menu item **Add Map** appears.
- Select **Add Map** and press Return. The Add NAT Map screen appears.



Add NAT Map ("my_map")

First Private Address: 192.168.1.1

Last Private Address: 192.168.1.254

Use NAT Public Range...

ADD NAT MAP CANCEL

- Select **First** and **Last Private Address** and enter the first and last interior IP addresses you want to assign to this mapping.
- Select **Use NAT Public Range** and press Return. A screen appears displaying the public ranges you have

defined.

```

Add NAT Map ("my_map")
+--Public Address Range-----Type-----Name-----+
+-----+-----+-----+-----+
| 0.0.0.0      --      pat      Easy-PAT      |
| 206.1.1.6    --      pat      my_first_range |
| 206.1.1.1    206.1.1.2  static  my_second_range |
| <<NEW RANGE...>> |
+-----+-----+-----+-----+

```

Select ←

Up/Down Arrow Keys to select, ESC to cancel, Return/Enter to Delete.

- From the list of public ranges you defined, select the one that you want to map to the interior range for this mapping and press Return.

If none of your preconfigured ranges are suitable for this mapping, you can select **<<NEW RANGE>>** and create a new range. If you choose **<<NEW RANGE>>**, the Add NAT Public Range screen displays and you can create a new public range to be used by this map. See [Add NAT Public Range on page 16-11](#).

- The Add NAT Map screen now displays the range you have assigned.

```

Add NAT Map ("my_map")

First Private Address:      192.168.1.1
Last Private Address:      192.168.1.254

Use NAT Public Range...    my_first_range
Public Range Type is:      pat
Public Range Start Address is: 206.1.1.6

ADD NAT MAP                CANCEL

```

- Select **ADD NAT MAP** and press Return. Your mapping is added to your map list.

Modifying map lists

You can make changes to an existing map list after you have created it. Since there may be more than one map list you must select which one you are modifying.

From the Network Address Translation screen select **Show/Change Map List** and press Return.

- Select the map list you want to modify from the popup menu.

```

Network Address Translation
+-NAT Map List Name--+
+-----+
Add Out  Easy-PAT List
Show/Ch  my_map
Delete
Add Map
Show/Ch
Delete
Add Ser
Show/Ch
Delete
NAT Ass

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.
```

The Show/Change NAT Map List screen appears.

```

Show/Change NAT Map List

Map List Name:          my_map

Add Map...
Show/Change Maps...
Delete Map...
Move Map...
```

- **Add Map** allows you to add a new map to the map list.
- **Show/Change Maps** allows you to modify the individual maps within the list.
- **Delete Map** allows you to delete a map from the list.
- **Move Map** allows you to change the priority order in which the map is evaluated within the list. See [Moving maps on page 16-16](#).

Selecting **Show/Change Maps**, **Delete Map**, or **Move Map** displays the same pop-up menu.

Show/Change NAT Map List				
+---Private Address Range-----		Type---	Public Address Range-----	
192.168.1.1	192.168.1.254	pat	206.1.1.6	--
192.168.1.253	192.168.1.254	static	206.1.1.1	206.1.1.2
192.168.1.1	192.168.1.252	dynamic	206.1.1.3	206.1.1.5

Scroll to the map you want to modify using the arrow keys and press Return.

The Change NAT Map screen appears.

Change NAT Map ("my_map")	
First Private Address:	192.168.1.253
Last Private Address:	192.168.1.254
Use NAT Public Range...	my_second_range
Public Range Type is:	static
Public Range Start Address is:	206.1.1.1
Public Range End Address is:	206.1.1.2
CHANGE NAT MAP	CANCEL

Make any modifications you need and then select **CHANGE NAT MAP** and press Return. Your changes will become effective and you will be returned to the Show/Change NAT Map List screen.

Moving maps

The Move Maps screen permits reordering the priority of maps in a map list. Since the maps are read from top to bottom, those at the top have the highest priority, those at the bottom have the lowest. If you used Easy Setup for your initial configuration, and added subsequent maps and server lists, you may need to reorder their priority since new maps are added to the top of the list.

Show/Change NAT Map List

Private Address Range	Type	Public Address Range
192.168.1.1	pat	206.1.1.6
192.168.1.252	static	206.1.1.1
192.168.1.2	dynamic	206.1.1.3

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

In the example screen above, you may want to reorder the priority of the maps such that the dynamic map applies first and any additional traffic is routed via PAT or static.

All operations are done from a single pop-up menu.

- In the Show/Change Map List screen, select **Move Map**. A selection mode pop-up menu appears. In this mode you scroll to the map you want to move and press **Return** to select it for moving.
- After pressing **Return** you are in Move mode. Arrow keys move the selected map up or down. When you press **Return** again the map is put in the new location permanently and the pop-up menu is dismissed.

Show/Change NAT Map List				
+---Private Address Range-----		Type-----	Public Address Range-----	
192.168.1.2	192.168.1.252	dynamic	206.1.1.3	206.1.1.252
192.168.1.252	192.168.1.253	static	206.1.1.1	206.1.1.2
192.168.1.1	192.168.1.251	pat	206.1.1.6	--

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- You can press **Escape** at any time in the pop-up menu to abort the move and restore the map list to its original ordering.

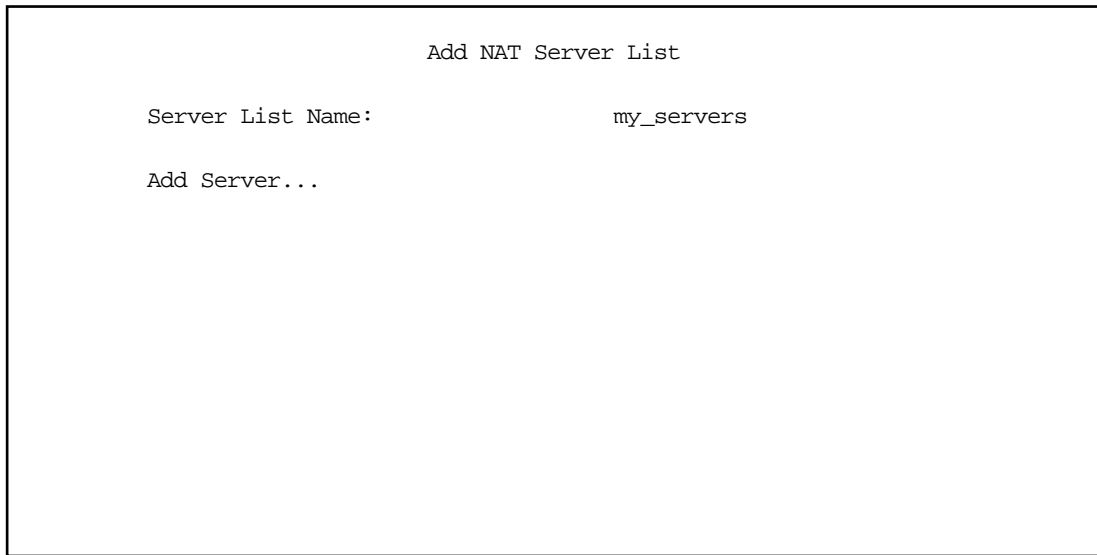
Note: The *pat* map is generally left at the bottom of the list.

Adding Server Lists

Server lists, also known as Exports, are handled similarly to map lists. If you want to make a particular server's port accessible (and it isn't accessible through other means, such as a static mapping), you must create a Server List.

Select **Add Server List** from the Network Address Translation screen.

The Add NAT Server List screen appears.



Add NAT Server List

Server List Name: my_servers

Add Server...

- Select **Server List Name** and type in a descriptive name. A new menu item, **Add Server**, appears.

- Select **Add Server** and press Return. The Add NAT Server screen appears.

```

                                Add NAT Server ("my_servers")

Service...

Server Private IP Address:      192.168.1.45
Public IP Address:             206.1.1.1

                                ADD NAT SERVER                                CANCEL

```

- Select **Service** and press Return. A pop-up menu appears listing a selection of commonly exported services.

```

                                Add NAT Server ("my_servers")
                                +-Type-----Port(s)-----+
Service...
Server Private IP Address:
Public IP Address:
                                +-----+
                                ftp      21
                                telnet   23
                                smtp     25
                                tftp     69
                                gopher   70
                                finger   79
                                www-http 80
                                pop2     109
                                pop3     110
                                snmp     161 - 162
                                timbuku  407
                                pptp     1723
                                irc      6665 - 6669
                                Other...
                                +-----+
                                ADD NAT SERVER                                CANCEL

```

- Choose the service you want to export and press Return.

You can choose a preconfigured service from the list, or define your own by selecting **Other**. If you select **Other**, a screen is displayed that allows you to enter the port number range for your customized service.

Other Exported Port

First Port Number (1..65535):	31337
Last Port Number (1..65535):	31337

OKCANCEL

- Enter the **First** and **Last Port Number** between ports 1 and 65535. Select **OK** and press Return. You will be returned to the Add NAT Server screen.

- Enter the **Server Private IP Address** of the server whose service you are exporting.

Since MultiNAT permits the mapping of multiple private IP addresses to multiple public IP addresses, your ISP or corporate site's router must be configured such that it knows that your multiple public addresses are accessible via your router.

If you want to use static mappings to map internal servers to public addresses, your ISP or corporate site's router must also be configured for static routes to these public addresses on the Netopia Router.

- Enter the **Public IP Address** to which you are exporting the service.

Note: For PAT Map lists and Server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and Server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and Server lists will acquire that address each time it is negotiated.

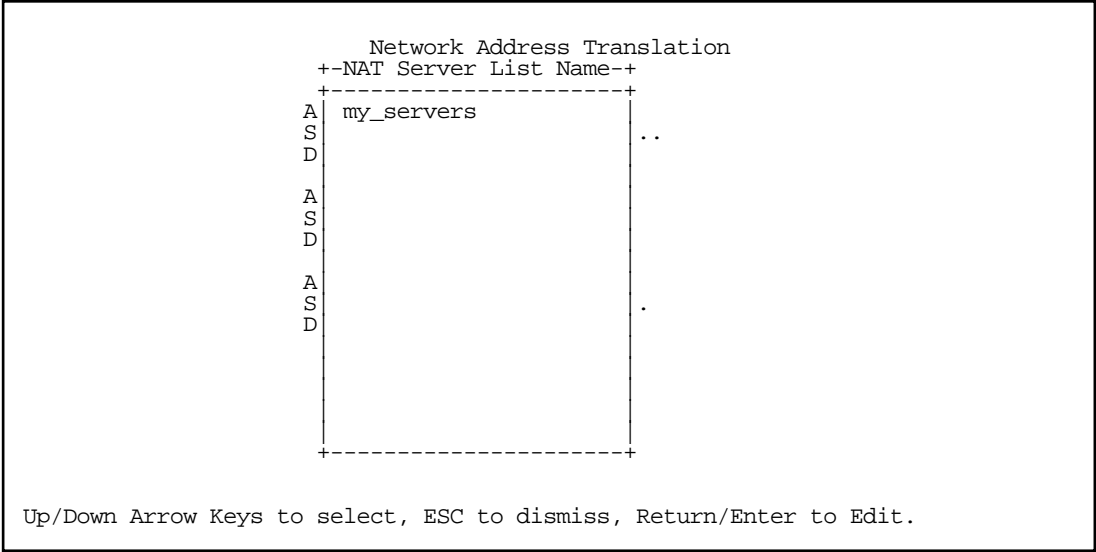
- Select **ADD NAT SERVER** and press Return. The server will be added to your server list and you will be returned to the Add NAT Server List screen.

Note: **CUSeeMe** (or other services that listen on specific ports) through MultiNat works as it did for non-MultiNat releases prior to version 4.4. In order to use **CUSeeMe** through the Netopia Router, you must export the ports 7648 and 7649. In MultiNat, you may use a port range export. Without the export, CUSeeMe will fail to work. This is true unless a static mapping is in place for the host using CUSeeMe. In that case no Server List entry is necessary.

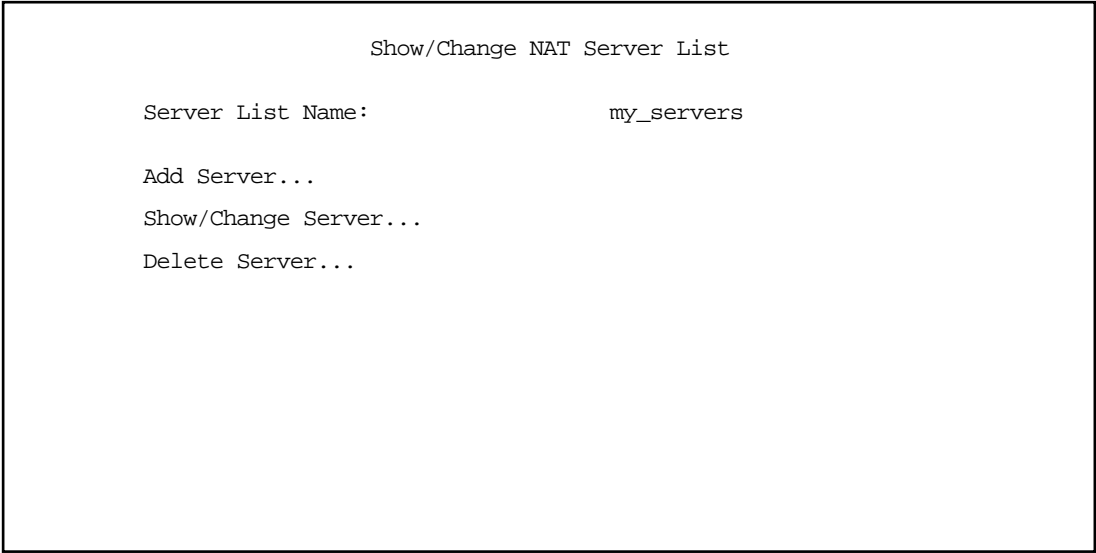
Modifying server lists

Once a server list exists, you can select it for modification or deletion.

- Select **Show/Change Server List** from the Network Address Translation screen.
- Select the Server List Name you want to modify from the pop-up menu and press Return.



The Show/Change NAT Server List screen appears.



- Selecting **Show/Change Server** or **Delete Server** displays the same pop-up menu.

```

                                Show/Change NAT Server List
      +-Private Address--Public Address---Port-----+
      +-----+-----+-----+
Se  192.168.1.254      206.1.1.6      smtp
    192.168.1.254      206.1.1.5      smtp
    192.168.1.254      206.1.1.4      smtp
Ad  192.168.1.254      206.1.1.3      smtp
    192.168.1.254      206.1.1.1      smtp
Sh
De

```

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Select any server from the list and press **Return**. The Change NAT Server screen appears.

```

Change NAT Server ( "My Exports" )

Service... smtp
Server Private IP Address: 192.168.1.254
Public IP Address: 206.1.1.1

CHANGE NAT SERVER CANCEL

```

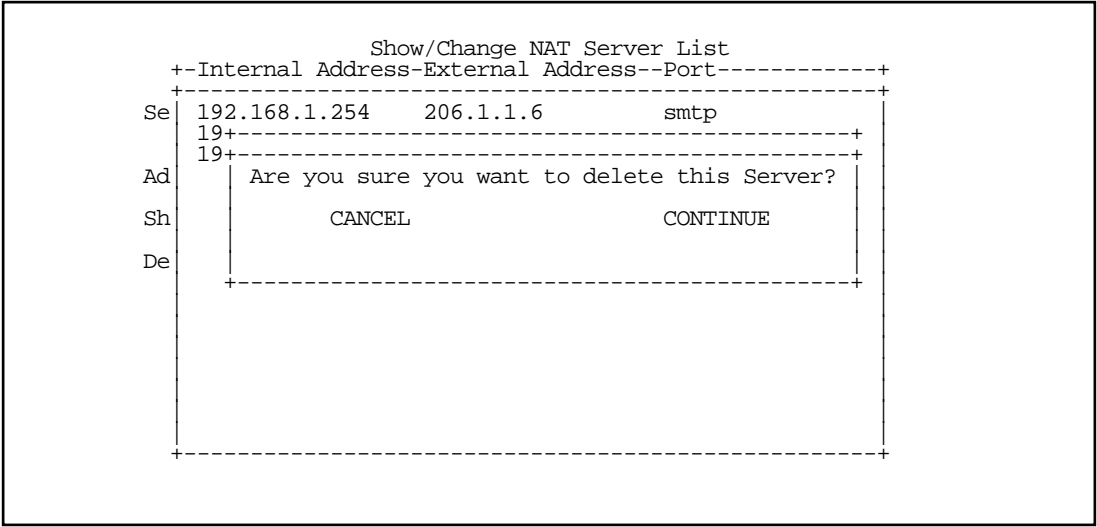
You can make changes to the server's service and port or internal or external address.

Select **CHANGE NAT SERVER** and press Return. Your changes take effect and you are returned to the Show/Change NAT Server List screen.

Deleting a server

To delete a server from the list, select **Delete Server** from the Show/Change NAT Server List menu and press Return.

A pop-up menu lists your configured servers. Select the one you want to delete and press Return. A dialog box asks you to confirm your choice.



Choose **CONTINUE** and press Return. The server is deleted from the list.

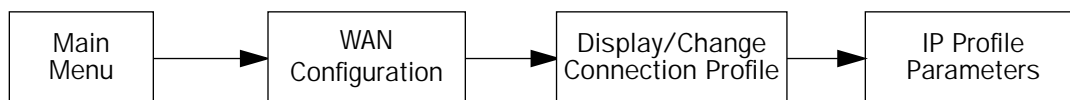
Binding Map Lists and Server Lists

Once you have created your map lists and server lists, for most Netopia router models you must bind them to a profile, either a Connection Profile or the Default Profile. For R9100 Ethernet-to-Ethernet routers, you bind your map lists and server lists directly to the WAN interface. You do this in one of the following screens:

- the [IP profile parameters](#) screen (see below) of the Connection Profile configuration menu
- the [IP Parameters \(WAN Default Profile\)](#) screen (see [page 16-26](#)) of the Default Profile configuration menu
- the [WAN Ethernet configuration](#) screen (see [page 16-28](#)) of the WAN Setup menu
- the [Default Answer Profile](#) screen (see [page 16-30](#))
- the [Binding Map Lists and Server Lists](#) screen (see [page 16-24](#))

IP profile parameters

To bind a map list to a Connection Profile, from the Main Menu go to the WAN Configuration screen then the Display/Change Connection Profile screen. From the pop-up menu list of your Connection Profiles, choose the one you want to bind your map list to. Select **IP Profile Parameters** and press Return.



The IP Profile Parameters screen appears.

IP Profile Parameters	
Address Translation Enabled:	Yes
IP Addressing...	Unnumbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	206.1.1.6
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	NetBIOS Filter
Remove Filter Set	
Receive RIP:	Both

Return/Enter to select <among/between> ...
 Configure IP requirements for a remote network connection here.

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

```

                                IP Profile Parameters
                                +--NAT Map List Name--+
                                +-----+
Address Trans  Easy-PAT          s
IP Addressing my_map           mbered
               <<None>>
NAT Map List. sy PAT
NAT Server Li
Local WAN IP
Remote IP Add 7.0.0.2
Remote IP Mas 5.255.255.255
Filter Set... tBIOS Filter
Remove Filter
Receive RIP:  th
                                +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

- Select the map list you want to bind to this Connection Profile and press Return. The map list you selected will now be bound to this Connection Profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

```

                                IP Profile Parameters
                                +--NAT Server List Name--+
                                +-----+
Address Trans  Easy-Servers      s
IP Addressing my_servers       mbered
               <<None>>
NAT Map List. sy PAT
NAT Server Li
Local WAN IP   0.0.0
Local WAN IP   0.0.0
Remote IP Add  7.0.0.2
Remote IP Mas  5.255.255.255
Filter Set...  tBIOS Filter
Remove Filter
Receive RIP:   th
                                +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

- Select the server list you want to bind to this Connection Profile and press Return. The server list you selected will now be bound to this Connection Profile.

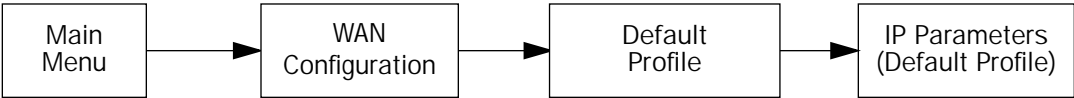
Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

IP Parameters (WAN Default Profile)

Some Netopia router models, such as the R7100, support a WAN default profile that permits several parameters to be configured without an explicitly configured Connection Profile.

For models that support the WAN default profile in the WAN Configuration menu, the procedure is similar to the procedure to bind map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the Default Profile screen. Select **IP Parameters** and press Return.



The IP Parameters (Default Profile) screen appears.

IP Parameters (Default Profile)

Address Translation Enabled:

Yes

NAT Map List...

Easy-PAT List

NAT Server List...

Easy-Servers

Filter Set (Firewall)...

Remove Filter Set

Receive RIP:

Both

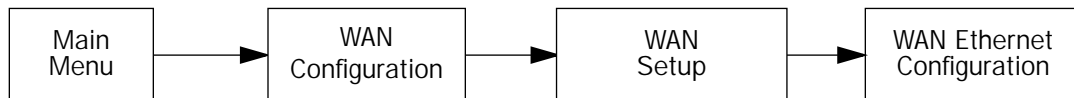
Return/Enter to select <among/between> ...

- Toggle **Address Translation Enabled** to Yes.

WAN Ethernet configuration

For the R9100 Ethernet-to-Ethernet router, the procedure is similar to binding map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the WAN (Wide Area Network) Setup screen. Select **WAN Ethernet Configuration** and press Return.



The WAN Ethernet Configuration screen appears.

WAN Ethernet Configuration	
Address Translation Enabled:	Yes
Local WAN IP Address:	206.1.1.6
NAT Map List...	
NAT Server List...	
Filter Set...	
Remove Filter Set	
Receive RIP:	Both
Aux Serial Port...	
Data Rate (kbps)...	57.6
Aux Modem Init String:	AT&F&C1&D2E0S0=1

Set up the basic IP attributes of your Ethernet Module in this screen.

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

```

                                WAN Ethernet Configuration
                                +--NAT Map List Name--+
                                +-----+
Address Trans  Easy-PAT List      s
Local WAN IP  my_map
              <<None>>

NAT Map List.
NAT Server Li _map

Filter Set...
Remove Filter

Receive RIP:  th

Aux Serial Po ync Modem
Data Rate (kb .6
Aux Modem Ini &F&C1&D2E0S0=1
                                +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

- Select the map list you want to bind to the Ethernet WAN interface and press Return. The map list you selected will now be bound to the Ethernet WAN interface.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

```

                                WAN Ethernet Configuration
                                +--NAT Server List Name--+
                                +-----+
Address Trans  Easy-Servers      s
Local WAN IP  my_servers      0.0.0
              <<None>>

NAT Map List.
NAT Server Li _first_map

Filter Set...
Remove Filter

Receive RIP:  th

Aux Serial Po ync Modem
Data Rate (kb .6
Aux Modem Ini &F&C1&D2E0S0=1
                                +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

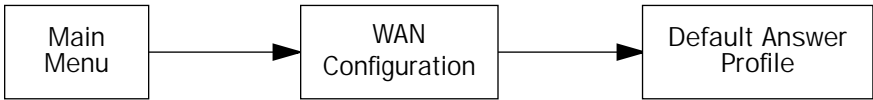
- Select the server list you want to bind to the Ethernet WAN interface and press Return. The server list you selected will now be bound to the Ethernet WAN interface.

NOTE: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

Default Answer Profile

For models that support the default answer profile for dial-in connections, the procedure is similar to binding map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the WAN (Wide Area Network) Setup screen. Select **Default Answer Profile** and press Return.



The Default Answer Profile screen appears.

Default Answer Profile

Must Match a Defined Profile:	No
IP Enabled:	Yes
IP Parameters...	
IPX Enabled:	No
Data Compression...	Standard LZS
Max. Receive Packet Size:	1500
Idle Timeout:	300

Return/Enter accepts * Tab toggles * ESC cancels.
Configure values which may be used when receiving a call in this screen.

If **Must Match a Defined Profile** is set to **Yes**, then the NAT attributes of the Connection Profile take precedence. If you toggle **Must Match a Defined Profile** to **No**, IP-related menu options become visible.

- Select **IP Parameters** and press Return. The IP Parameters (Default Answer Profile) screen appears.

IP Parameters (Default Answer Profile)

Filter Set (Firewall)...
Remove Filter Set

Address Translation Enabled: Yes
Interface IP Address: 0.0.0.0

NAT Map List... Easy-PAT List
NAT Server List... Easy-Servers

Receive RIP: Both
Transmit RIP: Off

Return/Enter to select a Firewall Filter Set for incoming calls.
Configure IP values to use when no matching Profile can be found.

You can then bind NAT Map Lists and NAT Server Lists in the same fashion as described in the section [IP profile parameters on page 16-24](#).

NAT Associations

Configuration of map and server lists alone is not sufficient to enable NAT for a WAN connection because map and server lists must be linked to a profile that controls the WAN interface. This can be a Connection Profile, a WAN Ethernet interface, a default profile, or a default answer profile. Once you have configured your map and server lists, you may want to reassign them to different interface-controlling profiles, for example, Connection Profiles. To permit easy access to this IP Setup functionality, you can use the NAT Associations screen.

You access the NAT Associations screen from the Network Address Translation screen.



Select **NAT Associations** and press Return. The NAT Associations screen appears.

NAT Associations		
Profile/Interface Name-----	Nat?-----	Map List Name-----Server List Name
Default Answer Profile	On	my_first_map my_servers
Easy Setup Profile	On	Easy-PAT my_servers
Profile 01	On	my_second_map my_servers
Profile 02	On	my_first_map my_server_list
Profile 03	On	<<None>> <<None>>

- You can toggle **NAT? On** or **Off** for each Profile/Interface name. You do this by navigating to the **NAT?** field associated with each profile using the arrow keys. Toggle NAT on or off by using the Tab key.
- You can reassign any of your map lists or server lists to any of the Profile/Interfaces. You do this by navigating to the **Map List Name** or **Server List Name** field associated with each profile using the arrow keys. Select the item by pressing Return to display a pop-up menu of all of your configured lists.

NAT Associations		
+NAT Map List Name-+		
Profile/Interface Name-----	Nat+-----	Server List Name
Easy Setup Profile	On	Easy-PAT List my_servers
Profile 01	On	my_first_map my_servers
Profile 02	On	my_second_map my_server_list
Profile 03	On	my_map <<None>>
Profile 04	On	<<None>> <<None>>
Default Answer Profile	On	-----+my_servers
Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.		

- Select the list name you want to assign and press Return again. Your selection will then be associated with the corresponding profile or interface.

MultiNAT Configuration Example

To help you understand a typical MultiNAT configuration, this section describes an example of the type of configuration you may want to implement on your site. The values shown are for example purposes only. *Make your own appropriate substitutions.*

A typical SDSL service from an ISP might include five user addresses. Without PAT, you might be able to attach only five IP hosts. Using simple 1-to-many PAT you can connect more than five devices, but use only one of your addresses. Using multiNAT you can make full use of the address range. The example assumes the following range of addresses offered by a typical ISP:

Local WAN IP address:	206.1.1.6
Local WAN subnet mask:	255.255.255.248
Remote IP address:	206.1.1.254
Default gateway:	206.1.1.254

Public IP addresses assigned by the ISP are 206.1.1.1 through 206.1.1.6 (255.255.255.248 subnet mask).

Your internal devices have IP addresses of 192.168.1.1 through 192.168.1.254 (255.255.255.0 subnet mask).

Netopia router's address is:	192.168.1.1
Web server's address is:	192.168.1.253
Mail server's address is:	192.168.1.254
FTP server's address is:	192.168.1.253

In this example you will statically map the first five public IP addresses (206.1.1.1 - 206.1.1.5) to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5). You will use these 1-to-1 mapped addresses to give your servers "real" addresses. You will then map 206.1.1.6 to the remaining private IP addresses (192.168.1.6 - 192.168.1.254) using PAT.

The configuration process is as follows:

From the Main Menu go to the Easy Setup and then the Connection Profile screen.



Enter your ISP-supplied values as shown below.

Connection Profile 1: Easy Setup Profile

Connection Profile Name:

Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

206.1.1.6

Local WAN IP Mask:

255.255.255.248

PREVIOUS SCREEN

NEXT SCREEN

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

Enter basic information about your WAN connection with this screen.

Select **NEXT SCREEN** and press Return.

Your IP values are shown here.

IP Easy Setup

Ethernet IP Address:

192.168.1.1

Ethernet Subnet Mask:

255.255.255.0

Domain Name:

ISP.net

Primary Domain Name Server:

173.166.101.1

Secondary Domain Name Server:

173.166.102.1

Default IP Gateway:

127.0.0.2

IP Address Serving:

On

Number of Client IP Addresses:

20

1st Client Address:

192.168.1.2

PREVIOUS SCREEN

NEXT SCREEN

Set up the basic IP & IPX attributes of your Netopia in this screen.

Then navigate to the Network Address Translation (NAT) screen.



Select **Show/Change Public Range**, then **Easy-PAT Range**, and press Return. Enter the value your ISP assigned for your public address (206.1.1.6, in this example). Toggle **Type** to *pat*. Your public address is then mapped to the remaining private IP addresses using PAT. (If you were not using the Easy-PAT Range and Easy-PAT List that is created by default by using Easy Setup, you would have to *define* a public range and Map List. For the purpose of this example you can just *alter* this range and list.)

Change NAT Public Range	
Range Name:	Easy-PAT Range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535
CHANGE NAT PUBLIC RANGE	CANCEL

Select **CHANGE NAT PUBLIC RANGE** and press Return. This returns you to the Network Address Translation screen.

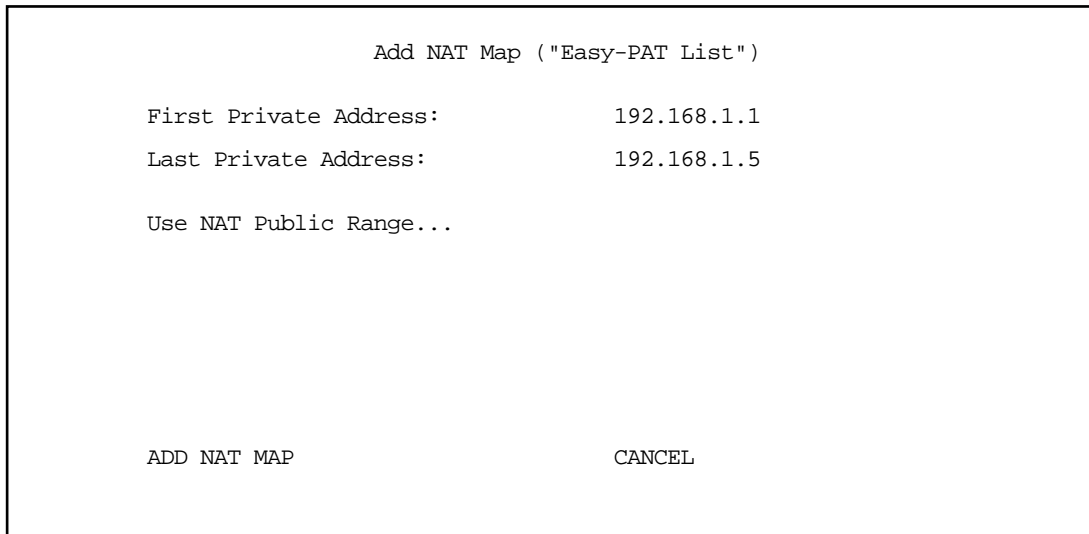
Select **Add Public Range** and press Return. Type a name for this static range, as shown below. Enter the first and last public addresses your ISP assigned in their respective fields as shown. The first five public IP addresses (206.1.1.1 - 206.1.1.5, in this example) are statically mapped to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5).

Add NAT Public Range	
Range Name:	Static Range
Type...	static
First Public Address:	206.1.1.1
Last Public Address:	206.1.1.5
ADD NAT PUBLIC RANGE	CANCEL

Return/Enter to commit changes.

Select **ADD NAT PUBLIC RANGE** and press Return. You are returned to the **Network Address Translation** screen.

Next, select **Show/Change Map List** and choose **Easy-PAT List**. Select **Add Map**. The **Add NAT Map** screen appears. (Now the name *Easy-PAT List* is a misnomer since it has a static map included in its list.) Enter in 192.168.1.1 for the **First Private Address** and 192.168.1.5 for the **Last Private Address**.



```

                                Add NAT Map ("Easy-PAT List")

First Private Address:           192.168.1.1
Last Private Address:           192.168.1.5

Use NAT Public Range...

ADD NAT MAP                      CANCEL

```

Select **Use NAT Public Range** and from the pop-up menu choose **Static Range**. Select **ADD NAT MAP** and press Return.

This will statically map the first five public IP addresses to the first five corresponding private IP addresses and will map 206.1.1.6 to the remaining private IP addresses using PAT.

Notes on the example

The Easy-Map List and the Easy-PAT List are attached to any new Connection Profile by default. If you want to use this NAT configuration on a previously defined Connection Profile then you need to *bind* the Map List to the profile. You do this through either the NAT Associations screen or the profile's configuration screens.

The PAT part of this example setup will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to *initiate* traffic flow to the outside world (for example, the Internet). No one on the Internet would be able to initiate a conversation with them.

The Static mapping part of this example will allow any of the machines in the range of addresses from 192.168.1.1 through 192.168.1.5 to communicate with the outside world as if they were at the addresses 206.1.1.1 through 206.1.1.5, respectively. It also allows any machine on the Internet to access any service (port) on any of these five machines.

You may decide this poses a security risk. You may decide that anyone can have complete access to your FTP server, but not to your router, and only limited access to the desired services (ports) on the Web and Mail servers.

To make these changes, first limit the range of remapped addresses on the Static Map and then edit the default Server List called Easy-Servers.

- First, navigate to the **Show/Change Map List** screen, select **Easy-PAT List** and then **Show/Change Maps**. Choose the **Static Map** you created and change the **First Private Address** from 192.168.1.1 to 192.168.1.4. Now the router, Web, and Mail servers' IP addresses are no longer included in the range of static mappings and are therefore no longer accessible to the outside world. Users on the Internet will not be able to telnet, web, SNMP or ping to them. It is best also to navigate to the public range screen and change the **Static Range** to go from 206.1.1.5.
- Next, navigate to **Show/Change Server List** and select **Easy-Servers** and then **Add Server**. You should export both the Web (www-http) and Mail (smtp) ports to one of the now free public addresses. Select **Service...** and from the resulting pop-up menu select **www-http**. In the resulting screen enter your Web server's address, 192.168.1.2 and the public address, for example, 206.1.1.2 and then select **ADD NAT SERVER**. Now return to **Add Server**, choose the **smtp** port and enter 192.168.1.3, your Mail server's IP address for the **Server Private IP Address**. You can decide if you want to present both your Web and Mail services as being on the same public address, 206.1.1.2, or if you prefer to have your Mail server appear to be at a different IP address, 206.1.1.3. For the sake of this example, alias both services to 206.1.1.2.

Now, as before, the PAT configuration will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to initiate traffic flow to the Internet. Someone at the FTP server can access the Internet and the Internet can access all services of the FTP machine as if it were at 206.1.1.5. The router cannot directly communicate with the outside world. The only communication between the Web server and the Internet is through port 80, the web port, as if the server were located on a machine at IP address 206.1.1.2. Similarly, the only communication with the Mail server is through port 25, the SMTP port, as if it were located at IP address 206.1.1.2.

Firmware Upgrades and NAT

If you are upgrading from an earlier firmware version, your previous NAT configuration will continue to work as you have configured it.

A NAT map list, and possibly a server list, will be created for each enabled profile that has NAT enabled. For each profile with a unique local WAN IP address, a single outside PAT public range will be created whose address is the profile's local WAN IP address. A map list will be created with as many maps as there are enabled subnets on the ethernet. Each of these maps will bind each subnet to the outside public range.

Likewise, if exports exist, a server list will be created for each NAT-enabled Connection Profile with a unique local WAN IP address that maps the interior server address and port to the local WAN IP address of the profile.

Both the map list and server list that applies to the particular profile will be bound to that profile.

Chapter 17

Connection Metering

Introduced in version 4.3.2, the firmware offers system-wide and per-Connection Profile enhanced connection metering and budgeting. You use this feature to track first minutes (an ISDN tariff factor) and additional minutes or megabytes per time period for initiated data and voice calls, either through the Web-based management pages or the console-based management screens.

Web-based management pages

The Web-based management pages replace the SmartView monitoring tool and add significant new features for managing your router.

You access the Web-based management pages by launching your Web browser and entering the URL:

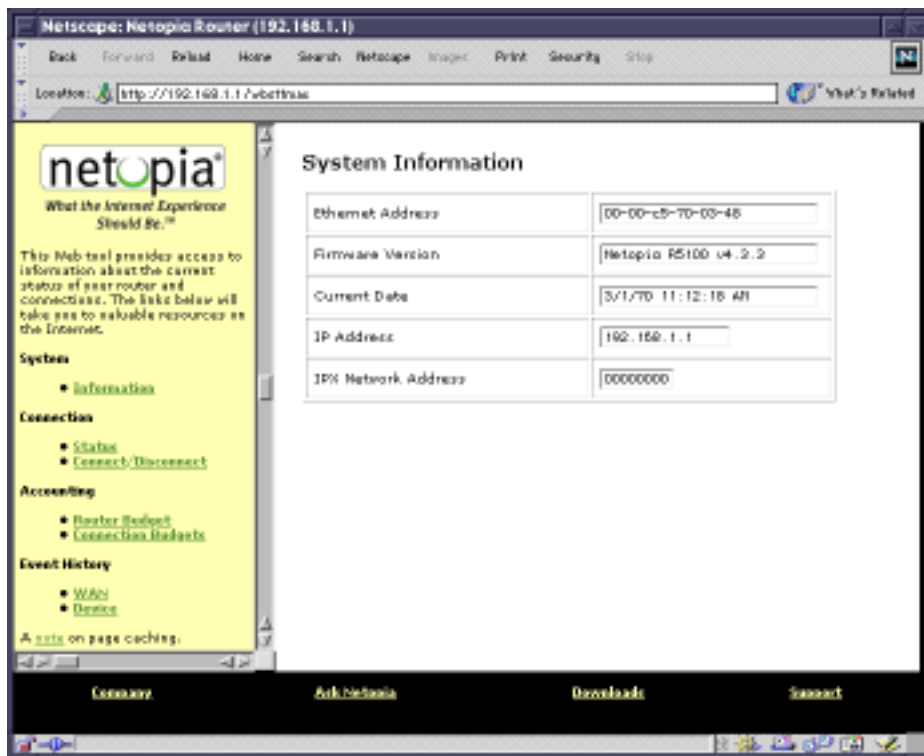
`http://router_IP_address`

where *router_IP_address* is the address of your router. The default address is 198.162.1.1.

The System Information page appears.

System Information page

This is the initial page you link to when you connect to the Web-based management pages.



It displays useful general information about your router:

Ethernet Address. The router's hardware or MAC address

Firmware Version. The router's model number and current firmware revision level

Current Date. The current date and time, as you have configured them

IP Address. The router's internal IP address

IPX Network Address. The router's IPX network address, if you have it enabled and are on an IPX network

The display contains two frames, a navigation frame on the left and the information and configuration page on the right.

The left frame permits you to navigate to:

- System
 - Information screen displays the router's hardware (MAC) address, the model number and firmware version currently installed, the current date and time, the router's IP address, and the IPX address, if any.
- Connection
 - "Frame Relay Statistics page" on page 17-4 (for frame relay configured devices only): displays a snap-

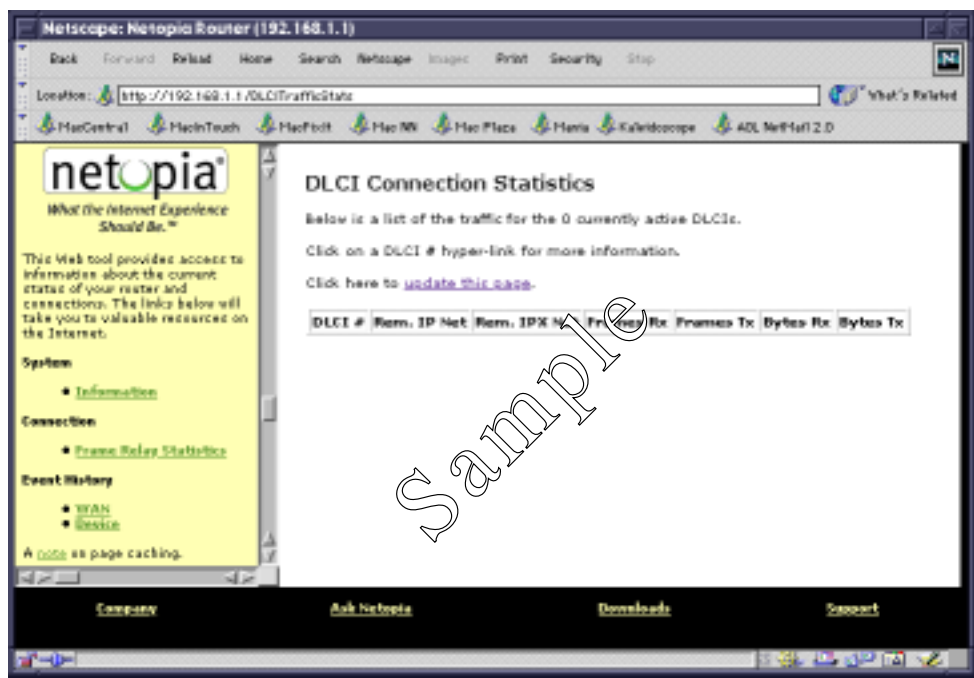
shot of the activity for your Frame relay DLCIs.

- [“Connection Status page” on page 17-5](#) (*for switched interfaces only*): displays the current state of your switched connection.
- [“Connect/Disconnect page” on page 17-6](#) (*for switched interfaces only*): displays a list of your Connection Profiles, allowing you to initiate connections using any one of them.
- Accounting (*for switched interfaces only*)
If you have a leased line with an unswitched interface, these options do not appear.
 - [“Router Budget Configuration page” on page 17-7](#): allows you to display and edit your aggregate connection accounting statistics and limits.
 - [“Connection Budgets page” on page 17-8](#): allows you to set up and track three connection budgets for cost control purposes.
- Event History
 - [“WAN Event History page” on page 17-11](#): displays the most recent events that the router reports for your WAN connections.
 - [“Device Event History page” on page 17-12](#): displays the most recent events that the router reports of its own internal activity.

If you click any link in the left frame, that page is displayed in the right frame.

Frame Relay Statistics page

For leased line connections, the Frame Relay Statistics page displays a snapshot of the activity for your Frame Relay DLCIs.



The table gives the following information:

DLCIs In Use: The number of Frame Relay DLCIs being used, if any.

DLCI #. The DLCI number as you have configured it.

Rem. IP Net. The remote IP network address.

Rem. IPX Net. The remote IPX network address, if any.

Frames Rx: The number of frames received.

Frames Tx: The number of frames transmitted.

Bytes Rx: The number of bytes received.

Bytes Tx: The number of bytes transmitted.

To update the information displayed, click the **update this page** link.

Connection Status page

For switched interface connections, the Connection Status page displays information for your active Connection Profile and, if applicable, any POTS calls currently active.



The table gives the following information:

Profile. The name you have assigned to the Connection Profile that is currently connected.

Rate. The data rate of this connection.

% Usage. The average percent use of the maximum capacity of the channels in use for the connection.

Established by. Whether the connection was locally ("Lcl") or remotely ("Rmt") established.

Remote IP Address. The address of the connection on the remote end.

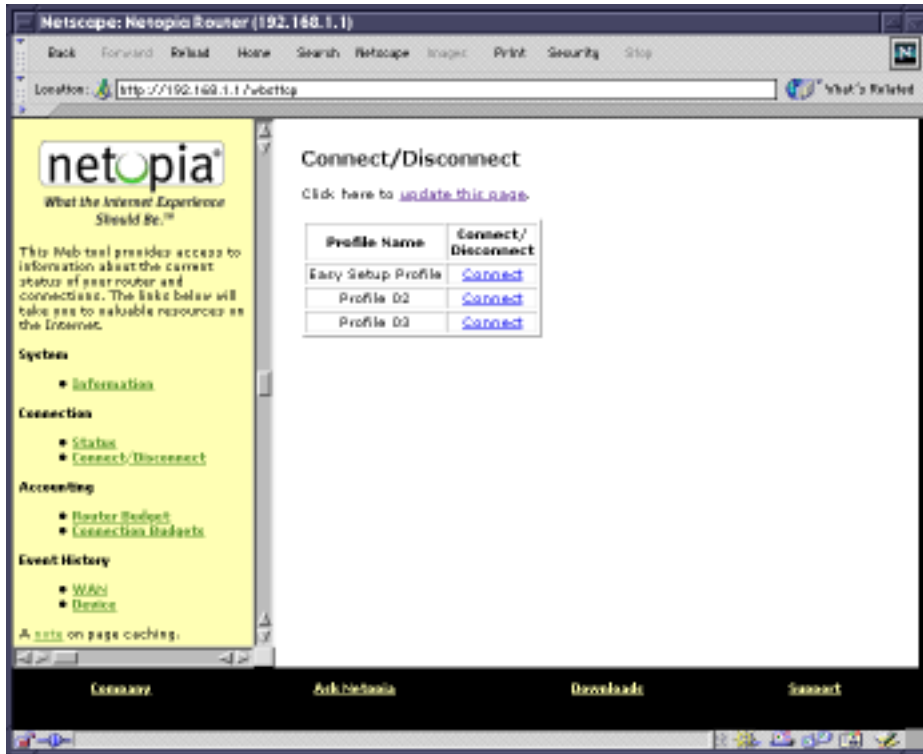
Remote IPX Network. If you are routing IPX traffic, the address of the remote IPX source.

More Info: In order of priority, the NAT address in use for this connection, the IPX address in use (if IP is also in use), or the ISDN caller identification (if available).

To update the information displayed, click the **update this table** link.

Connect/Disconnect page

The Connect/Disconnect page displays a list of your configured Connection Profiles and allows you to connect or disconnect any of them.

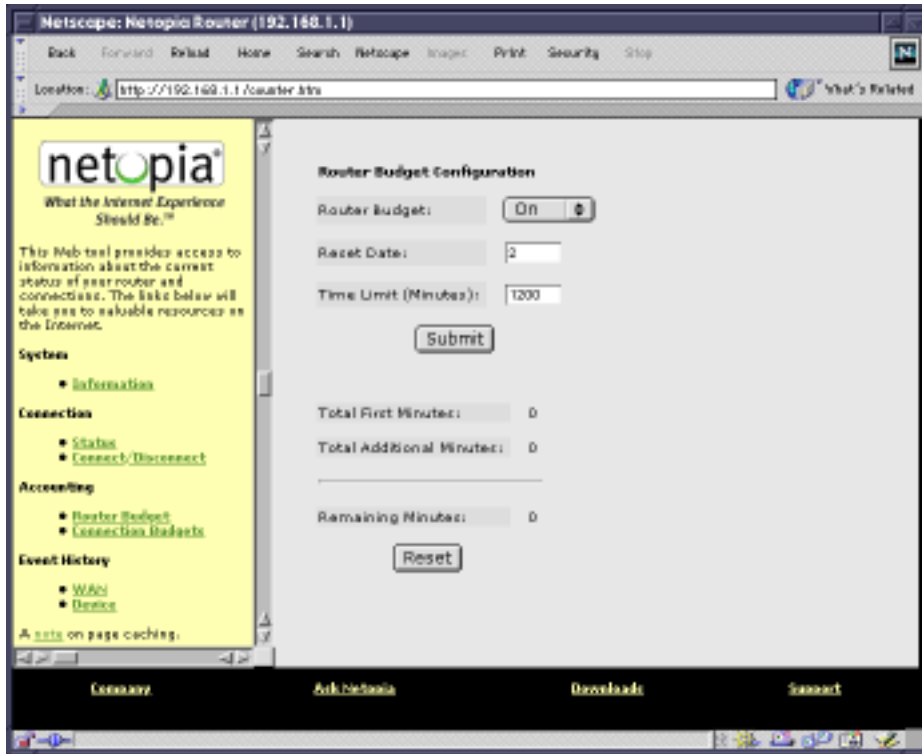


To initiate a connection using any of the displayed Connection Profiles, simply click the **Connect** link.

To disconnect from an active Connection Profile, click the **Disconnect** link.

Router Budget Configuration page

The Router Budget Configuration page allows you to modify the parameters for your overall connection accounting policy.



From this page you can:

- turn **Router Budget** either **On** or **Off** from the pull-down menu
- change the **Reset Date** (day) on which the counters begin counting again
- change the total aggregate **Time Limit** in minutes covered by all of your budgets

If you make any changes in this screen, click the **Submit** button.

To reset the aggregate minute counters to zero again, click the **Reset** button.

The table displays the following information:

Total First Minutes. The number of first minutes of outbound calls to be placed during the recording interval for all your configured budgets

Total Additional Minutes. The total time of all outbound calls to be placed during the recording interval for all your configured budgets

Remaining Minutes. The time remaining during the recording interval for all your configured budgets

Connection Budgets page

The Connection Budgets page displays information for three budgets or Connection Profiles for tracking and controlling connection usage on a per-Connection Profile basis.

netopia
What the Internet Experience Should Be.™

This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- [Information](#)

Connection

- [Status](#)
- [Connect/Disconnect](#)

Accounting

- [Router Budget](#)
- [Connection Budgets](#)

Event History

- [WAN](#)
- [Router](#)

A note on page caching.

Connection Budgets

	Connection Profile	Status	Enforced	Limit	Units	Time Period	Period Start	Options
Budget 1	Easy Setup Profile		x	1200	Minutes	Weekly	Monday	Edit Show Statistics
Budget 2	Profile 02		x	120	Minutes	Weekly	Tuesday	Edit Show Statistics
Budget 3	Profile 03		x	120	Minutes	Monthly	1	Edit Show Statistics

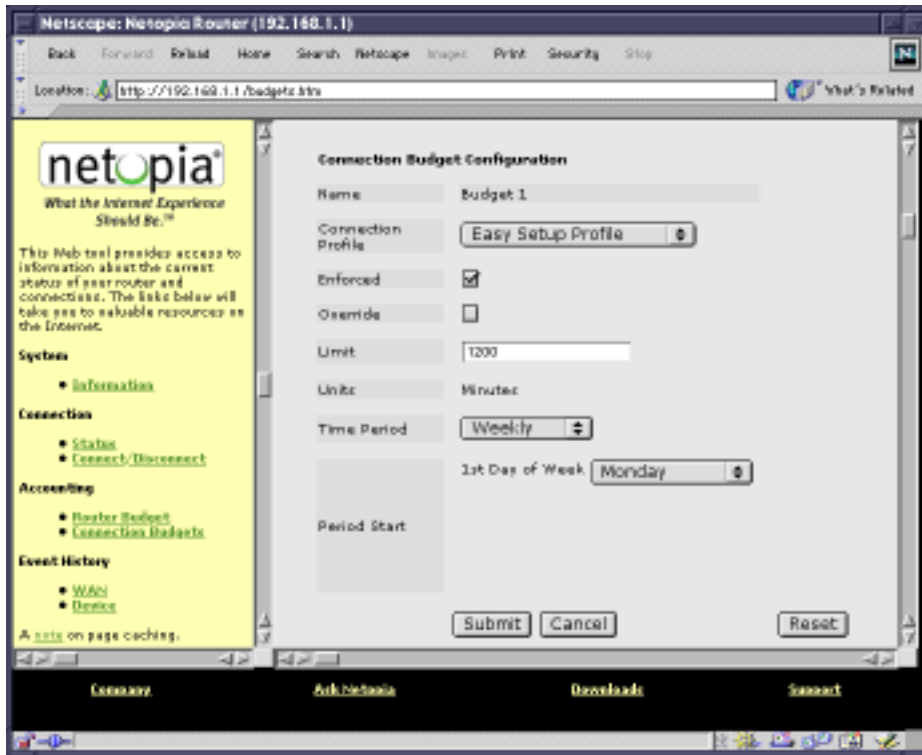
[Company](#) [Ask Netopia](#) [Downloads](#) [Support](#)

The status of your Connection Budgets is summarized on this page.

You configure your budgets in the Budget Configuration page. To configure a budget, click the **Edit** link for that budget. The [Connection Budget Configuration page](#) appears. (See [page 17-9](#).)

To view the statistics for each budget, click the **Show Statistics** link. The [Budget Statistics page](#) appears. (See [page 17-10](#).)

Connection Budget Configuration page



You can configure budgets to be:

- **Enforced**, meaning that when you reach the usage limit for the assigned time period, the Connection Profile will allow no more connections. If the budget is not enforced, the system will merely keep track of its usage. To enforce this budget, check the **Enforced** checkbox.
- in **Override** mode. Checking this option allows you to exceed your budget during the current time period without tearing down active connections. At the end of the current time period this option is automatically deactivated. If you want to be able to exceed your enforced budget again, you must check this option for each new time period.

Checking **Override** disables call blocking, even if the call is over its limit. The override flag is automatically reset to be off at the start of a new period. This is so that you don't need to disable **Enforced** to by-pass the limit and or remember to turn it back on when the new period starts.

- set to a predefined **Limit** of minutes of usage
- set to the **Time Period**, weekly or monthly, that you specify for your own budgeting requirements
- started on a specific day of the week or month by selecting the day you want to start from the pull-down menu. If you set a weekly schedule, you choose the day of the week to start it; if you set a monthly

schedule, you choose the day of the month to start it.

Click the **Submit** button to enable your entries and be returned to the Connection Budgets page or click the **Cancel** button to discard all your entries. Click the **Reset** button to reset all counters and archives to zero.

Budget Statistics page

netopia
What the Internet Experience Should Be.™

This Web tool provides access to information about the current status of your router and connections. The links below will take you to valuable resources on the Internet.

System

- [Information](#)

Connection

- [Status](#)
- [Connect/Disconnect](#)

Accounting

- [Router Budget](#)
- [Connection Budgets](#)

Event History

- [View](#)
- [Delete](#)

A note on page caching.

Budget Statistics

Budget Account: Format: Time Period: Options:

[Go to Budgets](#)

	Week to Date	Last Week	2 Weeks Ago	3 Weeks Ago
1st Minute	0	0	0	0
Additional Minutes	0	0	0	0
<hr/>				
Total	0	0	0	0
Budgeted	1440			
Remaining	1440			

[Company](#) [Ask Netopia](#) [Downloads](#) [Support](#)

You can view statistics for all of your budgets at once or one at a time.

- To view the statistics for a single budget or all enforced budgets, select the budget you want to view from the **Budget Account** pull-down menu.
- Select the **Format** you want to view, either **1st Minute/Additional Minutes** or **Channel 1/Channel 2**.
- Select the **Time Period** you want to view, either **Weekly** or **Monthly**.

The information display will immediately change to show the information you specified in the format you chose.

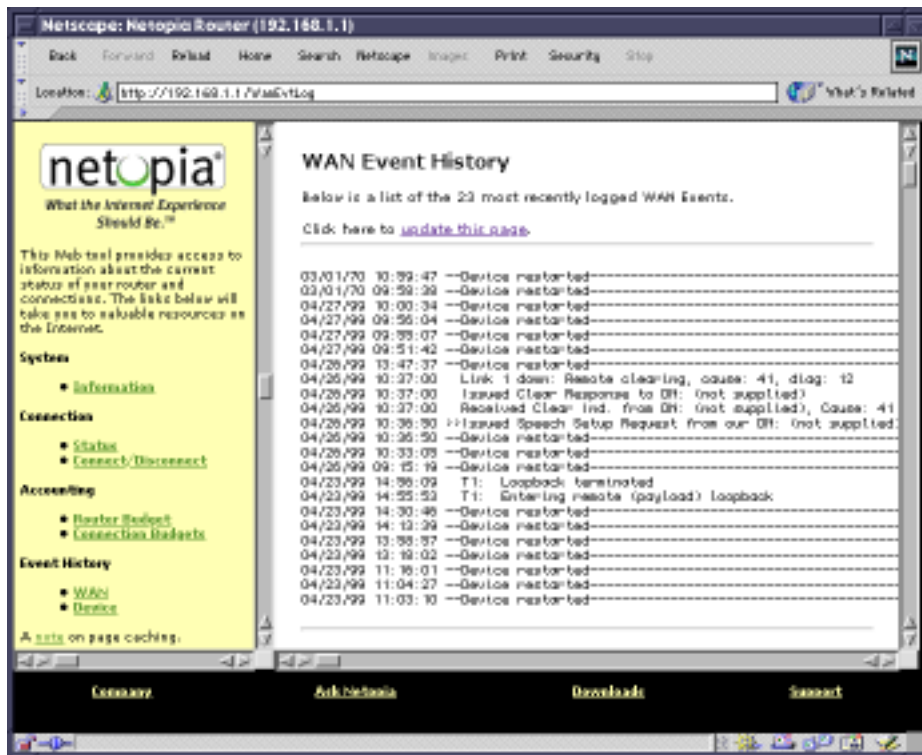
To return to the Connection Budgets page, click the **Go to Budgets** link.

Event History pages

The Netopia R-Series Routers record certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R-Series Routers' built-in battery backup prevents loss of event history from a shutdown or reset.

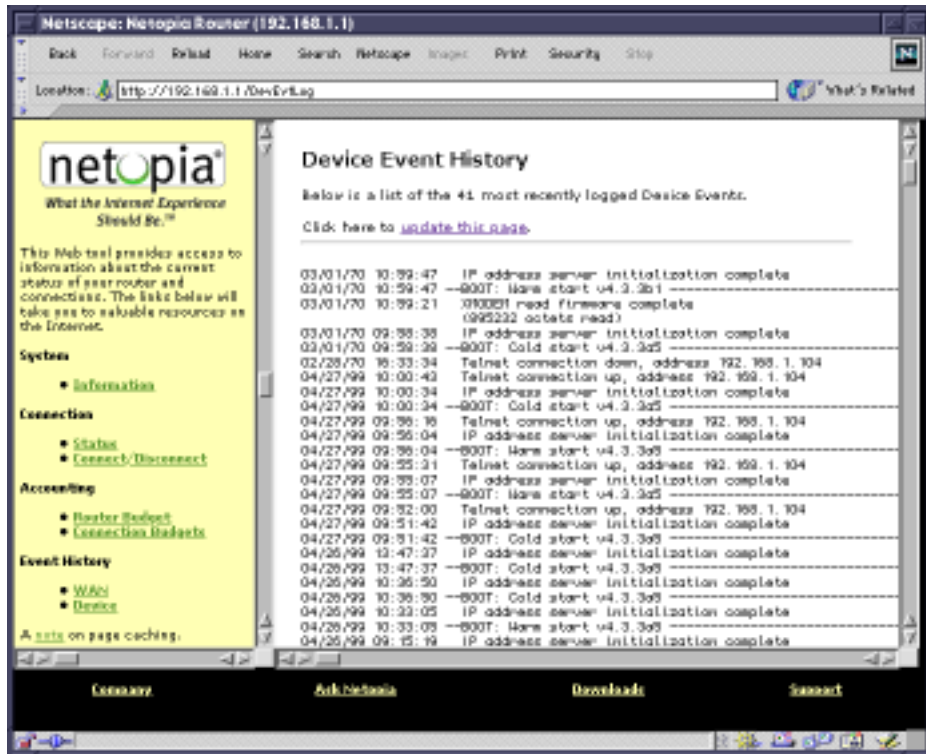
The router's event histories are structured to display the most recent events first and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History pages retain records of up to 128 of the most recent events.

WAN Event History page



You can refresh the WAN Event History log by clicking the **update this page** link.

Device Event History page

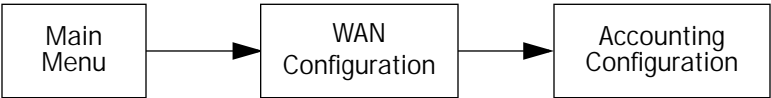


You can refresh the Device Event History log by clicking the **update this page** link.

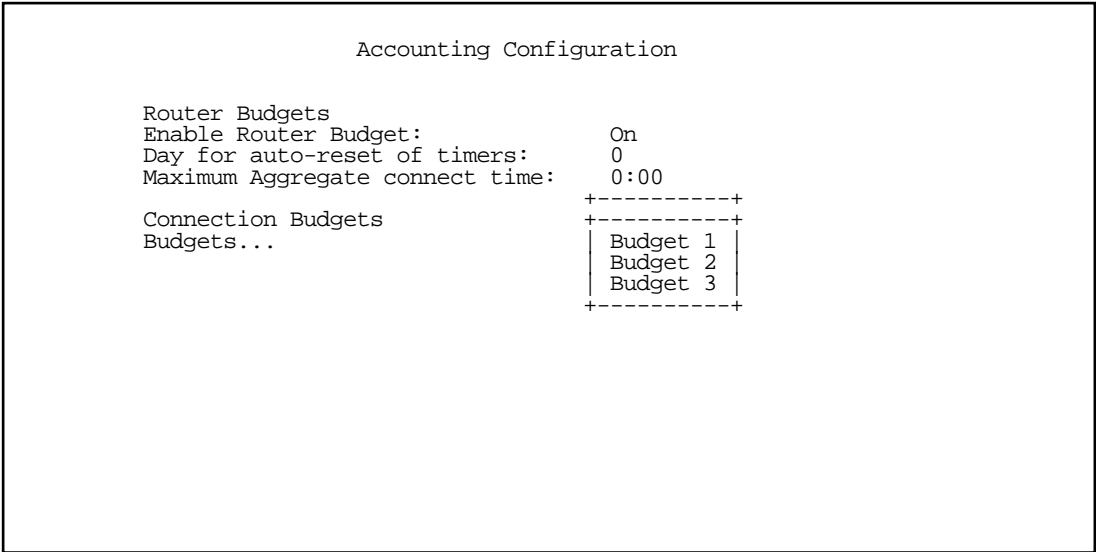
Console-based management screens

You access the console-based management screens either by running your Telnet application or your terminal emulator to the serial console. For details on how to do this, see the Console-based Management chapter in the *User's Reference Guide*.

Navigate to the Accounting screens.



The Accounting Configuration screen appears.



To edit your budgets select **Budgets**, and from the pop-up menu, select the budget you want to edit.

The Budget Setup screen appears.

Connection Budget Setup	
Name:	Budget 1
Use Connection Profile...	Easy Setup Profile
Enforced:	Off
Override:	Off
Units:	Minutes
Limit:	300
Time Period...	Week
1st Day of Week...	Sunday

Choose the Connection Profile this budget is for.

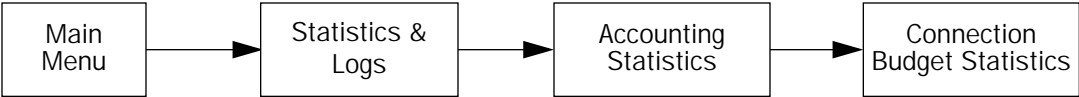
Configuration is similar to the Web-based management configuration screens.

- Selecting **Use Connection Profile** displays a pop-up list of all of your Connection Profiles. Choose the Connection Profile you want this budget to apply to and press Return.
- Toggle **Enforced** to either **On** or **Off** to enforce whether the connection is torn down when the budget limit is reached.
- Toggle **Override** to either **On** or **Off**. With Override on you can exceed your budget during the current time period without tearing down active connections. At the end of the current time period this option is automatically deactivated. If you want to be able to exceed your enforced budget again, you must toggle this option to On for each new time period.

Toggle **Override** to On disables call blocking, even if the call is over its limit. The override flag is automatically reset to be Off at the start of a new period. This is so that you don't need to disable **Enforced** to by-pass the limit or remember to turn it back on when the new period starts.

- The **Units** field is not editable.
- In the **Limit** field enter the number of minutes your budget allows.
- From the **Time Period** pop-up menu select either **Week** or **Month**, depending on your budgeting requirements.
- If you set the time period to Week, from the **1st Day of Week** pop-up menu select the day of the week on which your budget starts, or
if you set the time period to Month, from the **1st Day of Month** pop-up menu select the day of the month on which your budget starts.

You can monitor your usage against your budget by reviewing the Connection Budget Statistics screen in the Accounting Statistics. From the Main Menu navigate to the Connection Budget Statistics screen.



The Budget Statistics screen appears.

Budget Statistics (in HHHH:MM)					
Budget	Name-----	First Minutes----	Additional Minutes-----	Cutoff--	Expired
Budget 1		0:00	0:00	2:00	
Budget 2		0:00	0:00	5:00	
Budget 3		0:00	0:00	10:00	

You can view statistics for all your budgets at once or one at a time.

- **Budget Name** shows the names of your budgets.
- **First Minutes** displays the number of first minutes of outbound calls placed during the recording interval.
- **Additional Minutes** displays the remaining time of all outbound calls placed during the recording interval.
- **Cutoff** displays the number of hours budgeted for this Connection Profile.
- **Expired** displays the amount of time used against the budgeted amount.

To clear the counters and reset the statistics, use the down arrow key to select a budget and press Return. A pop-up window will ask you to confirm that you want to clear this budget’s statistics. You can cancel if you change your mind.

To return to the Accounting Statistics screen, press Escape.

Date and time setting

Note: If you have Connection Budgets configured, changing the date setting will reset the Connection Budgets under one of the following conditions:

- If the new date is greater than the old date and the new date falls outside of the current budget window; or
- If the new date is in the past and the date is not the current date (i.e., yesterday or earlier).

A warning message is displayed in the console window when a budget is reset.

See the *User's Reference Guide* for more information on setting the date and time.

Chapter 18

R5300-Series T1 Router Feature Enhancements

The version 4.10 firmware includes the following new T1 router features:

- PPP in Frame Relay (RFC1973) support on the R5300-Series T1 router family.
- The ability to select Normal vs. Copper Mountain operation via an Operation Mode pop-up menu.
- Management LED indication of locally or remotely initiated Line Loop Back (LLB) or Payload Loop Back (PLB).
- Command Line Interface support for configuration, monitoring, and diagnostics. See the *Netopia™ R-Series Routers Command Line Interface Commands Reference, Firmware version 4.9* for more information.

T1 Line Configuration

The version 4.10 firmware provides the ability to configure PPP in Frame Relay (RFC1973) on the R5300-Series T1 router family. This feature allows a PPP connection to be established over a Frame Relay permanent virtual circuit (PVC). The Netopia router firmware supports a single virtual circuit when the circuit is configured for RFC1973 encapsulation.

Certain R5300-Series router behavior must be customized in order to interoperate with a Copper Mountain DSLAM. When connected to a Copper Mountain DSLAM, the Copper Mountain Control Protocol (CMCP) must be enabled.

The version 4.10 firmware offers an Operation Mode pop-up menu on the T1 Line Configuration screen. This pop-up menu allows you to select whether or not the R5300 is connected to a Copper Mountain DSLAM.

The T1 Line Configuration screen offers three menu items required to configure PPP in Frame Relay:

T1 Line Conf	
Operation Mode...	Normal
Line Encoding...	Copper Mountain
Framing Mode...	
Transmit ANSI PRMs:	No
Number of DS0 Channels:	1
First DS0 Channel:	1
Buildout (-dB)...	0-0.6
Channel Data Rate...	Nx64k
Clock Source...	Network
Data Link Encapsulation...	Frame Relay
PPP over Frame Relay Enabled:	On
DLCI:	16
LMI:	None

- The **Operation Mode** pop-up menu allows you to select between the Normal mode of operation (the default) and the Copper Mountain mode of operation.
In the Copper Mountain mode, Copper Mountain Control Protocol (CMCP) is enabled.
- The balance of the Frame Relay configuration is identical to the corresponding configuration for other Netopia R-Series routers. For more information on PPP over Frame Relay, refer to the chapter “PPP over Frame Relay for R3100 and R7100 Routers” in the *Netopia™ D- and R-Series Equipment Firmware Addendum* on your Netopia CD.

The Easy Setup T1 Line Configuration screen also offers the same PPP over Frame Relay configuration options.

T1 Line Configuration	
Operation Mode...	Normal
Line Encoding...	B8ZS
Framing Mode...	ESF
Number of DS0 Channels:	1
First DS0 Channel:	1
Channel Data Rate...	Nx64k
Data Link Encapsulation...	Frame Relay
PPP over Frame Relay Enabled:	On
DLCI:	16
LMI:	None
TO MAIN MENU	NEXT SCREEN

Enter Information supplied to you by your telephone company.

Management LED Indication of Local/Remote Loopback and Blue Alarm States

The R5300-Series router will light the management LED solid yellow whenever it is in the Line Loop Back (LLB) or Payload Loop Back (PLB) state, regardless of whether the loopback was requested locally from the router or initiated by the remote end.

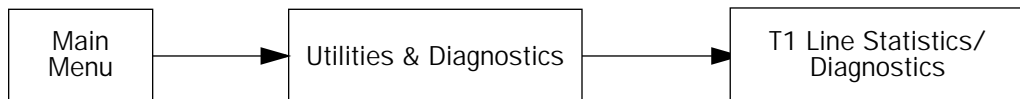
T1 Diagnostics for R5300 Routers

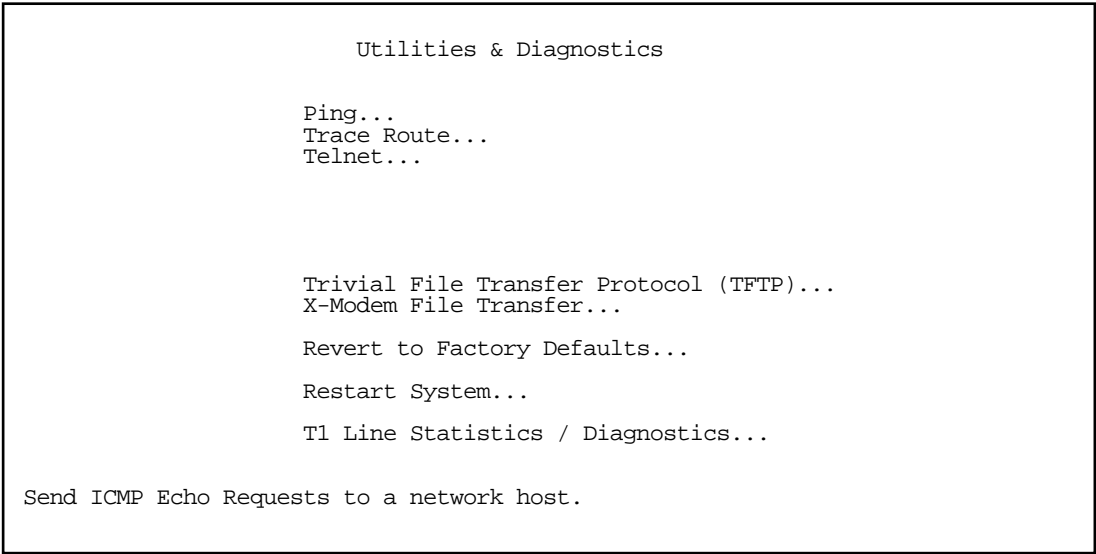
Introduced in version 4.3.2, the firmware offers T1 Line Statistics and Diagnostics for leased line routers.

T1 Line Statistics and Diagnostics screen

The Utilities and Diagnostics menu (see the *User's Reference Guide* section on Utilities and Diagnostics) includes an option for displaying T1 line statistics.

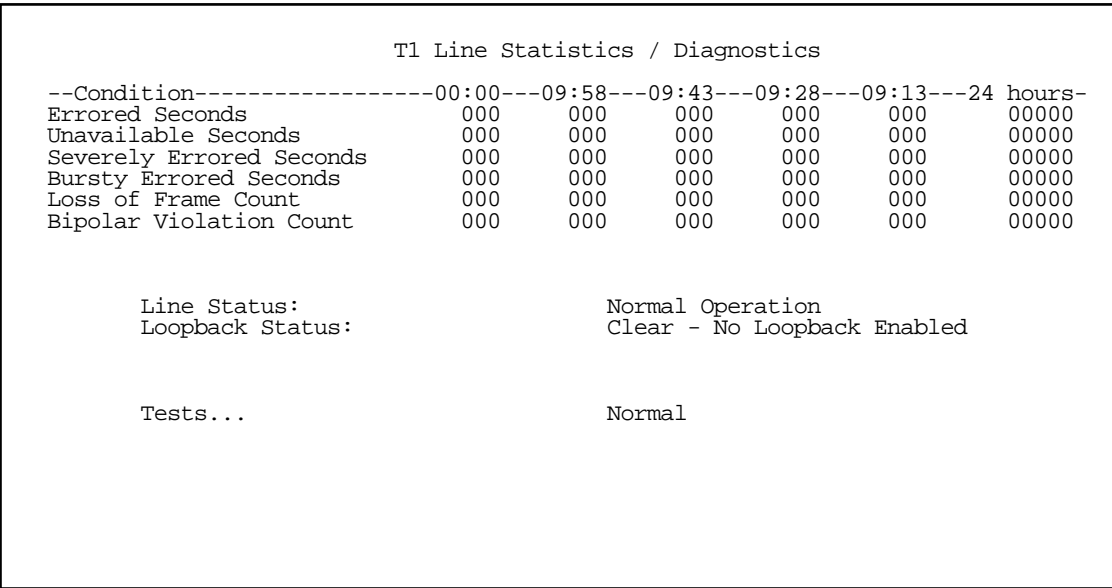
You access the Utilities and Diagnostics menu from the Main Menu.





Select **T1 Line Statistics / Diagnostics** and press Return.

The T1 Line Statistics / Diagnostics screen appears.



The screen displays the current condition of tests that you run. The counters display the occurrences of the indicated events in fifteen-minute increments, shifting the totals to the column to the right after each fifteen minute cycle until the total is accumulated in the **24 hours** column.

Condition: Displays the parameters tested.

Time columns: Current time (00:00) starts at zero and resets to zero at 15:00 minutes, shifting the counted total to the next column to its right.

24 hours: Cumulative statistics, for the preceding 24-hour period.

Line Status: Conditions may be Normal Operation, Red Alarm, Yellow Alarm, or (Rmt/Lcl) LoopBack

Loopback Status: Current loopback condition

Tests: Offers a pop-up menu with the following options:

- **Normal - Clear Loopback** clears any local loopbacks and sends an ANSI PLB clear to the remote CSU. This returns the Netopia Router to its normal state if any testing has been done and the router has been put into a looped state. Select this option after running tests to return the router to a normal state so that it is capable of passing traffic as it should.
- **Send Blue Alarm -all 1s** forces an error condition of all 1s; remote will send a yellow alarm if enabled. You can use this pattern in two different ways. Once a remote router has been looped you can use it to verify that you are receiving the same data that you are sending. For example, if you send all ones across the line and get back a mixture of ones and zeroes, there is a problem. You can also use this test in a different way. If you send all ones to a remote device, it should report that it is receiving all ones. This would verify (without having to put up a loop) that data is reaching the destination intact. It does not verify bi-directional integrity however, which is verified if you have the remote end in loop. This pattern is also for checking the remote end's capability of reporting back a yellow alarm (usually something that is optionally enabled on the remote CSU).
- **Remote Payload Loopback** sends an ANSI BPM payload loopback request to the remote CSU. This pattern tells the remote device (usually the CSU at the other end of the circuit) that it should go into a looped state. Use this pattern for putting up a loop to do testing from a remote portion of the circuit, either by the Telco or by the CPE at the remote end of the circuit. This test makes the remote CSU go into a looped state so that any data you send it is returned to you. This is useful for determining if the remote CSU is receiving data from the CPE. If it does not loop then you can conclude that it is not receiving any data from you.
- **Local Payload Loopback** enables a local payload loopback. This pattern is similar to the Remote Payload Loopback pattern except that it puts the local CSU into a looped state rather than the remote CSU. This is useful if the remote side is not able to send a remote loop code to the router to put it into a looped state. You can simply put it into loopback manually and see if that loop is reflected at the remote side.
- **Loopback Pattern Test** sends continuous 1200 byte packets and compares incoming packets (similar to ISDN loopback tests), counting good and bad packets. Twenty consecutive good packets are required to PASS. The loopback testing screen is only visible when this test is selected. It sends a pseudo-random sequence that is intended to simulate data so that you can check for errors on the circuit. This test requires that the remote CSU be in a payload loopback condition. (It will partially work if the remote CSU is in a LINE loopback condition as well, but this is less reliable.)

When you select one of these tests and press Return, the test runs and the screen provides feedback.

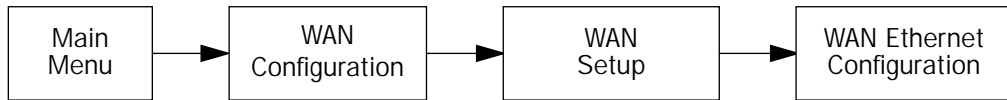
Chapter 19

Configurable Hardware (MAC) Address for R9100 Routers

For R9100 Ethernet-to-Ethernet routers, the firmware offers the capability of configuring an arbitrary hardware (MAC) address on the Ethernet WAN port. The reason you may want to take advantage of this feature is that some ISPs authenticate your connection by assigning your account to a particular hardware address. This address is not normally configurable because it uniquely identifies a particular Ethernet device, such as a Network Interface Card (NIC). Many ISPs supply a NIC as part of their DSL installation package and then identify your account by means of the MAC address when you connect.

If your account is so identified, you can configure the required MAC address on the Ethernet WAN port of your R9100 router. When connected to your DSL modem, the R9100 then appears the same as a NIC supplied by your ISP.

To configure your R9100 Ethernet MAC address, navigate to the WAN Ethernet Configuration screen in the console menu.



The WAN Ethernet Configuration screen appears.

WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
Filter Set...	
Remove Filter Set	
Receive RIP:	Both
Wan Ethernet MAC Address:	00:00:c5:70:03:4a
Aux Serial Port...	Async Modem
Data Rate (kbps)...	57.6
Aux Modem Init String:	AT&F&C1&D2E0S0=1

Set up the basic IP attributes of your Ethernet Module in this screen.

19-2 Firmware Version 4.10 Addendum

The WAN Ethernet MAC Address field is editable. Use the down arrow key to navigate to this field and enter the MAC address you want to use for your router's connection. Press Return. The new MAC address will be enabled.

Chapter 20

New R7100 SDSL Router Features

Introduced in version 4.4, the current firmware release contains new features and feature enhancements for R7100 SDSL Routers. Each feature is covered in its own section:

- “PPP over SDSL for R7100 Routers” on page 20-1
- “Priority Queuing for R7100 Routers” on page 20-4

PPP over SDSL for R7100 Routers

Netopia R7100 routers offer PPP data link encapsulation over the SDSL link. Two screens display this option: the Easy Setup SDSL Line Configuration screen and the SDSL Line Configuration screen under the WAN Configuration menu. Also, the option for Copper Mountain-compatible SDSL is changed from ATM FUNI, as shown in earlier firmware versions, to RFC1483.

- To access the Easy Setup SDSL Line Configuration screen from the console Main Menu select **Easy Setup** and press Return.



The SDSL Line Configuration screen appears.

SDSL Line Configuration

Data Link Encapsulation...

PPP
 Frame Relay
 RFC1483

TO MAIN MENU

NEXT SCREEN

From the **Data Link Encapsulation** pop-up menu, you can now choose **PPP**, **Frame Relay**, or **RFC1483**. If you choose PPP data link encapsulation, you are also offered the option of storing your user name and password for PPP authentication. You do this in the Easy Setup Profile screen. In the SDSL Line Configuration screen select **NEXT SCREEN** and press Return.

The Easy Setup Profile screen appears.

Connection Profile 1: Easy Setup Profile

Address Translation Enabled:

Yes

Local WAN IP Address:

0.0.0.0

Remote IP Address:

+-----+

Remote IP Mask:

+-----+

PPP Authentication...

None

Send User Name:

PAP

Send Password:

CHAP

PAP-TOKEN

CACHE-TOKEN

+-----+

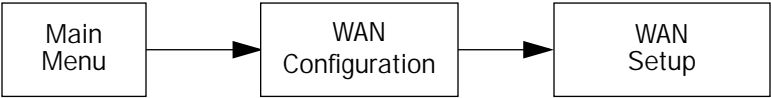
PREVIOUS SCREEN

NEXT SCREEN

PAP-- Password protection is used. Passwords are exchanged in clear text.

For PPP Authentication, you can choose any of the options shown above. If you choose any authentication method other than None, you can enter either **Send User Name** and **Password** (for PAP, PAP-TOKEN, or CACHE-TOKEN) or **Send Host Name** and **Secret** (for CHAP).

- To access the SDSL Line Configuration screen from the console Main Menu select **WAN Configuration**, then **WAN Setup**, and press Return.



The SDSL Line Configuration screen appears.

SDSL Line Configuration	
Clock Source...	Network
Data Link Encapsulation...	<div style="border: 1px dashed black; padding: 2px;"> PPP Frame Relay RFC1483 </div>
Prioritize Delay-Sensitive Data:	
Aux Serial Port...	Async Modem
Data Rate (kbps)...	57.6
Aux Modem Init String:	AT&F&C1&D2E0S0=1

From the **Data Link Encapsulation** pop-up menu, you can now choose **PPP**, **Frame Relay**, or **RFC1483**.

If you choose PPP data link encapsulation, you must create a Connection Profile to store your PPP authentication information, if any. See the *User's Reference Guide* for information on creating a new Connection Profile.

When you create a new Connection Profile, you store your user name and password information in the Data Link Options screen under the Add Connection Profile menu.

Datalink (PPP/MP) Options	
Data Compression...	
Send Authentication...	<div style="border: 1px dashed black; padding: 2px;"> None PAP CHAP PAP-TOKEN CACHE-TOKEN </div>
Send User Name:	
Send Password:	
Receive User Name:	
Receive Password:	
Maximum Packet Size:	1500
PAP-- Password protection is used. Passwords are exchanged in clear text.	

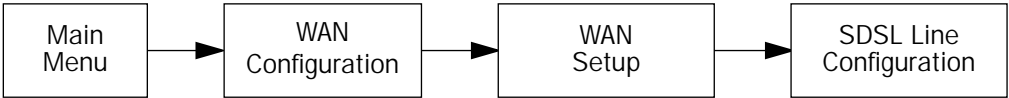
For PPP Authentication, you can choose any of the options shown above. If you choose any authentication method other than None, you can enter either **Send User Name** and **Password** (for PAP, PAP-TOKEN, or CACHE-TOKEN) or **Send Host Name** and **Secret** (for CHAP).

Priority Queuing for R7100 Routers

Netopia R7100 Routers offer the ability to prioritize delay-sensitive data over the SDSL link.

Certain types of IP packets, such as voice or multimedia packets, are sensitive to latency introduced by the network. This means that if such packets are not received rapidly, the quality of service degrades. If you expect to route significant amounts of such traffic you can configure your router to prioritize this type of traffic using the priority queuing feature.

To configure your R7100 router to prioritize delay-sensitive data, navigate to the SDSL Line Configuration screen in the console menu.



The SDSL Line Configuration screen appears.

SDSL Line Configuration

Clock Source...	Network
Data Link Encapsulation...	REC1483
Prioritize Delay-Sensitive Data:	No
Aux Serial Port...	Async Modem
Data Rate (kbps)...	57.6
Aux Modem Init String:	AT&F&C1&D2E0S0=1

Enter Information supplied to you by your telephone company.

The R7100 Router will recognize a delay-sensitive packet as having the low-latency bit set in the TOS field of the IP header.

If you toggle **Prioritize Delay-Sensitive Data** to **Yes** the router will place these packets at the front of the transmission queue to the SDSL link, overtaking non-delay-sensitive traffic. Accepting the default **No** will allow the normal sequential queue of data packets.

Chapter 21

Miscellaneous Notes

DNS Proxy and Caching Behavior

DNS Proxying is a standard Netopia router feature. This feature operates transparently with no configuration required.

If the Netopia router's DNS is 0.0.0.0 the router serves itself as the DNS to DHCP client workstations that are configured to acquire their IP addresses dynamically. If the router obtains a valid DNS supplied by the ISP, it does one of two things:

- either it forwards all DNS requests it receives to its DNS and remaps them when the response is received, or
- it constructs a DNS response if it finds the mapping in its own DNS cache.

This ensures that DHCP clients of the Netopia router will be able to use DNS as soon as the Netopia router is able to do so.

If the Netopia router is rebooted in a state wherein its DNS is non-zero, then the router will thereafter seed its DHCP clients with the router's DNS.

Beginning with firmware version 4.8 the only devices that can make use of DNS proxy are those whose addresses are acquired from the router via DHCP.

SNMP Community String Defaults

Beginning with the 4.3.8, 4.4.1, and 4.5 firmware releases, the default SNMP **Read/Write Community String** is now the empty string, which disables SNMP Set Request access to the router. Easy Setup does not change the **Read/Write Community** to match the password created as part of Easy Setup. You must go to the SNMP menu under the System Configuration menu to set a **Read/Write Community String** to enable Set Request access to the router.

The default **Read-Only Community String** remains "public".

16 Filter Rule Limitation Change

Beginning with firmware version 4.3.2, you can create up to 255 filter rules. You can use them in any combination of input or output in up to eight filter sets.

Correction to Filtering Documentation

This section corrects an error in the *User's Reference Guide* Security Chapter, filter set explanation. The R-3100 manual on Security, page 13-7, incorrectly shows the input filter setup to compare on src port rather than dest port to block incoming Telnet attempts. A few pages later, page 13-9, shows it correctly as a dest prt compare.

“Security, page 13-7, A filtering rule

Block all Telnet attempts that originate from the remote host 199.211.211.17. This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.”

Here is what this rule looks like when implemented as a filter on the Netopia R3100:

+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+									
+-----+-----+-----+-----+-----+-----+-----+-----+									
1	199.211.211.17	0.0.0.0		TCP	0		23	Yes	No
+-----+-----+-----+-----+-----+-----+-----+-----+									

Index

A

- accounting configuration 17-13
- ATMP 14-8
 - tunnel options 14-18

B

- backup, line 12-1
- budget statistics 17-15

C

- CompuServe Login Protocol 3-1
- connection metering 17-1

D

- Data Encryption Standard (DES) 14-8
- delayed configuration 10-6
- DES 15-1
- DHCP Lease 10-8
- DHCP Relay Agent 13-7
- diagnostics
 - T1 18-3

- DNS Proxying 21-1
- DNS resolution 10-1
- DSL bonding 11-2

E

- encryption 14-8, 15-1

H

- hardware (MAC) address 19-1

I

- ICMP Type and Code filtering 10-2
- IKE 15-1
- IMUX 11-1, 11-6
- Internet Key Exchange 15-1
- Internet Key Exchange (IKE) 15-1
- Inverse multiplexing 11-2
- IPCP 10-1
- IPsec 1-3, 15-1

L

- LAN-side filtering 7-1
- latency 20-4
- lease times 10-8
- line backup 12-1
 - backup IP gateway 12-8
 - connection profiles 12-9
 - management and statistics 12-11
 - scheduled connections 12-9
 - supported routers 12-2
 - WAN configuration 12-3

LLC/SNAP 6-4
LMI 4-16, 10-9

M

MAC address 19-1
MPPE 14-8
MS-CHAPv2 14-9
Multilink PPP 11-6

N

NAT
 adding server lists 16-18
 Easy Setup Profile 16-7
 firmware upgrades 16-37
 IP profile parameters 16-24
 IP setup 16-9
 map lists 16-10
 modifying map lists 16-14
 moving maps 16-16
 outside ranges 16-10
 server lists 16-10
Nokia EOC Fast 6-1
Nokia Fixed 6-1

O

Operation Mode 6-2

P

password confirmation 10-4
PAT (Port Address Translation) 16-2
permanent virtual circuit 4-6, 5-1
PPP over Ethernet 9-1
PPP over Frame Relay 8-1
PPP over SDSL 20-1
PPPoE 9-1
PPTP 14-8
 tunnel options 14-4
priority queuing 20-4
PVC 4-6, 5-1

Q

quality of service 20-4

S

Security Policy Database (SPD) 15-2
static routes 10-1
strong encryption 14-9

T

T1 diagnostics 18-3
troubleshooting
 event histories 17-11
tunnel options
 ATMP 14-18
 PPTP 14-4
tunneling 14-2

U

user-definable lease times 10-8

V

Virtual Path Identifier (VPI) 6-3
Virtual Private Networks (VPN) 14-1
VPN 14-1
 allowing through a firewall 14-22
 ATMP tunnel options 14-18
 default answer profile 14-10
 encryption support 14-8
 PPTP tunnel options 14-4

W

web-based management
 budget statistics 17-10
 connect/disconnect 17-6
 connection budget configuration 17-9
 connection budgets 17-8
 connection status 17-5
 frame relay statistics 17-4
 router budget configuration 17-7
 system information 17-2
Windows NT Domain Name 1-3, 14-7