Netopia™ Router
Reference Guide

netopia®

Copyright

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

Patents

EtherWave daisy-chainable 10Base-T technology is covered by
U.S. Patent Number 5,414,708. Other U.S. and foreign patents are pending.

Contents

Chapter 1

Introduction

Your Netopia Router offers Advanced Configuration features in addition to the Easy Setup features. The advanced feature screens are accessed through the Main Menu of the Router's console configuration screen. This *Reference Guide* documents the advanced features, including advanced testing, security, monitoring, and configuration features. This *Reference Guide* should be used as a companion to the Easy Setup configuration instructions in the Netopia Router *Getting Started* guide. You should read the *Getting Started* guide before reading this *Reference Guide*.

This chapter introduces the *Reference Guide* and tells you how to use it efficiently. You will also learn about different methods of accessing the configuration screens. Finally, you will learn how to locate and go to particular configuration screens.

How to use this guide

This guide is organized into chapters describing each of the Netopia Router's advanced features. You may want to read each chapter's introductory section to familiarize yourself with the various features available.

You can also use this summary to locate relevant sections:

- To configure ISDN setup parameters, see "ISDN WAN Setup" on page 2-2.
- To configure leased line setup parameters, see "Leased line WAN Setup" on page 2-5.
- To add or modify connection profiles, see "Connection profiles for ISDN and Leased lines" on page 2-13.
- To configure the default profile for an ISDN or leased line, see "Default profile" on page 2-39.
- To put the advanced configuration changes into effect, "Restarting the system" on page 10-8.
- To manually establish a connection with an existing connection profile, see "Establishing a WAN Connection" on page 2-30.

400 Netopia series models only

- To use the AppleTalk Update-Based Routing Protocol (AURP), see "AURP setup" on page 6-12.
- To schedule regular or one-time connections, see "Scheduled connections" on page 2-49.
- To configure dynamic IP address service (DHCP, MacIP, or BOOTP), see "IP address serving" on page 4-16.
- For testing network connections, see "The ISDN loopback test" on page 10-9 to test a switched ISDN line, and "Ping" on page 10-3 to test connections to IP hosts.

- For IP filters, see "About filters and filter sets" on page 7-6 and "Working with IP filters and filter sets" on page 7-16.
- To transfer firmware and configuration files, see "Transferring configuration and firmware files with XMODEM" on page 10-12 or "Transferring configuration and firmware files with TFTP" on page 10-17.
- To secure your network with SecurID, see Chapter 8, "Token Security Authentication."

Use the guide's table of contents and index to locate sections on other topics.

The appendices of this guide offer helpful information, such as troubleshooting tips and a technical support guide.

Netopia models

This *Reference Guide* covers all of the Netopia Router models. However some information in this guide will only apply to a specific model.

See the Netopia Router's Release Notes for more information, or call Farallon Customer Service.

Screen differences

Because different Netopia Router models offer different features and interfaces, the options shown on some screens in this *Reference Guide* may not appear on your own particular Netopia Router's console screen.

These differences are explained throughout the manual.

Connecting to the Advanced Configuration screens

There are three ways to connect to the Netopia Router's advanced configuration screens:

- Through the console port, using a local terminal (see the *Getting Started Guide*)
- Using Telnet with the Router's Ethernet port IP address (cannot be used for initial configuration)
- Over analog phone lines using a modem and terminal emulation software (see "Connecting a modem to the SmartPort," below)

You can also retrieve the Netopia Router's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 9-17).

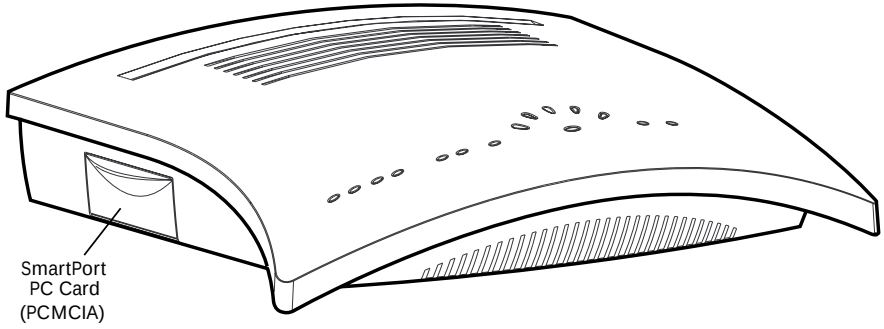
Note: Web-based management does not support advanced configuration.

Connecting a modem to the SmartPort

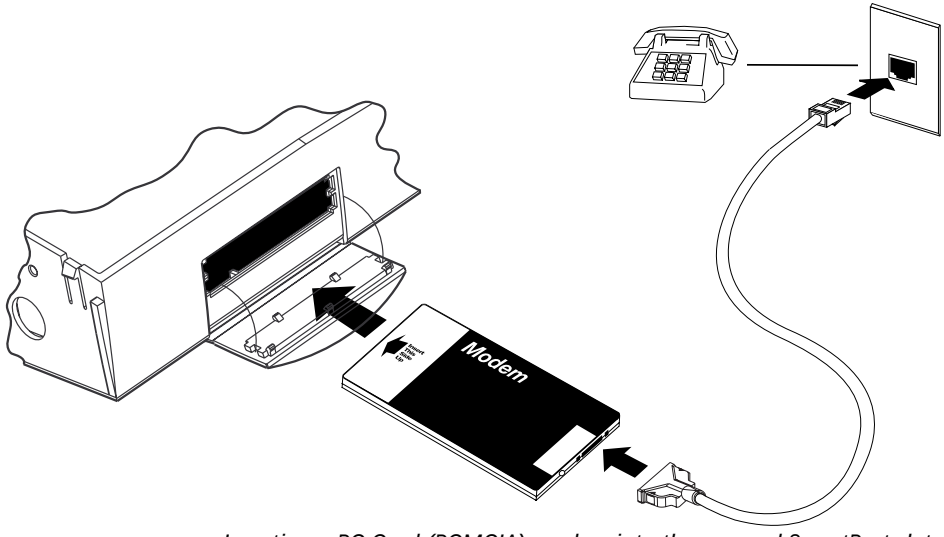
The Netopia Router has a SmartPort (also known as a PC Card port or a PCMCIA card port) for attaching a PC Card Type II modem. The port has two Type II slots and is located on the router's left side behind a pull-down cover.

You may want to attach a Farallon approved PC Card modem to the Netopia Router to remotely configure it or to upgrade its firmware (see "Updating firmware" on page 10-14 or page 10-18.) Contact Farallon Customer Service for information on Farallon approved PC Card modems.

Follow the manufacturer's instructions when unpacking and preparing to use the PC Card modem. One end of the telephone cable connects to your modem, while the other end (RJ-11) connects to an analog telephone line wall socket (*not* an ISDN or leased line).



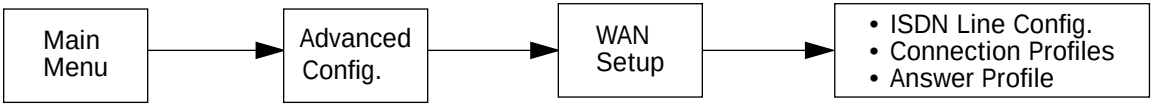
To attach the modem to the Netopia Router, pull down the rubber door that covers its SmartPort slots and insert the modem. You can use either slot.



Inserting a PC Card (PCMCIA) modem into the exposed SmartPort slot.

Navigating through the Advanced Configuration screens

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the WAN Setup screens. The path guide represents these steps:

1. Beginning in the Main Menu, select the Advanced Configuration item and press Return.
2. Select the WAN Setup item in the Advanced Configuration screen and press Return.
3. Select the ISDN Line Configuration, Connection Profiles, or Answer Profile item in the WAN Setup screen and press Return.

To go back in this sequence of screens, use the Escape key.

Keyboard navigation

Use your keyboard to navigate the Netopia Router's configuration screens, enter and edit information, and make choices. The following table lists the navigation keys.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
Execute action of a selected item or open a pop-up menu of options for a selected item	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Ctrl + k
Move one item down	Ctrl + j
Dump the device event log	^E
Dump the ISDN event log	^F
Refresh the screen	^L
Go to topmost selectable item	<
Go to bottom right selectable item	>

Chapter 2

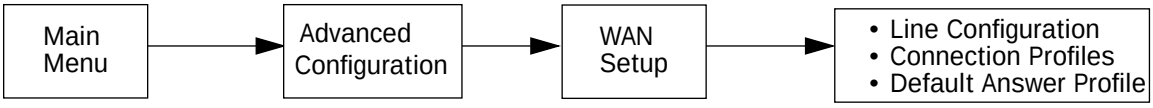
Configuring ISDN and Leased Line Connections

This chapter shows you how to configure the Netopia Router to make and receive network connections over an ISDN or leased line and how to control those connections. Topics include:

- "ISDN WAN Setup" on page 2-2 shows you how to configure your ISDN Netopia Router for outgoing calls.
- "Leased line WAN Setup" on page 2-5 shows you how to configure your SA/Serial, DDS, or T1 Netopia Router for outgoing calls.
- "Connection profiles for ISDN and Leased lines," beginning on page 2-13, shows you how to configure connection profiles for your ISDN, SA/Serial, DDS, or T1 Netopia Router.
- "Default profile," beginning on page 2-39, shows you how to set up an answer profile for incoming calls.
- "WAN IP Address Serving," beginning on page 2-48, discusses how to configure the router to allocate an IP address to callers from an address pool.
- "Scheduled connections," beginning on page 2-49, shows you how to control the dates and times when connection profiles can be used.
- "CSU Backup," beginning on page 2-55, describes how to automatically switch from an internal CSU to the SA port during a leased line failure.

Note: Netopia Router models offering different feature sets will have variations in the fields on certain screens. For example, there are switched (dial-up) or permanent (nailed-up) circuit ISDN or leased line models, as well as models that offer feature subsets such as AppleTalk, SmartIP (Network Address Translation and WAN IP Address Serving) and SmartPhone (Plain Old Telephone Service). Your own Advanced Configuration screens may look different from those illustrated in this chapter.

ISDN WAN Setup



The ISDN WAN Setup screen has three subscreens, each involving a different aspect of using the ISDN line to control connections to remote IP or IPX networks.

Note: If you have completed Easy Setup (see the *Getting Started Guide*), the information you have already entered will appear in some of the Advanced Configuration screens.

To go to the WAN Setup screen, select WAN Setup in the Advanced Configuration screen and press Return. A screen similar to the following appears:

```
                              WAN Setup


                        Line Configuration...

                        Connection Profiles...
                        Default Answer Profile...


From here you will configure yours and the remote sites' WAN information.
```

ISDN line configuration

Enter the information provided by your telephone service provider in the ISDN Line Configuration screen. Use the information recorded in the *Getting Started Guide's* ISDN worksheet as a reference when specifying this configuration information.

To go to the ISDN Line Configuration screen, select Line Configuration in the WAN Setup screen. Press Return, and the ISDN Line Configuration screen appears.

Note: If your ISDN Line Configuration screen contains items that are not discussed in this section, such as SPIDs, see Appendix C, "ISDN Configuration Guide."

The ISDN Line Configuration screen consists of up to three pop-up menus and up to four editable fields.

North America ISDN models only

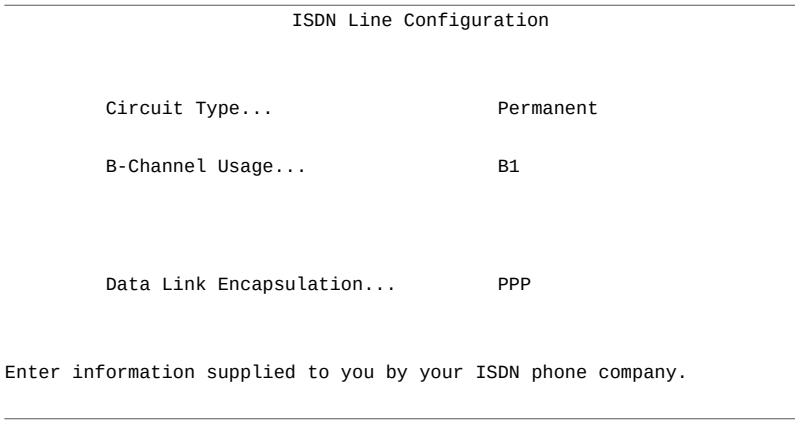
```
                        ISDN Line Configuration


        Circuit Type...                 Switched
        Switch Type...                  National ISDN-1 (NI-1)

        SPID 1:                         510.238.4166.1
        SPID 2:                         510.238.4167.2

        Directory Number 1:             510.577.4166
        Directory Number 2:             510.238.4167

        Data Link Encapsulation...      PPP


Return/Enter goes to new screen.
Enter information supplied to you by your ISDN phone company.
```

1. Select Circuit Type and press Return. From the pop-up menu, highlight Switched if you have an ISDN switched line, or Permanent if you have a dedicated or leased ISDN line. Press Return.

   If you select Switched, go to step 3. If you select Permanent, go to step 2.

   Note: The Switch Type, SPIDs, and Directory Numbers apply only to Switched ISDN service. If you select Permanent, these fields are not displayed.

2. If you select Permanent as your circuit type, select B-Channel Usage.



From the pop-up menu, select the appropriate B-channel, such as B1, B2, or Both. Then go to step 7.

Note: A permanent ISDN circuit type only supports 64 kbps and 128 kbps B-channel usages.

3. Select Switch Type and press Return. From the pop-up menu, select the switch protocol your ISDN service provider uses.

   Observe these guidelines:

   - NI-1 can appear on an AT&T 5ESS or a Northern Telecom DMS-100 Switch. Do not confuse it with a *custom* ISDN implementation, which also appears on these two switches.
   - Countries not shown in the list may use the generic EuroISDN protocol.

Outside North America models only

North America models only

4. Select SPID 1 and enter the primary SPID number. If you did not receive a SPID (AT&T 5ESS custom point-to-point switches have no SPID), you should skip this and the following step.

North America models only

5. If you have a second SPID, select SPID 2 and enter the secondary SPID number.

   Note: SPID1 and SPID2 are not displayed for models outside North America.

6. Select Directory Number 1 and enter the primary directory number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes). Press Return.

   Note: If you select an IDSL (Pt-to-Pt) switch, the Directory Number 1 field will default to 555-1234.

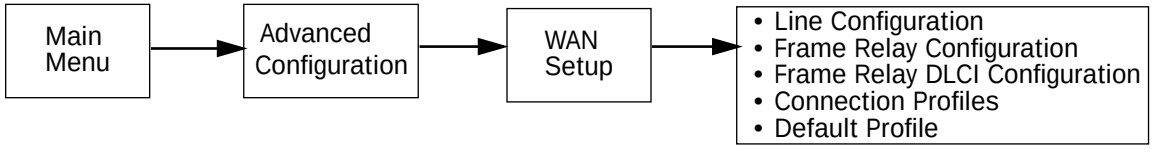
   Since an IDSL line is already physically hooked up in a pt-to-pt configuration, a specific directory number is not necessary. However, the Netopia Router does require a directory number in this field to allow a connection to dial out.

7. If you have a second directory number, select Directory Number 2 and enter the secondary directory number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes). Press Return.

8. Select Data Link Encapsulation and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP or HDLC. Press Return.

In order for the changes that you have entered in the ISDN Line Configuration screen to take effect, you must reset the Netopia Router. Press the Escape key to return to the Main Menu. Select Statistics, Utilities, Tests and then select Restart System.

Leased line WAN Setup



The leased line WAN Setup screen will vary for an SA/Serial, 56k DDS, or T1 line depending on the circuit type and datalink encapsulation parameter that is selected for that specific leased line.

To begin WAN Setup, select WAN Setup in the Advanced Configuration menu, then press Return.

```
                              WAN Setup


                         Line Configuration...

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

                         Connection Profiles...
                         Default Profile...



From here you will configure yours and the remote sites' WAN
information.
```

Note: For all leased line Netopia Router models using PPP or Cisco-HDLC datalink encapsulation, the Frame Relay Configuration and Frame Relay DLCI Configuration options will be hidden.

For all leased line Netopia Router models using Cisco-HDLC datalink encapsulation, the Default Profile option will remain hidden.

If you have completed Easy Setup (see the *Getting Started Guide*), the information you have already entered will appear in some of the WAN Setup screens.

Leased line configuration

The following Leased line configuration section describes the first step in configuring the Line Configuration screen in the WAN Setup menu for an SA/Serial, T1, and DDS Netopia Router wanlet module with PPP, Cisco-HDLC, or Frame Relay datalink encapsulation enabled.

The Serial Line Configuration screen appears for SA/Serial leased line models (with an external CSU/DSU connection). See below.

The T1 Line Configuration screen appears for T1 leased line models (with an internal CSU/DSU connection). See page 2-9.

The DDS Line Configuration screen appears for DDS leased line models (with an internal CSU/DSU connection). See page 2-12.

Line configuration for an SA/Serial line

The Serial Line Configuration screen is where you enter the configuration parameters for your leased line, in order for the Netopia Router to communicate with the physical connection. Use the information in the Leased Line worksheet in the *Getting Started Guide*, as a reference when specifying this configuration information.

Permanent circuit only

```
                        Serial Line Configuration

        Circuit Type...                 Permanent Sync

        Data Rate (kbps)...             64

        Invert Tx Clock:                No
        Circuit Activation Requires...  DCD and DSR

        Data Link Encapsulation...      Frame Relay

Enter Information supplied to you by your telephone company.
```

1. Select Circuit Type and select Permanent Sync or Switched Async. If you select permanent sync, continue with Step 2. If you select Switched Async, skip to Step 6.
2. Select Data Rate (kbps) and press Return. From the pop-up menu, select a fixed data rate for your digital line or select Auto. (The data rates to choose from range from 56 kbps to the highest synchronized line speed.) The Auto setting allows your Netopia Router to determine the data rate of your serial line at the time of circuit activation. Press Return.

Permanent circuit only

3. Select Invert Tx Clock and toggle to Yes or No depending on whether you use this selection. Press Return.

   Invert Tx Clock causes transmitted data to be delayed by half a clock phase. This option is useful for X.21 DTEs (Data Terminal

Equipment) because their transmit data can become altered in relation to the clock sourced by the DCE (Data Communications Equipment).

A DTE (Data Terminal Equipment) is a term used to define the equipment rate. It is a designation for the maximum rate at which a router can exchange information.

A DCE (Data Communications Equipment) is a term defined by both Frame Relay and X.25 committees, that applies to switching equipment and is distinguished from the devices that attach to the network (DTE).

Permanent circuit only

4. Select Circuit Activation Requires and select DCD-only, DSR-only, or DCD and DSR. Press Return.

   Some V.35 interfaces represent their capability to transfer user data end-to-end with the DCD signal, while others offer a more accurate representation with DSR. For this latter case, you may choose to use DSR-only.

   Note: This option will be hidden if an X.21 cable is attached.

5. Select Data Link Encapsulation and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP, HDLC, and Frame Relay. The default setting is Frame Relay. Press Return.

   Continue to the last step.

Switched circuit only

```
                    Serial Line Configuration


Circuit Type...                     Switched Async

Data Rate (kbps)...                 57.6

Modem Initialization String:        AT&C1&D2E0S0=1
Modem Dialing Prefix:               ATDT

Data Link Encapsulation is          Async PPP
```

Switched async only

6. Select Date Rate (kbps) and press Return. From the pop-up menu, select 19.2, 38.4, 57.6, 115.2, or 230.4. Choose the data rate that is about twice your modem's capabilities. For instance, if you have a 28.8K modem, select 57.6 for your data rate. Press Return.
7. The Modem Initialization String and Modem Dialing Prefix fields configure the connection to the external modem. For information on editing this configuration, see the Netopia Router 3.2 Release Note.
8. The Data Link Encapsulation is set to Async PPP.
9. You are now finished configuring the Serial Line Configuration screen. Press the Escape key to return to the WAN Setup screen. Go to page 2-13 for information on how to configure your leased line connection profile.

Line configuration for a T1 line

The T1 Line Configuration screen is where you enter the configuration parameters for your leased line, in order for the Netopia Router to communicate with the physical connection. Use the information in the Leased Line worksheet in the Getting Started Guide as a reference when specifying your T1 configuration information.

```
                          T1 Line Configuration

        Line Encoding...                  B8ZS

        Framing Mode...                   ESF
        Transmit ANSI PRMs:               No

        Number of DS0 Channels:           1
        First DS0 Channel:                1


        Buildout (-dB)...                 Auto

        Channel Data Rate...              Nx64k
        Clock Source...                   Network

        Data Link Encapsulation...        Frame Relay

Enter Information supplied to you by your telephone company.
```

1. Select Line Encoding and press Return. From the pop-up menu, highlight the encoding your telephone service provider uses: B8ZS or AMI. The default setting is B8ZS. Press Return.
2. Select Framing Mode and press Return. From the pop-up menu, highlight either ESF or D4, depending on the framing mode that your telephone service provider advises you to use. The default setting is ESF. Press Return.
3. The ANSI T1.403 standard defines Performance Report Messages (PRMs) that may be transmitted each second from a T1 Integrated CSU to the telephone service provider's network. By default, the Netopia Router does not send PRMs. However, you can enable these transmissions by toggling Transmit ANSI PRMs to Yes.
4. Select Number of DS0 Channels and enter the number of DS0 channels that you and your telephone service provider have determined are necessary for your T1 line. The default setting for DS0 Channels is 1 (one). Press Return.

Note: Each DS0 channel represents a 56k or 64k increment in bandwidth. Selecting a number less than the maximum of 24 specifies a fractional-T1 interface.

For fractional-T1, you may also specify in the check box whether the DS0 channels are contiguous or alternating.

5. Select First DS0 Channel and enter the number of the first active DS0 channel you will be using. The default setting is 1 (one). Press Return.

   Note: You may change the First DS0 Channel number, which has a valid range from one to the maximum number minus the number of active channels. If the number of active DS0 channels is 24 (maximum), First DS0 Channel is hidden.

6. Select Buildout (-dB) and press Return. From the pop-up menu, highlight the line Buildout, which is the transmit attenuation of your line that you will be using. The choices in the menu include Auto, 0-0.6, 7.5, 15.0, 22.5, and None. The default setting is Automatic. Press Return.

   If Automatic is chosen, the attenuation of the transmission will be set to match the receiving signal level.

7. Select Channel Data Rate and highlight the data rate specified by your service provider. The channel data rate choices are Nx56k or Nx64k. The default is Nx64k. Press Return.

8. Select Clock Source and press Return. From the pop-up menu, highlight the clock source, that you wish to use. The choices offered are Internal Clock Source, or Network Clock Source. The default is Network. Press Return.

9. Select Data Link Encapsulation and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP, HDLC, and Frame Relay. The default setting is Frame Relay. Press Return.

10. You are now done configuring the Line Configuration screen. Press the escape key to return to the WAN Setup screen. Go to page 2-13, for information on how to configure your leased line connection profile.

Line configuration for a DDS line

The DDS Line Configuration screen is where you enter the configuration parameters for your leased line, in order for the Netopia Router to communicate with the physical connection. Use the information in the Leased Line worksheet in the Getting Started Guide as a reference when specifying your DDS line configuration information.

```
                          DDS Line Configuration


        Circuit Type...                    Permanent

        Data Rate...                       Auto

        Clock Source...                    Network

        Data Link Encapsulation...         Frame Relay


Enter Information supplied to you by your telephone company.
```

---

1. Select Circuit Type and press Return. From the pop-up menu, highlight Switched for a dial-up digital line or Permanent for a nailed-up leased line. The default setting is Permanent. Press Return.

   Note: The DDS data rate is capable of handling 56 or 64 kbps. If the Switched circuit type is selected, 56 kbps data rate is the only available option. If the Permanent circuit type is selected, 56 kbps and 64 kbps data rates will be available.

2. Select Data Rate and press Return. From the pop-up menu, highlight the data rate that you want your DDS line connection to transmit at. The data rate choices are 56 kbps and 64 kbps. The default is Automatic. Press Return.

   Note: As noted above, DDS Netopia Routers may run 56 kbps or 64 kbps data rates on permanent circuits. You may alternately select Automatic, in which case the router will hunt between modes until it can determine what the telephone company has provisioned your DDS line for.

3. Select Clock Source and press Return. From the pop-up menu, highlight the clock source, that you wish to use. The choices offered are Internal Clock Source, or Network Clock Source. The default is Network. Press Return.
4. Select Data Link Encapsulation and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP, HDLC, and Frame Relay. The default setting is Frame Relay. Press Return.
5. You are now done configuring the Line Configuration screen. Press the escape key to return to the WAN Setup screen. Go to page 2-13, for information on how to configure your leased line connection profile.

Connection profiles for ISDN and Leased lines

A connection profile is a set of parameters that tells the Netopia Router how to connect to a remote destination. Connection profiles are also used to make out-bound calls and optionally to help answer calls.

Some Netopia models support up to 4 different connection profiles while most models support up to 16 connection profiles.

To go to the Connection Profiles screen, select Connection Profiles in the WAN Setup screen.

```
                        Connection Profiles

                Display/Change Connection Profile...

                Add Connection Profile...

                Delete Connection Profile...


                Establish WAN Connection...

                Disconnect WAN Connection...

Return/Enter to modify an existing Connection Profile.
This Screen is the main point of navigation for Connection Profiles.
```

Note: The Establish WAN Connection and Disconnect WAN Connection fields in the Connection Profiles screen will only appear for a Netopia Router model with switched circuit selected. This field will remain hidden when permanent circuit is selected.

Displaying connection profiles

To display a view-only table of connection profiles, select Display / Change Connection Profile in the Connection Profiles screen. Press Return and the connection profiles that you have created will appear.

The Connection Profiles table is a handy way to quickly see the names and destination IP or IPX addresses of your connection profiles.

```
                        Connection Profiles
        +-Profile Name---------------------IP Address----IPX Network-+
        +-----------------------------------------------------------+
        | Easy Setup Profile               127.0.0.2       0         |
        | Panost Inc.                      0.0.0.0                   |
        | XYZ Corporation                  0.0.0.0                   |
        +-----------------------------------------------------------+

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

Changing a Connection Profile

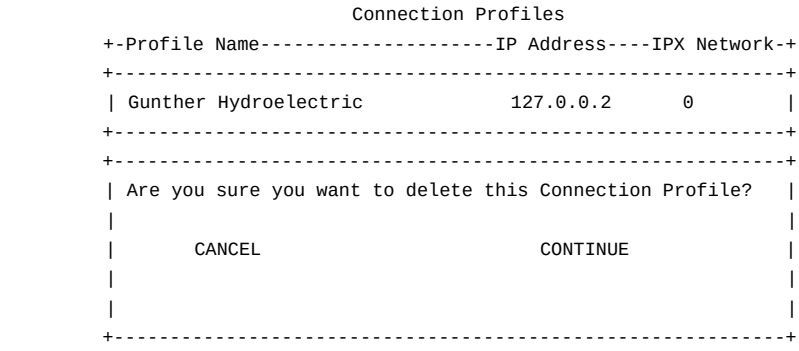
To modify a connection profile, select Display / Change Connection Profile in the Connection Profiles screen to display a table of connection profiles.

Select a connection profile from the table and press Return to go to the Change Connection Profile screen. The parameters in this screen are the same as the parameters found in the Add Connection Profile screen. To find out how to set them, see “Adding a connection profile” on page 2-16.

```
                        Change Connection Profile

        Profile Name:                    Panost Inc.
        Profile Enabled:                 Yes

        IP Enabled:                      Yes
        IP Profile Parameters...

        IPX Enabled:                     Yes
        IPX Profile Parameters..

        Data Link Encapsulation...       PPP

        Data Link Options...
        Telco Options...

Modify Connection Profile here. Changes are immediate.
```

Deleting a Connection Profile

To delete a connection profile, select Delete Connection Profile in the Connection Profiles screen and press Return to display a table of connection profiles.



1. Highlight the connection profile you wish to delete. Press Return.
2. A connection profile table appears with a prompt asking you if you want to delete the connection profile you have just highlighted. Select CONTINUE if you wish to delete this connection profile or CANCEL if you do not.

Adding a Connection Profile

To add a new connection profile, select Add Connection Profile in the Connection Profiles screen. Press Return and the Add Connection Profile screen appears.

```
                    Add Connection Profile

      Profile Name:                     Profile 04
      Profile Enabled:                  Yes

      IP Enabled:                       Yes
      IP Profile Parameters...

      IPX Enabled:                      Yes
      IPX Profile Parameters..

      Data Link Encapsulation...        PPP
      Data Link Options...

      Interface Group...                Int CSU
      Telco Options...


         ADD PROFILE NOW                  CANCEL

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

1. Select Profile Name and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Select Profile Enabled and toggle it to Yes to activate the profile.
3. Select IP Enabled and toggle it to Yes or No depending on whether you will be using TCP/IP over your WAN connection.
4. Select IP Profile Parameters. This option is only available if IP Enabled is toggled to Yes.

```
                        IP Profile Parameters

        Address Translation Enabled:       Yes

        IP Addressing...                   Numbered
        Local WAN IP Address:              0.0.0.0
        Local WAN IP Mask:                 0.0.0.0
        Remote IP Address:                 0.0.0.0
        Remote IP Mask:                    0.0.0.0

        Filter Set...
        Remove Filter Set

        Receive RIP:                       Yes

Configure IP requirements for a remote network connection here.
```

Applicable only to SmartIP models

5. In the IP Profile Parameters screen, toggle Address Translation Enabled to Yes if you choose to use Network Address Translation.

   Network Address Translation allows communication between the LAN connected to the Netopia Router and the Internet using a single IP address, instead of a routed account with separate IP addresses for each computer on the network. Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia Router from the outside world.

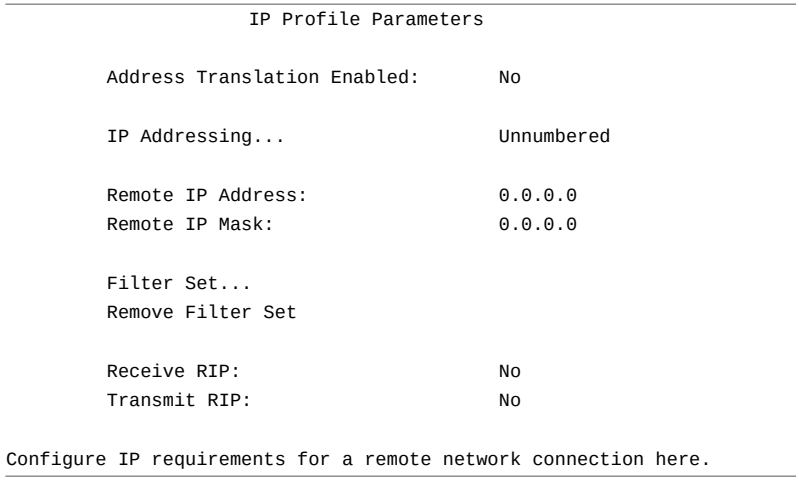
   Note: See “Summary of the Netopia Router models and features” on page 1-5 of the *Getting Started Guide*.

- If you did not enable Network Address Translation, select IP Addressing and, from the pop-up menu, choose the IP routing method that your ISP or network administrator specifies (either Numbered or Unnumbered).
- If your ISP uses Numbered (Interface-based) Routing, select Local WAN IP Address and enter the local WAN address your ISP gave you. Then select Local WAN IP Mask and enter the WAN subnet mask of the remote site you will connect to.

The default address for the Local WAN IP Address is 0.0.0.0, which allows for dynamic addressing, when your ISP assigns an address each time you connect. However, you may enter another address if you want to use static addressing.

Note: When using Cisco-HDLC datalink encapsulation and Network Address Translation, you must use a static address.

When using numbered interfaces, the Netopia Router will use its local WAN IP address and subnet mask to send packets to the remote router. Both routers have WAN IP addresses and subnet masks associated with the connection.



- If your ISP uses Unnumbered (System-based) Routing, select Remote IP Address and enter the IP address your ISP gave you. Then select Remote IP Mask and enter the IP subnet mask of the remote site you will connect to.

  Note: If your ISP has not given you their IP or subnet mask addresses, then you may enter an IP address such as 127.0.0.2 and an IP subnet mask such as 255.0.0.0.

  When using unnumbered interfaces, the Netopia Router will use either its local Ethernet IP address or its NAT (Network Address Translation) address (if so configured) and subnet mask to send packets to the remote router. Neither router has

a WAN IP address or subnet mask associated with this connection. These default addresses will request that the remote router dynamically assign an address at the time the connection is made.

To configure a profile for a terminal adapter or Netopia Router that is dialing into your router using dynamic Network Address Translation, you may enter a 0.0.0.0 remote IP address and enable IP WAN Address Serving.

Note: If you are interested in serving a WAN IP Address to an incoming caller, see “WAN IP Address Serving” on page 2-48.

- Select Filter Set and then select an appropriate filter set from the list. If you do not want to block any TCP/IP traffic, then leave this entry blank.
- To remove a filter set, select Remove Filter Set and press Return. A pop-up menu will appear displaying the filter sets you have set up previously. Highlight the specific filter set that you want to remove and press Return. A window will appear asking you if you are sure that you want to delete that specific filter set. You can either select Continue or Cancel.
- Select Receive RIP and toggle it to Yes if you want the Netopia Router to receive RIP information sent by remote routers that are connected to your local area network (LAN).
- Select Transmit RIP and toggle to Yes if you want the Netopia Router to send RIP information to remote routers that are connected to your LAN. If Transmit RIP has been enabled, the TX RIP Policy field will appear. Select TX RIP Policy and press Return and the Poison Reverse field will appear.
- Press the Escape key when you are finished configuring IP Profile Parameters to go back to the Add Connection Profile screen. The next step describe how to configure the IPX parameters. If you do not wish to enable IPX, skip to step 7, which describes how to set up Data Link Encapsulation.

6. From the Add Connection Profile screen, select IPX Enabled and toggle it to Yes or No depending on whether you will be using IPX over your ISDN connection.

Note: Using the IPX protocol is required with other remote networks using IPX for an intranet connection. For more information on IPX, refer to Chapter 5, “IPX Setup” of this guide.

- Select IPX Profile Parameters and press Return. This option is only available if IPX Enabled is toggled to Yes.

```
                        IPX Profile Parameters

     Remote IPX Network:               00000000
     Path Delay:                       10
     NetBios Packet Forwarding:        Off

     Incoming Packet Filter Set...     <<NONE>>
     Outgoing Packet Filter Set...     <<NONE>>

     Incoming SAP Filter Set...        <<NONE>>
     Outgoing SAP Filter Set...        <<NONE>>

     Periodic RIP Timer:               60
     Periodic SAP Timer:               60

Configure IPX requirements for a remote network connection here.
```

- Select Remote IPX Network and enter the network address of the IPX network being called. Do not use an address already in use by another connection profile. If this value is set to zero and the Netopia Router is answering a call, the remote address will be learned when the profile is active.

  Note: If you are trying to connect two Netopia Routers using Frame Relay and IPX, be sure to enter an IPX address for the remote side in the connection profiles. If the remote IPX address is all zeros (the default), the two Netopia Routers will not be able to connect.

  Note: Unlike IP, the IPX network address is never used in matching a profile when answering a non-authenticated call.

- To change the default Path Delay, select and enter a value (in ticks).
- To enable NetBIOS Packet Forwarding, toggle the selection to Yes.
- Select Incoming Packet Filter Set to attach a filter set for filtering incoming packets. Choose a filter set from the list and press Return.
- Select Outgoing Packet Filter Set to attach a filter set for filtering outgoing packets. Choose a filter set from the list and press Return.
- Select Incoming SAP Filter Set to attach a filter set for filtering server entries within incoming Service Advertising Protocol (SAP) packets. Choose a filter set from the list press Return.
- Select Outgoing SAP Filter Set to attach a filter set for filtering server entries within outgoing Service Advertising Protocol (SAP) packets and choose a filter set from the list.
- Select Periodic RIP Timer, and enter a new value (in seconds) to change the periodic RIP timer's default value.
- Select Periodic SAP Timer, and enter a new value (in seconds) to change the periodic SAP timer's default value.
- Press the Escape key to go back to the Add Connection Profile screen when you are finished configuring IPX Profile Parameters.

For more information on creating an IPX filter set, go back to the Advanced Configuration screen and select the Filter Sets (Firewalls) screen. Also refer to Chapter 6, "IPX Setup".

7. Select Data Link Encapsulation and highlight the method of encapsulation that you want to use from the pop-up menu. The choices offered are PPP, HDLC, or Frame Relay. Press Return.

   If you have enabled PPP/MP, go to step 8. If you have enabled Frame Relay, go to step 9. If you have enabled HDLC, go to step 11.

8. Select Data Link Options and press Return. The PPP/MP Options screen appears.

Point-to-Point Protocol (PPP) and Multilink Point-to-Point Protocol (MP) allow the Netopia Router to make adaptable and secure connections to other networks.

```
                              PPP/MP Options

     Data Compression...                Ascend LZS

     Send Authentication...             PAP

     Send User Name:
     Send Password:

     Receive User Name:
     Receive Password:

     B-Channel Usage...                 Dynamic

     BAP Usage...                       Off


Return/Enter to choose PPP Authentication type (or None).
```

- Select the Data Compression pop-up menu, choose the type of data compression supported by the network you are calling, and press Return. The choices are Ascend LZS, Standard LZS, or None (if the remote network does not use Ascend LZS or Standard LZS). Ascend LZS is compatible with the type used by Ascend Communications. This is the default setting for Data Compression, as most ISP's (Internet Service Providers) and remote networks use Ascend's proprietary data compression utility. Standard LZS is an IETF (Internet Engineering Task Force) standard for LZS data compression.

Applicable only to Switched circuits

- Select the Send Authentication pop-up menu and choose the type of connection security supported by the network you are calling. From the pop-up menu highlight PAP, CHAP, PAP-TOKEN, CACHE-TOKEN, or None (if the remote network does not use PAP or CHAP). On the Netopia Router the default

authentication is set for PAP, as this is usually the most popular security parameter that ISP's and other remote networks set up for a point-to-point connection use.

- If you choose None, and the remote network expects to connect to the Netopia Router using this connection profile, you may need to set the answer profile to accept calls using no authentication (None). See "Default profile" on page 2-39.
- If you choose to use PAP for calling the remote network, you will need to obtain a name and password from the remote network's administrator. Enter the name in Send User Name and enter the password in Send Password. If you want the remote network to use this connection profile when it calls the Netopia Router, select Receive Name and enter a name. Select Receive Password and enter a password. You will need to give this name and password to the remote network's administrator.

If you choose PAP, and the remote network expects to connect to the Netopia Router using this connection profile, you may need to set the answer profile to accept calls using PAP. See "Default profile" on page 2-39.

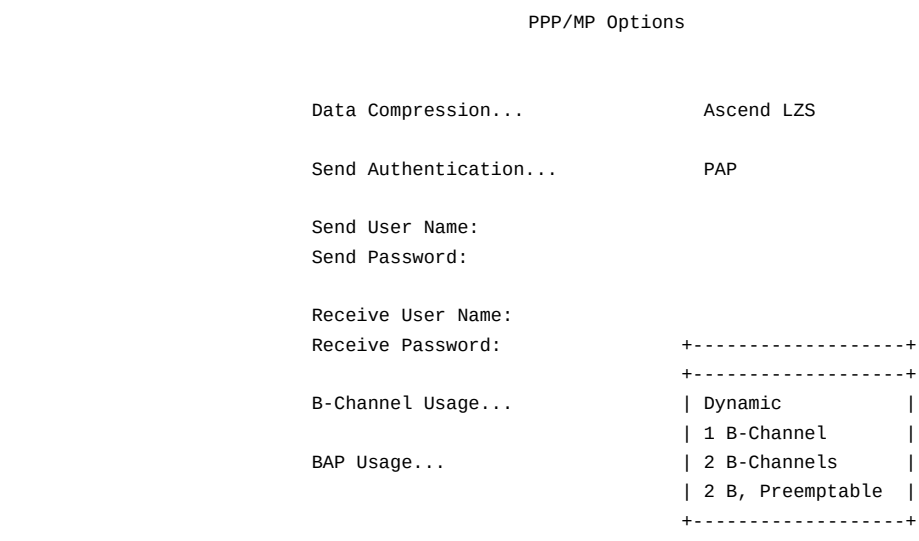
- If you choose to use CHAP for calling the remote network, obtain a name and secret (the CHAP term for password) from the remote network's administrator. Enter the name in Send Host Name and enter the password in Send Secret. If you want the remote network to use this connection profile when it calls the Netopia Router, select Receive Host Name and enter a name. Select Receive Secret and enter a secret. You will need to give this name and secret to the remote network's administrator.

Note: If you choose CHAP, and the remote network expects to connect to the Netopia Router using this connection profile, you may need to set the answer profile to accept calls using CHAP. See "Default profile" on page 2-39.

- If you choose to use PAP-TOKEN, select Send User Name and enter a name for your Netopia Router. You will not need to enter a Send Password for PAP-TOKEN.

- If you choose to use CACHE-TOKEN, select Send User Name and enter a name for your Netopia Router. Then, select Send Password and enter a secret name or number.

If you will be using SecurID (an added method of security authentication), check with your network administrator to find out if you will need to use either PAP-TOKEN, or CACHE-TOKEN. (Also, see Chapter 9, “Security-Token Authentication”.)



Applicable only to Switched circuits

- Select B-Channel Usage and choose how this connection profile will use the ISDN line’s B-channels. From the pop-up menu highlight either Dynamic, 1 B-Channel, 2 B-Channels, or 2 B, Pre-emptable.
  - Dynamic (default setting), allows the connection profile to use one or both channels at any time during a call. The decision to alternately use or drop the second B-channel is based on an algorithm that looks at traffic volume over time. With Dynamic, one B-channel may be relinquished to

accept an incoming call through or when a second connection profile is used to make a call. See Appendix D for information on “Dynamic B-channel usage”.

- 1 B-Channel forces a call to remain within one B-channel. (Throughput will generally be at either 56k or 64k, depending on how the local telephone company installs your ISDN line. This will also depend on certain geographic locations in North America. The standard ISDN data rate outside of North America is 64k.)
- 2 B-Channels forces a call to use both B-channels. (Throughput connection will generally run at 128k.)
- 2 B Pre-emptable allows calls to use 2 B-channels in a dynamic, Pre-emptable manner. This option is very similar to Dynamic, in that the second B-channel may be relinquished to accept an incoming call or to initiate a second outgoing call. However, 2B Pre-emptable will always try to add a second B-channel to the call when the second channel is otherwise unused, much like a fixed 2 B-channel selection.

Note: If you select Dynamic or 2 B, Pre-emptable while using PPP/MP, the Netopia Router may attempt to use both B-channels during a call. However, during a call, your second B-channel may be blocked from use if the answering side drops that B-channel before you begin sending data over it. The Netopia Router will try four times to bring up the second B-Channel; if all attempts fail and you wish to retry, end the call and reinitiate it.

Applicable only to Switched circuits

- Select BAP Usage and from the pop-up menu highlight the method of BAP usage that your ISP or network administrator has suggested that you use when establishing a connection to a remote site. The choices offered for BAP usage are On - Old IDs, On - New IDs, and Off. Press Return.

  BAP refers to the PPP Bandwidth Allocation Control Protocol. The BAP Usage feature allows a Netopia Router to either dial out to provide a telephone number for a multilink call, or allows the Netopia Router to answer a call, while also providing a

telephone number for a multilink call. In addition, the Netopia Router can bring WAN links up and down with a remote router.

Note: There are two specifications for BAP protocol. The first specification was proposed before January 1997 and the latter was proposed after that date.

The On-Old IDs selection refers to the earlier BAP proposal and On-New IDs refer to the new proposal.

Because there is no set standard at this time for BAP protocol the Netopia Router allows you to select either specification.

Models with Frame Relay enabled only

9. Select Data Link Options and press Return. The Frame Relay Parameters screen appears.

```
                        Frame Relay Parameters


        Auto-Detect DLCIs:                Yes

        Multicast DLCI Number:            0

Configure Frame Relay-specific parameters of your Connection Profile
here.
```

- Select Auto-Detect DLCIs and toggle to either Yes or No. If you select Yes, you are enabling your Frame Relay profile to auto-detect the DLCIs associated with its network layer attributes. This feature is also called SmartMatch. If you select No, you will need to manually configure each DLCI in the DLCI configuration table. See “Frame Relay DLCI configuration” on page 2-34. The default setting for this option is Yes. Press Return.
- Select Multicast DLCI Number. In this field you may add a number that will be used for multicasting in conjunction with the network layer attributes of your given profile. The default setting for this option is 0. If you choose to leave 0 as the value for this field, the specific profile that you are configuring will not be used for multicasting.

T1 and DDS models only

10. The Interface Group field reflects the active port selection: the internal CSU for T1 or DDS, or SA port for SA, if backup is enabled. See “CSU Backup” on page 2-55 for more information.

Models with Switched circuits only

11. Select Telco Options and press Return. The Telco Options screen appears. The Telco Options screen contains items that allow you to control the calls made on the WAN line with this particular connection profile.

```
                              Telco Options

    Initiate Data Service...          64 kb/sec

    Dial...                           Dial In/Out

    Number to Dial:
    Alternate Number to Dial:

    Dial On Demand:                   Yes
    Idle Timeout (seconds):           300

    CNA Validation Number:
    Callback:                         No


In this Screen you configure options for the ways you will establish a
link.
```

ISDN Switched circuit models only

- Select Initiate Data Service and choose the correct ISDN bandwidth to use with this connection profile. In North America, users are not guaranteed of having a 64k connection to their destination, but only when 64k is not available from point A to point B should 56k be selected. The Router automatically falls back to 56k when 64k service is not available. It is advised to select 56k when you know that the 64k service will fail. You may also select Speech if your line is provisioned for this feature and the call is within your local ISDN region. Selecting Speech may save money, but it is not guaranteed to work outside of your switch.

- Select Dial and set this connection profile to only make calls, only receive calls, or do both. Choose from In Only (receive calls), Out Only (make calls), or Dial In/Out (receive and make calls).
- Select Number to Dial and enter the telephone number you received from your ISP. This is the number the Netopia Router dials to reach your ISP. Enter the number as you would dial it, including any required prefixes (such as area, access, and long-distance dialing codes).

  If you selected IDSL (Pt-to-Pt) as your Netopia Router's switch type the connection profile's number to dial will default to 555-4321. The same default information applies to this number as the directory number, in order for the Netopia Router to allow a connection to dial out.

  Note: If you previously selected Permanent as your router's Circuit Type in the ISDN Easy Setup screen, Number to Dial will not be an available option.
- Select Alternate Number to Dial if your ISP requires that you use a second telephone number to dial, or as an alternative backup when the first channel is unavailable to use.

Available for outbound calls only

- Select Dial On Demand and toggle No if manual connections are required for this profile. The default for Dial On Demand is Yes, which is correct for most uses. When Dial On Demand is set to Yes, the Netopia Router can automatically make calls as the need arises, such as when a request to connect to a host on the Internet is made by a computer on the local network. Dial on demand also comes into action when IP and or IPX traffic needs to go to a route defined by the profile attributes. Every dial-on-demand profile becomes a part of the routing table.

  See "Establishing a WAN Connection" on page 2-30 for more information.
- Select Idle Timeout (seconds) and enter the time limit desired before the Netopia Router drops a call if there is no activity on the line. The default timeout setting is 300 seconds (5 minutes.)

ISDN Switched circuit models only

Available for inbound calls only

- The CNA Validation Number is the telephone number that your Netopia Router will match to incoming calls. Question marks "?" can be used in place of numbers as wild card characters to ensure that matches are made on different directory numbers. See "Default profile" on page 2-39 for information on CNA (Calling Number Authentication).

Available for inbound calls only

- Select Callback and toggle to Yes to drop incoming answered calls and use this connection profile to call the remote network back. (See "Default profile" on page 2-39 for information on incoming calls matching connection profiles). The default for Callback is No.

  You are now finished configuring the Telco options screen. Press the Escape key to return to the Add Connection Profile screen.

12. From the Add Connection Profile screen, select ADD PROFILE NOW to save the current connection profile information that you have just entered, and press Return to go to the Connection Profiles screen. Alternatively, you can cancel the connection profile you have just constructed by selecting CANCEL to exit the Add Connection Profile screen.

Establishing a WAN Connection

Switched circuit models only

To establish a manual WAN connection call, select Establish WAN Connection from the Connection Profiles screen and press Return.

The Establish WAN Connection pop-up menu displays a table of all of the connection profiles you have previously defined. Highlight the connection profile you wish to manually call. Press Return and the connection you select will initiate a call.

```
                              Call Status

                    Profile Name -- Panost, Inc.
                    Connection State -- Acquiring

Hit ESCAPE/RETURN/ENTER to return to previous menu.
```

If a connection is establishing properly, the Connection State will initially read Acquiring but will change to Up once the call has successfully connected. You will be able to access information at the remote site that you are connecting to once authentication is completed successfully.

Disconnecting a WAN Connection

Switched circuit models only

To hang up a manual WAN connection call, select Disconnect WAN Connection from the Connection Profiles screen and press Return.

The Disconnect pop-up menu displays a table of all of the connection profiles you have previously defined. Highlight the connection profile you wish to disconnect. Press Return and the connection you select will be disconnected. Press Esc to cancel.

Frame Relay configuration

If you chose Frame Relay as your datalink encapsulation type you will now need to configure your Netopia Router to support Frame Relay. From the WAN Setup screen, select the Frame Relay Configuration option and press Return.

The Frame Relay Configuration screen consists of two pop-up menus. Use the information in the Leased Line worksheet in the *Getting Started Guide* as a reference when specifying this configuration information.

```
                        Frame Relay Configuration

        LMI Type...                          ANSI (Annex D)
        T391 (Polling Interval in secs):     10
        N391 (Polls/Full Status Cycles):     6
        N392 (Error Threshold):              3
        N393 (Monitored Event Window):       4

        Tx Injection Management...           Standard
        Default CIR:                         64000
        Default Bc:                          64000
        Default Be:                          0

        Congestion Management Enabled:       Yes

         Maximum Tx Frame Size:              1536

Enter Information supplied to you by your telephone company.
```

1. Select LMI Type (Link Management Type) and press Return. From the pop-up menu, highlight either ANSI (Annex D), CCITT (Annex A), LMI, or None. The world-wide default is ANSI (Annex D). Press Return.

   Note: If you select None as an LMI Type, the four LMI options listed below will remain hidden, and you will need to manually configure DLCIs. See “Frame Relay DLCI configuration” on page 2-34 for instructions.

   Specifying the Link Management Type is the first step in configuring Frame Relay.

   - If you select an LMI Type (Link Management Type) other than None, the T391 option specifies the number of seconds between the Status Enquiry messages. The default setting is 10.
   - The N391 option specifies the frequency of full status polls, in increments of the basic (T391) polling cycle. The default setting is 6.

- The N392 option specifies the maximum number of (link reliability, protocol, and sequence number) error events that can occur within the N393 sliding window. If an N392 threshold is exceeded, the switch declares the Netopia Router inactive. The default setting is 3.
- The N393 option allows the user to specify the width of the sliding N392 monitored event window. The default setting is 4.

2. Select Tx Injection Management and press Return. From the pop-up menu, highlight Standard if you want the frames on your line that exceed the link capacity to be acknowledged and marked as discard-eligible, Buffered if you want the frames on your line that exceed the link capacity to be delayed until the link is less busy, or None if you want all of the frames on your line to be transmitted. Press Return.

   Note: If you select None as the Tx Injection Management type, the three Tx Injection Management options listed below will remain hidden. Go to step 4.

   If you select Standard or Buffered as the Tx Injection Management type, then the Default CIR, Bc, and Be values will appear (in the corresponding fields below the Tx Injection Management field) in order for you to define the parameters the management algorithm.

   - The Default CIR (CIR also referred to as Committed Information Rate) represents the average capacity available to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 64000, but you may modify the capacity rate if this setting will not be applicable to you.
   - The Default Bc (Bc also referred to as Committed Burst Size) represents the maximum amount of data that your Frame Relay service provider agrees to transfer from a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 64000, but you may change the capacity rate if this setting needs to be modified.

- The Default Be (Be also referred to as Excess Burst Size) represents the maximum amount of data that your Frame Relay service provider will attempt to deliver to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). This setting defaults to 0, but you may change the capacity rate if this setting needs to be modified.

See Appendix B, "Understanding Frame Relay" in the *Getting Started Guide* for information on the these parameters.

Note: Some Frame Relay service providers allow for over-subscription of the DLCIs, which occurs when the total number of CIRs for all PVCs exceeds the line rate setup.

3. Select Congestion Management Enabled and toggle to Yes or No depending on whether you use this selection. Press Return.

   If Congestion Management is enabled, this option causes the Netopia Router to use in-bound FECNs (Forward Explicit Congestion Notification). This feature is designed to notify you that congestion avoidance procedures should be initiated where applicable for traffic in the same direction as the received frame. It indicates that the frame in question, has encountered congested resources.

   Note: The Congestion Management Enabled field will only appear if Standard or Buffered is selected as the option from the Tx Injection Management field.

4. Select Maximum Frame Size and press Return. The default is automatically set to a value suitable for encapsulating a full ethernet packet's transmission load, however you may change the Maximum Frame Size to suit your networks transmission load. Press Return.

You are now done configuring the Frame Relay Configuration screen. Press the Escape key to return to the WAN Setup screen. If you need to configure your DLCIs, go to the section below. Otherwise, go to "Connection Profiles for ISDN and Leased lines" on page 2-13 to set up your connection profile for a remote site.

Frame Relay DLCI configuration

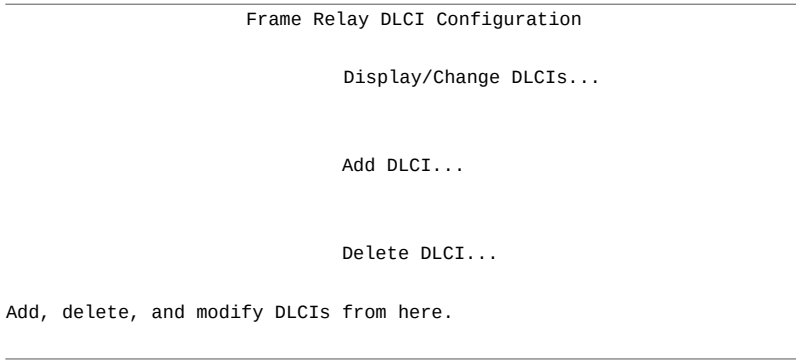
If you selected None as your LMI Type then you will need to manually configure your DLCIs.

A Frame Relay DLCI is a set of parameters that tells the Netopia Router how to initially connect to a remote destination.

The Netopia Router leased line models support up to 16 different Frame Relay DLCI configuration profiles.

Each Frame Relay DLCI configuration you set up allows the Netopia Router to connect your network to another network that uses IP or IPX over Frame Relay.

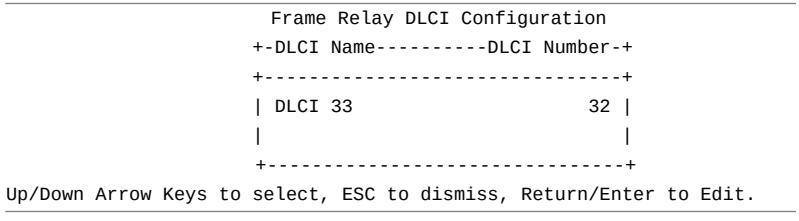
To go to the Frame Relay DLCI configuration screen, select Frame Relay DLCI Configuration in the WAN Setup screen.



Displaying a Frame Relay DLCI configuration table

To display a view-only table of the Frame Relay DLCIs, select Display / Change DLCIs in the Frame Relay DLCI Configuration screen, and press Return.

The Frame Relay DLCI Configuration table is a handy way to quickly view the DLCI names and DLCI numbers that you attribute to your Frame Relay profiles.



Changing a Frame Relay DLCI configuration

To modify a Frame Relay DLCI configuration, select Display / Change DLCIs in the Frame Relay DLCI Configuration screen.

Select a DLCI Name from the table and press Return to go to the Change DLCI screen. The parameters in this screen are the same as the parameters in the Add DLCI screen. To find out how to set them, see “Adding a Frame Relay DLCI configuration” on page 2-37.

```
                              Change DLCI

         DLCI Name:                          DLCI 33

         DLCI Enabled:                       Yes

         DLCI Number (16-991):               32

         Remote IP Address:                  2.0.0.2

Here you configure the parameters for a single DLCI (Data Link Circuit ID).
```

Deleting a Frame Relay DLCI configuration

To delete a Frame Relay DLCI configuration, select Delete DLCI in the Frame Relay DLCI Configuration screen and press Return to display the Frame Relay DLCI configuration table.

```
+-------------------------------------------------------------------------+
  |                                                                       |
  | Are you sure you want to delete this DLCI?                            |
  |                                                                       |
  |              CANCEL                         CONTINUE                  |
  |                                                                       |
  |                                                                       |

+-------------------------------------------------------------------------+
```

1. Highlight the Frame Relay DLCI configuration you wish to delete. Press Return.

2. A Frame Relay DLCI Configuration table appears with a prompt asking you if you want to delete the connection profile you have just highlighted. Select CONTINUE if you wish to delete this DLCI or CANCEL if you do not.

You are now done configuring the Frame Relay DLCI Configuration screen. Press the escape key to return to the WAN Setup screen. Go to "Connection profiles for ISDN and Leased lines," beginning on page 2-13, for information on how to configure your leased line connection.

Adding a Frame Relay DLCI configuration

To add a new Frame Relay DLCI, select Add DLCI in the Frame Relay DLCI Configuration screen. Press Return and the Add DLCI screen appears.

```
                                Add DLCI

        DLCI Name:                          DLCI 17

        DLCI Enabled:                       Yes

        DLCI Number (16-991):               17

        Remote IP Address:                  2.0.0.2

        Data Flow Parameters---------------Use Default---------Value----
        CIR:                                No                  64000
        Bc:                                 No                  64000
        Be:                                 Yes

        ADD DLCI NOW                        CANCEL

Return accepts * Tab toggles * ESC cancels.
```

1. Select DLCI Name and enter a name for this individual Frame Relay DLCI profile. It can be any name you wish. For example: the name of your ISP or remote branch your connecting to such as the corporate headquarters of your company.

Note: The Netopia Router allows Frame Relay DLCIs to be named, so that you can easily reference and differentiate them. This is accomplished by giving a DLCI Name to a DLCI Number.

```
                    Frame Relay DLCI Configuration
                     +-DLCI Name----------DLCI Number-+
                     +-------------------------------+
                     | Panost Inc.                16 |
                     | THARPER Inc.               32 |
                     |                               |
                     +-------------------------------+
Up/Down Arrow Keys to select, ESC to cancel, Return/Enter to Delete.
```

2. Select DLCI Enabled and toggle it to Yes to activate the profile. If you disable this profile, the Netopia Router will automatically disable and block access to a specific remote DLCI.
3. Select DLCI Number (16-991) and enter a number for this individual DLCI. Check with your Frame Relay provider to find out what numbers are allocated for each of your DLCI profiles. The DLCI number range should fall within the range of 16-991. For more information, refer to the Leased line worksheet that you filled out in Chapter 2 of the *Getting Started Guide*.
4. Select Remote IP Address and enter the remote IP address your ISP or network administrator gave you that represents the remote sites IP address for their router. Press Return.

If you select Standard or Buffered as the Tx Injection Management type in the Frame Relay Configuration screen go to the next bulleted item below. If you selected None in the Frame Relay Configuration screen go to step 6.

Below the Remote IP Address field, the following Data Flow Parameters appear:

- The CIR (Committed Information Rate) represents the average capacity available to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). The setting defaults to 64000, but you may modify the capacity rate by toggling the selection in the Use Default field to No. You can then enter a different capacity rate in the Value field.

- The Bc (Committed Burst Size) represents the maximum amount of data that your Frame Relay service provider agrees to transfer from a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). The setting defaults to 64000, but you may modify the committed burst size by toggling the selection in the Use Default field to No. You can then enter a different committed burst size in the Value field.
- The Be (Excess Burst Size) represents the maximum amount of data that your Frame Relay service provider will attempt to deliver to a given PVC (Permanent Virtual Circuit) or DLCI (Data Link Connection Identifier). The setting defaults to 0, but you may modify the excess burst size by toggling the selection in the Use Default field to No. You can then enter a different excess burst size in the Value field.

Note: Some Frame Relay service providers allow for over-subscription of the DLCIs, which occurs when the total number of CIRs for all PVCs exceeds the line rate set up.

5. Select ADD DLCI NOW to save the current static Frame Relay DLCI profile that you have just entered, and press Return to go back to the Frame Relay DLCI Configuration screen. Alternately, you can cancel the Frame Relay DLCI profile you have just created by selecting CANCEL to exit the Add DLCI screen.

Default profile

Netopia can answer calls as well as initiate them over switched circuits. To answer calls, Netopia uses a default profile. The default profile controls how incoming calls are set up, authenticated, filtered, and more.

For information on how to set up a default profile for a switched circuit, see the next section.

For information on how to set up a default profile for a permanent circuit, see "How the default profile works for a permanent circuit," beginning on page 2-45.

How the default profile works for a switched circuit

The Default Profile works like a guard booth at the gate to your network: it scrutinizes incoming calls. Like the guard booth, the default profile allows calls based on a set of criteria that you define.

The main criterion used to check calls is whether they match one of the connection profiles already defined. If PAP or CHAP authentication is being used, the default profile checks that the incoming call's name and password/secret match the receive name and password/secret of a connection profile. If PAP or CHAP is not being used, an incoming call is matched to a connection profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If an incoming call is matched to an existing connection profile, the call is accepted. All of that connection profile's parameters, except for authentication, are adopted for the call.

You could set up the default profile to allow calls in even if they fail to match a connection profile. Continuing the guard booth analogy, this would be like removing the guards or having them wave all calls in, regardless of their source.

If an incoming call is not required to match a connection profile, and fails to do so, it is accepted as a standard IP connection. Accepted, unmatched calls adopt the call parameter values set in the default profile.

To determine how which call parameter values unmatched calls will adopt, customize the default profile parameters in the Default Profile screen.

Customizing the default profile

You can customize the Netopia Router's default profile in the Default Profile screen.

```
                                    WAN Setup

                                Line Configuration...


                                Connection Profiles...
                                Default Answer Profile...

From here you will configure yours and the remote sites' WAN information.
```

1. Select Default Answer Profile in the WAN Setup screen. Press Return. The Default Profile screen appears.
2. To enable CNA authentication, select Calling Number Authentication in the Default Profile screen and choose one of the following settings:

   Ignored: Calling Number Authentication (CNA) is not in effect. This is the default setting.

   Preferred: Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the call proceeds as usual and the caller may still connect successfully. Use this setting if you expect to receive both regular and CNA-authenticated calls.

   Required: Authentication is attempted if the calling number is available. If authentication fails, or the calling number is not available, the Netopia Router disconnects the caller. Use this setting if you require all calls to be CNA-authenticated.

   Calling Number Authentication (CNA), is an application of CallerID. It is a method of verifying that an incoming call is originating from an expected site. Using CNA, you can increase the security of your network by requiring that callers not only possess the correct PPP authentication information, but also are calling from a particular physical location.

   CNA works by matching the actual calling number to the number entered in the Calling Number field in the answering side's connection profile. When a match occurs, the incoming call is handled by the connection profile containing the matched number.

Note: If the actual calling number and entered calling number do not have the same number of digits, CNA can still match the numbers. The smaller number determines how many digits must match. For instance, if the actual calling number is 10 digits and the entered calling number is 7 digits, only 7 digits must be matched. The 7 digits that must be matched in this example are the last 7 digits of each calling number. In this example then, the first 3 digits of the actual calling number will be ignored. This method allows the actual calling number to include prefixes and area codes without requiring the entered calling number to include them.

Calling numbers can also be matched using the wildcard character, ?, which will match any digit. For example, if you enter 555-123? in the Calling Number field, the following actual calling numbers will be matched: 555-1231, 555-1232, 555-1233, 555-1234, 555-1235, 555-1236, 555-1237, 555-1238, 555-1239, and 555-1230.

Using CNA can also provide cost savings because calls are not billed during the CNA phase. With CNA, a caller can set up a connection to the Netopia Router without incurring any charges by accessing a dial-back connection profile. If the caller's rates are higher than those charged to the Netopia Router's return call, then using CNA has saved the difference.

CNA should be available where CallerID services are available. You will need to consult with your telephone service provider to find out if your line is provisioned for CallerID.

Also note that if the calling side has instructed the phone company to block delivery of its caller ID, the answering side will not be able to authenticate.

North America models only

If you have a Northern Telecom DMS-100 line (either Custom or NI-1) you should verify that the line supports "Calling Number Delivery" service.

If your line is an AT&T 5ESS (either custom or NI-1) verify that it supports "CPN/BN (Calling Party Number/Billing Number) Delivery" service.

If your line does not support the appropriate service, CNA may not work properly.

Note: For an ISDN switched circuit with HDLC datalink encapsulation enabled, the Default Profile screen will only show the Calling Number Authentication pop-up menu.

3. To force incoming calls to match connection profiles, select Must Match a Defined Profile and toggle it to Yes. Incoming calls that cannot be matched to a connection profile are dropped. To allow unmatched calls to be accepted as standard IP or IPX connections, toggle Must Match a Defined Profile to No.

   If Must Match a Defined Profile is set to Yes, the answer profile only accepts calls that use the same authentication method defined in the Authentication item. If PAP or CHAP are involved, the caller must have a name and password or secret that match one of the connection profiles. The caller must obtain these from you or your network administrator before initiating the call.

   For example, if Must Match a Defined Profile is set to Yes, and Authentication is set to PAP, then only incoming calls that use PAP and match a connection profile will be accepted by the answer profile.

   If authentication in the default answer profile is set to CHAP, the value of the CHAP Challenge Name item must be identical to the value of the Send Host Name item of the connection profile to be matched by the caller.

   If Must Match a Defined Profile is set to No, Authentication is assumed to be None, even if you've set it to PAP or CHAP. The answer profile uses the caller's IP address to match a connection profile. However, the answer profile cannot discover a caller's subnet mask; it assumes that the caller is *not* subnetting its IP address:

   Class A addresses are assumed to have a mask of 255.0.0.0

   Class B addresses are assumed to have a mask of 255.255.0.0

   Class C addresses are assumed to have a mask of 255.255.255.0. Class C address ranges are generally the most common subnet allocated.

   If a remote network has a non-standard mask (that is, it uses subnetting), the only way for it to successfully connect to the Netopia Router is by matching a connection profile. In other

words, you will have to set up a connection profile for that network.

You can set the following default parameters for incoming calls:

- Authentication

Non-North America models only

- Force 56K on Answer
- Data Compression
- Maximum Receive Packet Size

If Must Match a Defined Profile is set to No, you can also set the following parameters for accepted calls that do not match a connection profile:

- B-Channel Usage
- Idle Timeout

ISDN switched circuit models with PPP enabled only

- BAP Usage
- Firewall Filter Set

Non-Small Office models only

- Tx RIP

Non-Small Office models only

- Rx RIP
- Net BIOS Packet Forwarding
- Net BIOS Path Delay
- Periodic RIP Timers
- Periodic SAP Timers

All of these parameters are similar to the connection profile parameters of the same names. To find out how to set them, see "Adding a Connection Profile" on page 2-16.

Note: The only options that would be offered for ISDN profiles would be applied to the Default Profile for ISDN.

How the default profile works for a permanent circuit

The default profile works like a guard booth at the gate to your network: it scrutinizes WAN connections. Like the guard booth, the default profile allows connections based on a set of criteria that you define.

The main criterion used to check connections is whether they match one of the connection profiles already defined. A connection is matched to a connection profile using the remote network's IP address (that is, the caller is defined as the destination of a particular connection profile).

If a connection matches an existing profile, all of the connection profile parameters are adopted for the call.

When using PPP or Cisco-HDLC datalink encapsulation on a permanent circuit, you must configure a connection profile. Note, that you may have already configured this connection profile in Easy Setup. See the *Getting Started Guide* for information on configuring an Easy Setup connection profile.

When using Frame Relay datalink encapsulation on a permanent circuit, you may require that the frame relay DLCIs explicitly match up to your connection profile, or you may allow your Frame Relay network to automatically confirm this by using the Default Frame Profile.

Customizing the default profile

You can customize the Netopia Router's default frame relay profile in the Default Frame Profile screen.

```
                                WAN Setup

                          Line Configuration...

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

                          Connection Profiles...
                          Default Frame Profile...

Return/Enter for default WAN connection parameters.
```

1. Select Default Frame Profile in the WAN Setup screen. Press Return. The Default Frame Profile screen appears.

```
                        Default Frame Profile


        Must Match a Defined Profile:      No

        IP Enabled:                        Yes
        IP Parameters...

        IPX Enabled:                       Yes
        IPX Parameters...

Configure Default WAN Connection Parameters here.
```

2. To force matches with connection profiles, select Must Match a Defined Profile and toggle to Yes. To allow the frame relay network to automatically configure a frame profile, toggle to No.

   If Must Match a Defined Profile is set to Yes, the fields in the Default Profile screenshot above will remain hidden.

If Must Match a Defined Profile is set to No, you can also set the following parameters for accepted calls that do not match a connection profile:

- Network Address Translation
- Interface-based Routing or System-based Routing
- Firewall Filter Set
- Transmit RIP
- Receive RIP
- TX RIP Policy to use either Split Horizon or Poison Reverse
- Net BIOS Packet Forwarding
- Net BIOS Path Delay
- Periodic RIP Timers
- Periodic SAP Timers

Call acceptance scenarios

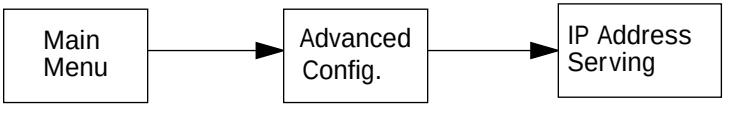
The following are a few common call acceptance scenarios and information on how to configure the router for those purposes.

- To accept all calls, regardless of whether they match a connection profile:
  - Toggle Must Match a Defined Profile to No.
- To only accept calls that match a connection profile through use of a name and password (or secret):
  - Toggle Must Match a Defined Profile to Yes, *and*
  - Set Authentication to PAP or CHAP.

  Note: The authentication method you choose determines which connection profiles are accessible to callers. For example, if you choose PAP, callers using CHAP or no authentication will be dropped by the answer profile.

- To allow calls that *only* match a connection profile's remote IP and/or IPX address:
  - Toggle Must Match a Defined Profile to Yes, *and*
  - set Authentication to None.
- To not allow *any* incoming calls to connect to the Netopia Router:
  - Toggle Must Match a Defined Profile to Yes, *and*
  - Set the Dial option in the Telco Options screen of every connection profile to Dial Out Only

WAN IP Address Serving



Small Office ISDN models only

The Netopia Router supports WAN IP Address Serving.

With WAN IP Address Serving the Netopia Router serves an IP address to an incoming call. The incoming caller can be either a TA (Terminal Adapter), such as the Netopia ISDN Modem, or another Netopia Router with the NAT (Network Address Translation) feature set. The incoming caller will dynamically obtain an IP address from a pool of IP addresses that the Netopia Router serves.

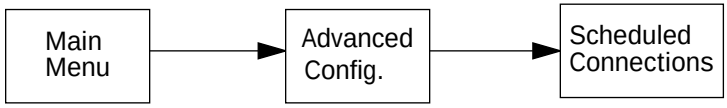
The Netopia Router serving the IP address should have a connection profile with an IP address of 0.0.0.0 defined for the calling TA or router.

```
                    IP Address Serving

IP Address Serving:                On
Server Name is                     Netopia PN435
```

To select WAN IP Address Serving, go to the IP Address Serving screen from the Advanced Configuration menu and toggle On.

Note: WAN IP Address Serving is used for *only incoming caller connections*. Refer to "IP address serving" on page 4-16, for more information on how to use WAN IP Address Serving.

Scheduled connections



You can set a Netopia Router using a switched circuit to make scheduled connections using designated connection profiles. This is useful for creating and controlling regularly scheduled periods when the router can be used by hosts on your network. It is also useful for once-only connections that you want to schedule in advance.

To go to the Scheduled Connections screen, select Scheduled Connections in the Advanced Configuration screen.

```
                    Scheduled Connections


                Display/Change Scheduled Connection...

                Add Scheduled Connection...

                Delete Scheduled Connection...
```

Viewing scheduled connections

To display a table of view-only scheduled connections, select Display / Change Scheduled Connection in the Scheduled Connections screen. Each scheduled connection occupies one row of the table.

```
                          Scheduled Connections
+-Days ----Begin At - HH:MM--- When -----Conn. Prof. NameEnabled ------+
| MTWTFSS  08:30PM    06:00    weekly    Profile 3       Forced        |
|                                                                      |
|                                                                      |
+----------------------------------------------------------------------+
```

The first column in the table shows a one-letter representation of the Days of the week, from Monday (M or m) to Sunday (S or s). If a letter representing a day is capitalized, the connection will be activated on that day; a lower-case letter means that the connection will not be activated on that day. If the scheduled connection is configured for a once-only connection, the word “once” will appear instead of the days of the week.

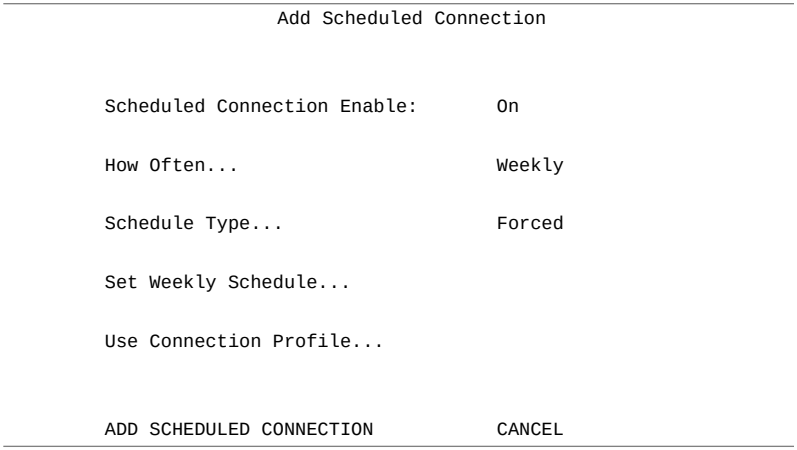
The other columns show:

- The time of day that the connection will Begin At
- The duration of the connection (HH:MM)
- Whether it’s a recurring Weekly connection or used Once Only
- Which connection profile (Conn. Prof.) is used to connect
- Whether the scheduled connection is currently Enabled

You should make sure that the Netopia Router’s system date and time are correct (see “Setting the system date and time” on page 10-2). The router checks the date and time set in scheduled connections against the system date and time.

Adding a scheduled connection

To add a new scheduled connection, select Add Scheduled Connection in the Scheduled Connections screen and go to the Add Scheduled Connection screen.



Follow these steps to configure the new scheduled connection:

- To activate the connection, select Scheduled Connection Enable and toggle it to On. You can make the scheduled connection inactive by toggling Scheduled Connection Enable to Off.
- Decide how often the connection should take place by selecting How Often and choosing Weekly or Once Only from the pop-up menu. The item directly below How Often allows you to set the exact weekly schedule or once-only schedule. If How Often is set to Weekly, the item directly below How Often reads Set Weekly Schedule. If How Often is set to Once Only, the item directly below How Often reads Set Once-Only Schedule.
- If you selected Weekly, select Schedule Type and select from the pop-up menu.

  Forced schedules the connection according to the parameters you set in the next step.

  Periodic retries the connection several times during the scheduled time.

  Demand-Allowed defines the schedule when demand calls are enabled.

Demand-Blocked defines the schedule when demand calls are prevented.

- If you selected Weekly, select Set Weekly Schedule and go to the Set Weekly Schedule screen.
- Select the days for the scheduled connection to occur and toggle them to Yes.

```
                    Set Weekly Schedule

    Monday:                              No
    Tuesday:                             No
    Wednesday:                           No
    Thursday:                            No
    Friday:                              No
    Saturday:                            No
    Sunday:                              No

    Scheduled Window Start Time:      02:08
    AM or PM:                            PM

    Call Window Duration:                00:00

    Every ...                            15 min.
```

- Select Scheduled Window Start Time and enter the time to initiate the scheduled connection. Be sure to use the same clock, either 12-hour or 24-hour, as the system time format in the Set Date and Time screen. See “Setting the system date and time” on page 10-2.

  You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o’clock. The entry 7:0 (or 7:00) would be accepted as seven o’clock, exactly. The entries 44, :5, and 2: would be rejected.

- Select AM or PM and choose AM or PM from the pop-up menu.
- Select Scheduled Window Duration and enter the maximum duration allowed for this scheduled window (not for the call).
- If you selected Periodic, select Every and choose how often the call should be attempted. The default is every 15 minutes.

  You are done configuring the weekly options. Return to the Add Scheduled Connection screen to continue.
- If you set How Often to Once Only, select Set Once-Only Schedule and go to the Set Once-Only Schedule screen.

```
                    Set Once-Only Schedule


Place Call on (DD/MM/YY):          02/11/1998

Scheduled Window Start Time:         02:08
AM or PM:                          PM

Scheduled Window Duration:           00:00
```

- Select Place Call On (DD/MM/YY) and enter a date in the format DD/MM/YY (day, month, year).

  Note: You must enter the date in the format specified. The slashes are mandatory. For example, the entry 5/1/95 would be accepted as January 5, 1995. The entry 1/6 would be rejected.
- Select Schedueld Window Start Time and enter the time to initiate the scheduled connection.

  Note: You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

- Select AM or PM and choose AM or PM. The AM or PM item appears only if the time is in the 12-hour clock format.
- Select Scheduled Window Duration and enter the maximum duration allowed for this scheduled window (not for the call). Use the same format restrictions noted above.

  You are done configuring the once-only options. Return to the Add Scheduled Connection screen to continue.
- In the Add Scheduled Connection screen, select Use Connection Profile and choose from the list of connection profiles you have already created. A scheduled connection must be associated with a connection profile to be useful. The connection profile becomes active during the times specified in the associated scheduled connection, if any exists.
- Select ADD SCHEDULED CONNECTION to save the current scheduled connection. Select CANCEL to exit the Add Scheduled Connection screen without saving the new scheduled connection.

Modifying a scheduled connection

To modify a scheduled connection, select Display / Change Scheduled Connection in the Scheduled Connections screen to display a table of scheduled connections.

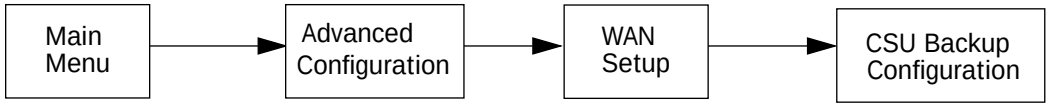
Select a scheduled connection from the table and go to the Change Scheduled Connection screen. The parameters in this screen are the same as the ones in the Add Scheduled Connection screen (except that ADD SCHEDULED CONNECTION and CANCEL do not appear). To find out how to set them, see “Adding a scheduled connection” on page 2-51.

Deleting a scheduled connection

To delete a scheduled connection, select Delete Scheduled Connection in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press the Return key to delete it. To exit the table without deleting the selected scheduled connection, press the Escape key.

CSU Backup



When you are using the leased line interfaces T1 and DDS, you can configure an automatic CSU backup, to switch to the SA port during a leased line failure.

```
                    CSU Backup Configuration


Enable SA Port as CSU Backup        Yes
Requires Data Link Failure of...    30 Sec

Circuit Type...                     Switched Async

Data Rate (kbps)...                 57.6

Modem Initialization String:        AT&C1&D2E0S0=1
Modem Dialing Prefix:               ATDT

Data Link Encapsulation is          Async PPP
```

In the CSU Backup Configuration Screen, follow these steps to enable the SA port as the CSU backup.

1. Select Enable SA Port as CSU Backup and toggle it to Yes.
2. Select Requires Data Link Failure of. From the pop-up menu, select how long the failure must be to enable the backup. The default is 30 seconds.
3. The remaining fields configure the SA port. See “Line configuration for an SA/Serial line” on page 2-7 for more information.

Chapter 3

Connecting Your Local Network

In this chapter, you will learn how to physically connect the Netopia Router to your local area network (LAN). Before you proceed, make sure the Netopia Router is properly configured. You can configure the Router using Console-based Management or Web-based Management (see the *Getting Started Guide*).

Overview

You can connect the Netopia Router to an IP or IPX network that uses Ethernet. You can connect to the Router's Ethernet ports with either a PC LAN using IP over Ethernet or Apple Macintosh computers using native IP.

You can also connect the Router to an AppleTalk network that uses either Ethernet or LocalTalk. AppleTalk networks based on Ethernet cabling (EtherTalk) connect to all models of the Router through the Ethernet port.

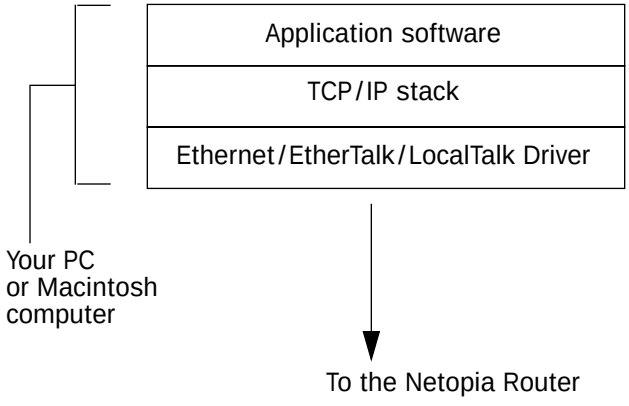
AppleTalk networks based on LocalTalk cabling connect to the 400 series models through the PhoneNET port. If you have both kinds of AppleTalk networks, you can connect the LocalTalk network to the Netopia Router's PhoneNET port and the AppleTalk (EtherTalk) network to the Ethernet ports. AppleTalk traffic will be routed between these two networks.

Caution! Before connecting the Netopia Router to any AppleTalk LANs that contain other AppleTalk routers, you should read "Routers and seeding" in "Routers and seeding" on page 6-5.

See the sections later in this chapter for details on how to connect the Netopia Router to the two types of networks.

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia Router. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora Light e-mail client, and the web browsers Microsoft's Internet Explorer and Netscape Navigator.

TCP/IP stack: This is the software that lets your PC or Macintosh communicate using Internet protocols. TCP/IP stacks must be configured with some of the same information you used to configure the Netopia Router. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. Macintosh computers use either MacTCP or Open Transport.

Ethernet: Ethernet hardware and software drivers enable your PC or Macintosh computer to communicate on the LAN.

EtherTalk and LocalTalk: These are AppleTalk protocols used over Ethernet.

Once the Netopia Router is properly configured and connected to your LAN, PC and Macintosh computers that have their required components in place will be able to connect to the Internet or other remote IP networks.

Connecting to a LocalTalk network—for 400 series models

Connect one end of the LocalTalk cable to the Netopia Router's PhoneNET port. Connect the other end of the cable to your LocalTalk network.

If your LocalTalk network is not based on standard PhoneNET cabling, use a PhoneNET-to-LocalTalk adaptor cable. Connect the adaptor cable's RJ-11 connector to the Netopia Router. Connect the cable's mini-DIN-3 connector to your LocalTalk network.

The PhoneNET port is terminated, so the Netopia Router should only be used at the end of your LocalTalk network. Be sure to observe the standard rules governing maximum cable lengths and limits on the number of nodes on a PhoneNET network.

Note: Make sure you *do not* connect your LocalTalk network to the Telco port, one of the EtherWave ports, or one of the POTS (Phone 1 and 2) ports.

Connecting to an Ethernet network

The Netopia Router supports an Ethernet connection to either its AUI or its EtherWave ports. The Router's autosensing feature eliminates the need for a switch; connection to the AUI or EtherWave ports is automatically detected and the connected port is used.

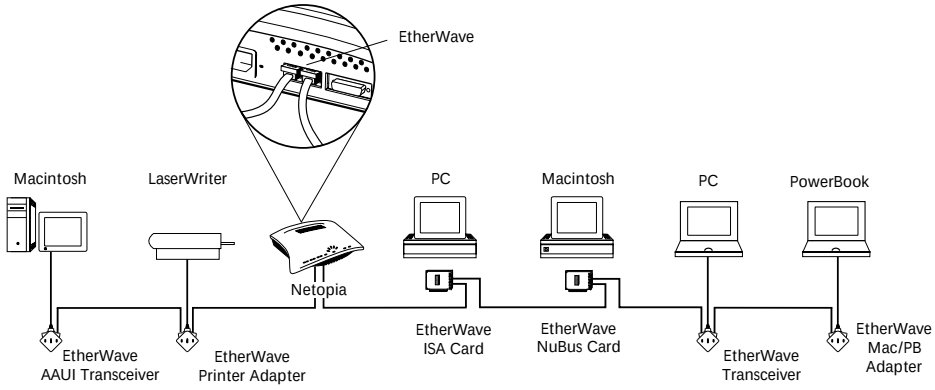
You can connect several types of Ethernet networks to the Netopia Router. Most are distinguished by the type of cable they use. The table below displays some important attributes of four types of Ethernet.

Attribute	EtherWave	10Base-T	10Base-2 (thin)	10Base-5 (thick)
Max. length of backbone, branch, or end to end (cable length)	330 feet (100 meters)	330 feet (100 meters)	600 feet (185 meters)	1500 feet (450 meters)
Cable type	Twisted pair (10Base-T)	Twisted pair (10Base-T)	Flexible (thin) coaxial	Coaxial (thick)
Netopia Router port used	EtherWave	EtherWave	AUI	AUI
Other restrictions	Maximum 8 devices (daisy chained)	No daisy chain	Requires transceiver	Requires transceiver

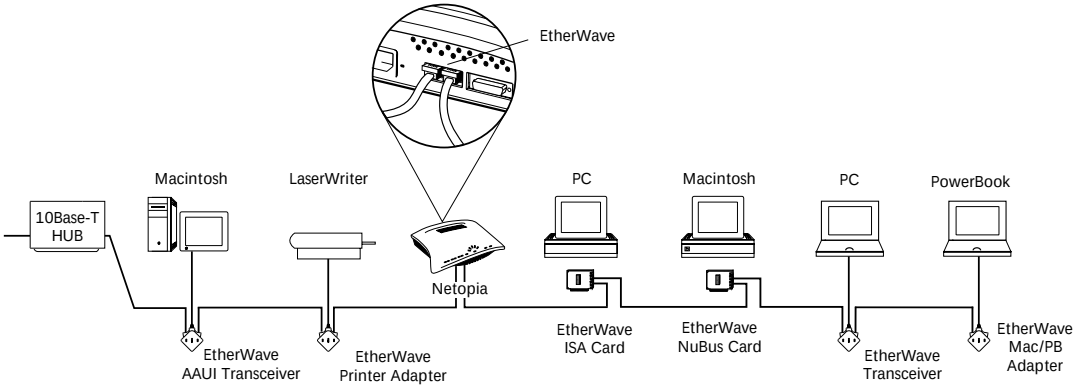
Caution! Do *not* connect to both the AUI and EtherWave ports. Connect to *either* the AUI port *or* to the EtherWave ports. Connecting to both the AUI and EtherWave ports will result in communications errors on the networks connected to these ports.

EtherWave

To add the Netopia Router to your EtherWave daisy chain, use a 10Base-T cable with RJ-45 connectors. The router can be connected to your EtherWave network at any point in the daisy chain.

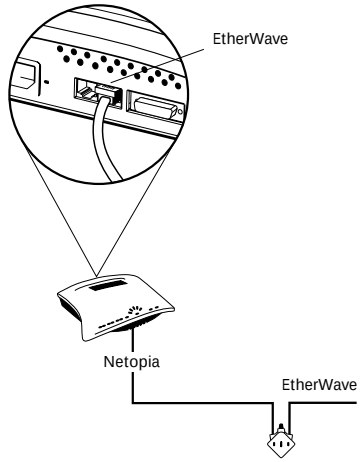


The Netopia Router in the middle of an EtherWave daisy chain



The Netopia Router in the middle of an EtherWave daisy chain that's part of a larger network

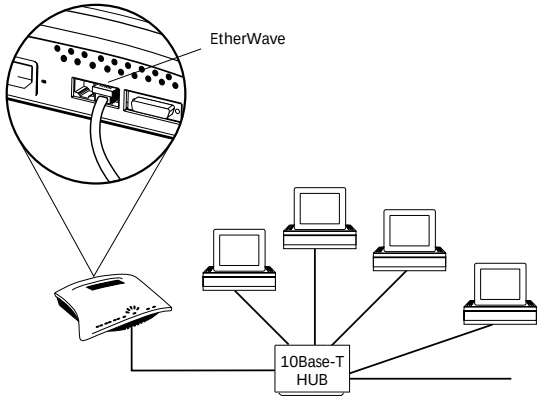
You may use either or both of the EtherWave ports to connect the Netopia Router, as needed. No termination is necessary, even when the router is at the end of your EtherWave network.



The Netopia Router at the end of an EtherWave daisy chain

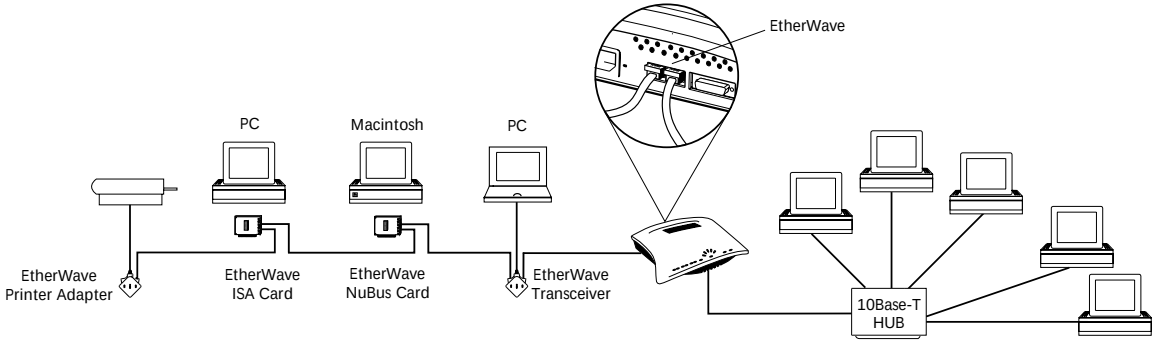
10Base-T

You can connect a 10Base-T Ethernet network to the Netopia Router either through one of its EtherWave ports or through its AUI port.



The Netopia Router in a 10Base-T network

To connect your 10Base-T network to the Netopia Router through its EtherWave port, use a 10Base-T cable with RJ-45 connectors. You may connect your 10Base-T network to either EtherWave port.



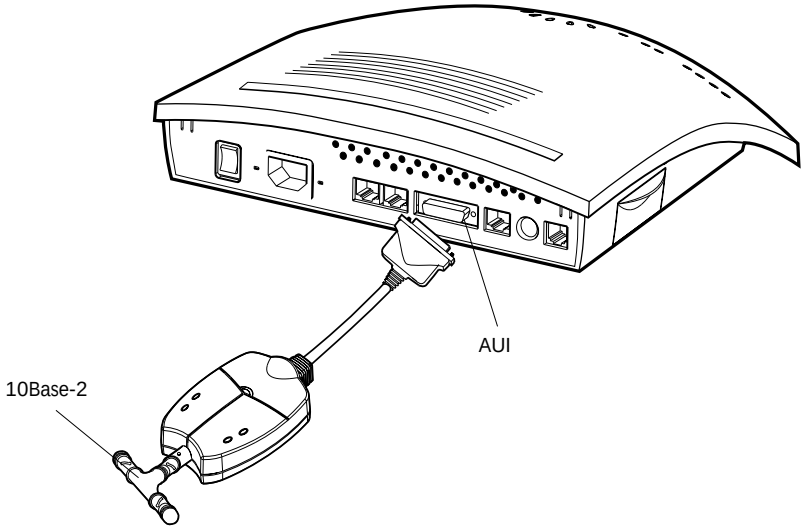
When there are no more free ports on the 10Base-T hub, the network can be extended using EtherWave.

Thick and Thin Ethernet

You can connect a 10Base-5 (Thick Ethernet) or 10Base-2 (Thin Ethernet) network to the Netopia Router's AUI port.

To connect your 10Base-5 network to the Netopia Router's AUI port, use a standard Ethernet 10Base-5 transceiver and cable.

To connect your 10Base-2 network to the Netopia Router's AUI port, use a standard Ethernet 10Base-2 transceiver and cable.



Connecting to a 10Base-2 network using Farallon's EtherMac™ Transceiver

Chapter 4

IP Setup

The Netopia Router uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the Router to effectively route IP traffic. You also learn how to configure the Router to serve IP addresses to hosts on your local network.

Some models of the Netopia Router support the SmartIP feature, which includes Network Address Translation (NAT).

NAT is a powerful feature that allows the user to represent an entire LAN to the outside world as a single IP address. Instead of having an ISP assign a separate IP address for each computer on the network, the ISP provides one public IP address called a proxy address. Each computer then has a separate private IP address, but uses the proxy address to communicate with the outside world.

Key Features of IP Network Address Translation (NAT)

- NAT is selectable on a per connection basis, optionally allowing real addresses to be used for intranet connections and proxied addresses to be used for Internet connections.
- The NAT user can use any combination of proxied and unproxied addresses simultaneously with ISDN on the two B-channels. For instance, one unproxied address connection profile can be used to connect to a central office, while another proxied address connection profile can simultaneously connect the user's Netopia Router and LAN to the Internet.

- The single proxy address is acquired at connection time from the answering side. The address can be assigned by the remote router from either a dynamic pool of addresses or a fixed, static address.
- Static NAT (Network Address Translation) Security is made simpler and more reliable by only having to firewall one IP address and by obscuring the internal network structure from the Internet.

Using NAT

Follow these steps to use NAT.

1. Pick a network number for your local (internal) network. This can be any IP address range you want. For this example, we will use 10.0.0.0.

   Note: The outside world (the external network) will not see this network number.

2. Using the internal network number, assign addresses to the local nodes on your LAN. For example, you may assign
   - 10.0.0.1 to your Netopia Router
   - 10.0.0.2 to a node running as a World Wide Web server
   - 10.0.0.3 to an FTP server
   - 10.0.0.4 to a Macintosh computer
   - 10.0.0.5 to a Windows 95 PC
3. Create a connection profile for your ISP or other remote network. See “Adding a Connection Profile” on page 2-16. In the IP Profile Parameters screen, toggle Address Translation Enabled to Yes, to turn on NAT for this profile.
4. When your Netopia Router calls the ISP, the remote router that answers the call assigns your Netopia Router an IP address that external users use to communicate with your network. To view this address, go to the QuickView menu and check More Info in the Current Status section of the profile.

In the following example screen, 192.163.100.6 is assigned to the calling Netopia Router.

Note: The QuickView screen varies by your Netopia Router model and line type.

```
                                  Quick View

Ethernet Address - 00-00-c5-ff-60-8d  Current Date - 5/31/97 03:09:43PM
Firmware Version --  3.0

IP Address - 163.176.8.128             AppleTalk ET Address - 33051:150
IPX Network Address - 00000000         AppleTalk LT Address - 33050:149


                        Current ISDN Connection Status
---Profile Name-------State--%Use---Remote Address--------Est.----More Info-----
ISP                    B1      10   IP 192.163.4.1         Lcl  NAT 192.163.100.6


                                  LED Status
 -----ETHERNET------+--CH1-----MGMT----CH2---+-CARD-+-PWR +-------LEDS--------
 LNK LNK TX COL AUI   RX LNK  RDY TX  RX LNK              |'-'= Off 'E'= Error
  -   -   -   -   -     -  -    E   -   -  -      -     O  |'O' = On '*'= Blink
```

Internal users can access the Internet as they always do; the external Internet, however, views all traffic that the computers generate on the internal network as originating from 192.163.100.6. Similarly, all traffic received by your Netopia Router on that network is addressed to 192.163.100.6.

Associating port numbers with nodes

When an IP client, such as a Netscape or Microsoft Internet Explorer web browser, wants to establish a session with an IP server, such as a web server, the client must know the IP address to use and the IP port where the traffic is to be directed.

Just as an IP address specifies a particular computer on a network, ports are addresses that specify a particular service in a computer. There are many universally agreed-upon ports assigned to various services. For example:

- Web servers use port number 80.
- FTP servers use port number 21.
- Telnet uses port number 23.
- SNMP uses port number 161.

The Netopia Router lets you associate these and other port numbers with nodes on your internal LAN. See page 4-8 for details on how to accomplish this.

NAT guidelines

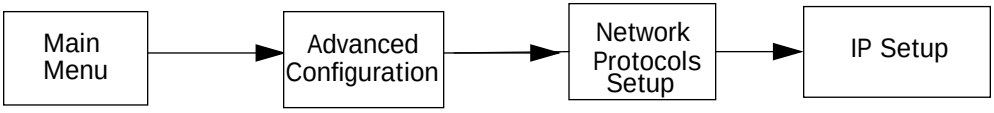
Observe the following guidelines when using Network Address Translation.

- The router can export just one local IP address per TCP port, so you can have just one machine available for a given service, such as one FTP server. However, some services, such as Web servers (www-http servers), allow you to change the TCP port on both the server and client. With two different TCP ports exported, you can have Web servers on two different IP hosts.
- Associate your primary Domain Name Server (DNS) with whichever profile is more accessible. If neither profile is dial-on-demand, you may associate a secondary DNS with the other profile.

You can enable Network Address Translation on one connection profile, disable it on another, and use the two profiles simultaneously. The profiles might have the following attributes:

- A profile with Network Address Translation disabled connects to your branch or main office. Your company network administrator has assigned you a local IP address range that is consistent with the address space assigned to your company so that you seamlessly integrate when connected. The remote IP address and mask for this profile define only the company's address space, so that the only IP traffic you send over this connection is for hosts and servers within your company.
- A Network Address Translation profile connects to the Internet via an ISP. Even though the ISP assigns you a dynamic address each time you connect, there will be no address space conflict, since Network Address Translation hides the corporate address you use locally. You enter the ISP's remote IP address as your default IP gateway so that any IP traffic not intended for your corporate intranet will be directed to the ISP.

IP setup



The IP Setup options screen is where you configure the Ethernet side of the Netopia Router. The information you enter here controls how the Router routes IP traffic.

Consult your network administrator or Internet Service Provider to obtain the IP setup information (such as the Ethernet IP Address, Ethernet Subnet Mask, Default IP Gateway and DNS Server IP Address) you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia Router is reset.

To go to the IP Setup options screen, from the Main Menu select Advanced Configuration and then select Network Protocols Setup and then select IP Setup.

Note: If you have completed Easy Setup, the information you have already entered will appear in the IP Setup options screen.

Small Office models only

```
                              IP Setup


Ethernet IP Address:              192.168.6.137
Ethernet Subnet Mask:             255.255.255.248

Default IP Gateway:               0.0.0.0

DNS Server:                       0.0.0.0
Secondary DNS Server:             0.0.0.0
Domain Name:

Exported Services...
```

Follow these steps to configure IP Setup for your Small Office Netopia Router:

- Select Ethernet IP Address and enter the IP address for the Netopia Router's Ethernet port.
- Select Ethernet Subnet Mask and enter the subnet mask for the Ethernet IP Address that you entered in the last step.
- Select Default IP Gateway and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia Router.

  A default gateway should be able to successfully route packets when the Netopia Router cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.
- Select DNS Server and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).

- If a secondary DNS server is available, select Secondary DNS Server and enter its IP address. The secondary DNS server is used by the Netopia Router when the primary DNS server is inaccessible. Entering a secondary DNS is useful but it is not necessary.
- Select Domain Name and enter your network's domain name (for example, farallon.com). Entering a Domain Name is strongly recommended.

Models supporting SmartIP only

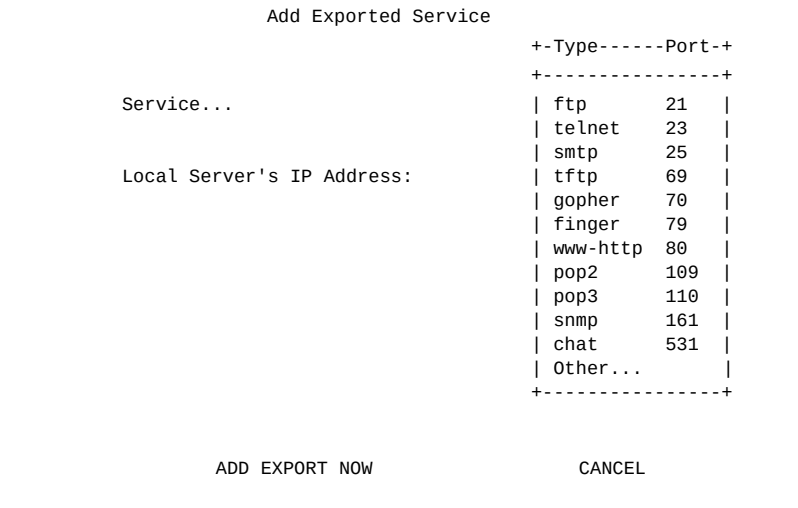
- Select Exported Services. The Exported Services screen appears with three options, Show/Change Exports, Add Export, and Delete Export.

```
                    Exported Services
          (Local Port to IP Address Remapping)

                    Show/Change Exports...

                    Add Export...

                    Delete Export...
```

- Select Add Export. The Add Exported Service screen appears.

```
                  Add Exported Service

        Service...

        Local Server's IP Address:    0.0.0.0

              ADD EXPORT NOW          CANCEL
```

- Select Service. A pop-up menu of services and ports appears.



Select any of the services/ports and press Return to associate it with the address of a server on your local area network. Press the Escape key when you are finished configuring Exported Services to go back to the IP Setup screen.

Non-Small Office models only

```
                                IP Setup


        Ethernet IP Address:              192.168.6.137
        Ethernet Subnet Mask:             255.255.255.248

        Default IP Gateway:               0.0.0.0

        DNS Server:                       0.0.0.0
        Secondary DNS Server:             0.0.0.0
        Domain Name:



        Receive RIP:                      Off
        Transmit RIP:                     Off

        Static Routes...


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

Follow these steps to configure IP Setup for your Corporate Netopia Router:

- Select Ethernet IP Address and enter the IP address for the Netopia Router's Ethernet port.
- Select Ethernet Subnet Mask and enter the subnet mask for the Ethernet IP Address that you entered in the last step.
- Select Default IP Gateway and enter the IP address for a default gateway. This can be the address of any major router accessible to the Netopia Router.

  A default gateway should be able to successfully route packets when the Netopia Router cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.

- Select DNS Server and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, www.netopia.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).
- If a secondary DNS server is available, select Secondary DNS Server and enter its IP address. The secondary DNS server is used by the Netopia Router when the primary DNS server is inaccessible. Entering a secondary DNS is useful but it is not necessary.
- Select Domain Name and enter your network's domain name (for example, farallon.com). Entering a Domain Name is strongly recommended.

Non-Small Office models only

- If there are IP routers on your Ethernet network that the Netopia Router needs to recognize, select Receive RIP and toggle it to On. With Receive RIP on, the Netopia Router's Ethernet port will accept routing information provided by Routing Information Protocol (RIP) packets. RIP is used on all Netopia Router models except the SO-Smart models.

Non-Small Office models only

- If you want the Netopia Router to advertise its routing table to other routers via RIP, select Transmit RIP and toggle it to On. With Transmit RIP on, the Netopia Router will generate RIP packets to those other routers.

Non-Small Office models only

- Select Static Routes to manually configure IP routes. See the following section.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia Router how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia Router (see "IP routing table" on page 9-13).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

To go to the Static Routes screen, select the Static Routes item in the IP Setup screen.

```
                              Static Routes


                      Display/Change Static Route...

                      Add Static Route...

                      Delete Static Route...



Configure/View/Delete Static Routes from this and the following Screens.
```

Viewing static routes

To display a view-only table of static routes, select Display / Change Static Route in the Static Routes screen.

```
     +-Dest. Network---Subnet Mask-----Next Gateway----Priority-Enabled-+
     +-------------------------------------------------------------------+
     | 0.0.0.0         0.0.0.0         163.176.8.1     Low      Yes     |
     |                                                                   |
     |                                                                   |
     |                                                                   |
     +-------------------------------------------------------------------+

Select a Static Route to modify.
```

The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the router that will be used to reach the destination network.

Priority: An indication whether the Netopia Router will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication whether the static route should be installed in the IP routing table.

Adding a static route

To add a new static route, select Add Static Route in the Static Routes screen and go to the Add Static Route screen.

```
                          Add Static Route

    Static Route Enabled:                        Yes
    Destination Network IP Address:              0.0.0.0
    Destination Network Subnet Mask:             0.0.0.0
    Next Gateway IP Address:                     0.0.0.0
    Route Priority...                            High
    Advertise Route Via RIP:                     No

              ADD STATIC ROUTE NOW        CANCEL


Configure a new Static Route in this Screen.
```

- To install the static route in the IP routing table, select Static Route Enabled and toggle it to Yes. To remove the static route from the IP routing table, select Static Route Enabled and toggle it to No.
- Be sure to read the rules on the installation of static routes in the IP routing table. See “Rules of static route installation” on page 4-15.
- Select Destination Network IP Address and enter the network IP address of the destination network.

- Select Destination Network Subnet Mask and enter the subnet mask used by the destination network.
- Select Next Gateway IP Address and enter the IP address for the router that the Netopia Router will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select Route Priority and choose High or Low. High means that the static route takes precedence over RIP information; Low means that the RIP information takes precedence over the static route.
- If the static route conflicts with a connection profile, the connection profile will always take precedence.
- To make sure that the static route is known only to the Netopia Router, select Advertise Route Via RIP and toggle it to No. To allow other RIP-capable routers to know about the static route, select Advertise Route Via RIP and toggle it to Yes. When Advertise Route Via RIP is toggled to Yes, a new item called RIP Metric appears below Advertise Route Via RIP.

  With RIP Metric you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting RIP Metric to 1 means that a route can involve 15 routers, while setting it to 15 means a route can only involve one router.
- Select ADD STATIC ROUTE NOW to save the new static route, or select CANCEL to discard it and return to the Static Routes screen.
- Up to 16 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in Advanced Configuration.

Modifying a static route

To modify a static route, select Display / Change Static Route in the Static Routes screen to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see “Adding a static route” on page 4-13).

Deleting a static route

To delete a static route, select Delete Static Route in the Static Routes screen to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press the Escape key.

Rules of static route installation

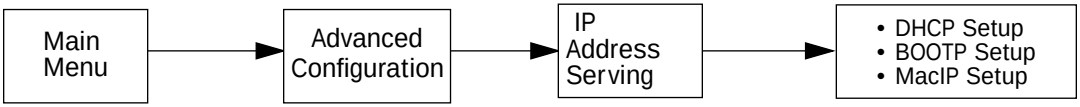
The Netopia Router applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route’s Next Gateway IP Address matches the IP address used by a connection profile or the Netopia Router’s Ethernet port.
- The static route’s Next Gateway IP Address matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.
- The static route’s Next Gateway IP Address is determined to be unreachable by the Netopia Router.
- The static route’s route information conflicts with a connection profile’s route information.
- The connection profile associated with the static route is set for dial-in connections only, and there is no incoming call connected to that connection profile.

- The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

IP address serving



In addition to being a router, the Netopia Router is also an IP address server. There are four protocols it can use to distribute IP addresses.

- The first, called Dynamic Host Configuration Protocol (DHCP), is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are "leased" or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called BOOTP (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BOOTP address assignments are "permanent" since there is no lease renewal mechanism in BOOTP.

- The third protocol, called IPCP, is part of the PPP/MP suite of wide area protocols used for ISDN WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.
- The fourth protocol, called MacIP, is used only for computers on AppleTalk networks. MacIP provides a protocol translation (or gateway) function between IP and AppleTalk as well as an IP address assignment mechanism. Like DHCP, MacIP address assignments are normally temporary, although you may also use static IP addresses with MacIP.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia Router, and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

To go to the IP Address Serving screen, select IP Address Serving in the Advanced Configuration screen and press Return.

```
                        IP Address Serving

        Server Name is                    Netopia PN455 #221393

        Number of Client IP Addresses:    5
        1st Client Address:               163.176.56.90

        Serve DHCP Clients:               Yes
        DHCP Serving Options...
        DHCP NetBios Options...

        Serve BOOTP Clients:              Yes

        Serve Dynamic WAN Clients         Yes

        Serve MacIP/KIP Clients:          Yes
        MacIP/KIP Static Options...

Configure DHCP, BOOTP, WAN IP, and/or MacIP Address Serving here.
```

Follow these steps to configure IP Address Serving:

- Server Name is lists the Netopia Router's name, model number and individual serial number. It is filled in automatically.

Small Office models only

- To serve IP addresses to clients, select IP Address Serving and toggle it to Yes. Activating IP Address Serving automatically enables DHCP, WAN clients, and dynamic MacIP/KIP clients (if you have an AppleTalk model).
- Select Number of Client IP Addresses and enter the total number of contiguous IP addresses that the Netopia Router will distribute to the client machines on your local area network.
- In the screen example shown above, five Client IP addresses have been allocated.
- Select 1st Client Address and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may first want to figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BOOTP and or MacIP.
- Example: Your ISP has given your Netopia Router the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on understanding IP addressing refer to Appendix C). Your address range will be from .137-.143. In this example you would enter 192.168.6.138 as the 1st client address.

Non-Small Office models

- To enable DHCP, select Serve DHCP Clients and toggle it to Yes. DHCP serving is automatic for other models when IP Address Serving is enabled.

Non-Small Office models only

- If Yes is selected in Serve DHCP Clients, select DHCP Serving Options item and press Return. The DHCP Options screen appears.

```
                    DHCP Options

Serve Domain Name:                Yes
Domain Name:

Serve Default Gateway:            Yes
Default Gateway:                  192.168.6.137

Serve DNS Servers:                Yes
Primary DNS Server IP Addr.:      163.176.4.10
Secondary DNS Server IP Addr.:    0.0.0.0
```

The DHCP Options screen offers a set of parameters that can be passed to each client requesting an IP address. These additional parameters simplify each client's setup.

- Select Serve Domain Name, toggle to Yes, and press Return. By toggling this item to Yes, once the domain name is entered the Netopia Router will send this information to client machines requesting it. (Note that you will need to configure each client machine for the Netopia Router and clients to communicate with each other).
- In the Domain Name menu item, type in the domain name that will be used on your network. For example: farallon.com.
- Select Serve Default Gateway, toggle to Yes, and press Return.
- In the Default Gateway menu item,enter the IP address of the Netopia Router.
- Select Serve DNS Servers, toggle to Yes, and press Return. By toggling this item to Yes, once the DNS Server's IP address or addresses (Primary and Secondary DNS Server IP Address) are entered the Netopia Router will automatically broadcast this information to the client machine. (Note that you will need to configure each client machine for the Netopia Router).
- In the Primary DNS Server IP Address menu item, the Primary DNS Server IP Address will be automatically generated from the connection profile screen if one has been entered.

- In the Secondary DNS Server IP Address menu item, the Secondary DNS Server IP Address will be automatically generated from the connection profile screen, if an address has been entered. (A secondary DNS IP address is not required, but may be helpful. For instance, if the Netopia Router attempts to communicate to the primary DNS but it is unavailable, then it will attempt to communicate with the secondary DNS. If the secondary DNS is available and the IP address is resolved than the Netopia will be able to connect to the ISP or remote network.)

You are now finished setting up DHCP Options. To return to the IP Address Serving screen press the Escape key once.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia Router to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications, a variety of "hooks" to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM's NetBIOS calls.

- Select Serve NetBIOS Options and press Return. The DHCP NetBIOS Options screen will appear.

```
                        DHCP NetBios Options


        Serve NetBios Type:                Yes
        NetBios Type...                    Type B

        Serve NetBios Scope:               No
        NetBios Scope:

        Serve NetBios Name Server:         No
        NetBios Name Server IP Addr:       0.0.0.0
DHCP allows you to allocate IP Addresses dynamically.
```

- To serve DHCP clients with the type of NetBIOS used on your network, select Serve NetBIOS Type and toggle it to Yes.
- From the NetBIOS Type pop-up menu, select the type of NetBIOS used on your network.

```
                        DHCP NetBios Options

                                          +--------+
        Serve NetBios Type:               +--------+
        NetBios Type...                   | Type B |
                                          | Type P |
        Serve NetBios Scope:              | Type M |
        NetBios Scope:                    | Type H |
                                          +--------+
        Serve NetBios Name Server:          No
        NetBios Name Server IP Addr:        0.0.0.0
```

- To serve DHCP clients with the NetBIOS scope, select Serve NetBIOS Scope and toggle it to Yes.

  Select NetBIOS Scope and enter the scope.
- To serve DHCP clients with the IP address of a NetBIOS name server, select Serve NetBIOS Name Server and toggle it to Yes.

  Select NetBIOS Name Server IP Address and enter the IP address for the NetBIOS name server.

You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen press the Escape key once.

- To enable BOOTP's address serving capability, select Serve BOOTP Clients and toggle to Yes.

  Note: Addresses assigned through BOOTP are permanently allocated from the IP Address Serving pool. To release these addresses, toggle Serve BOOTP Clients to No and restart your Netopia Router.

MacIP (Kip Forwarding) Options

When hosts using AppleTalk (typically those using LocalTalk) are not directly connected to an IP network (usually an ethernet), they must use a MacIP (AppleTalk-IP) gateway. Such a service is provided by AppleTalk models of the Netopia Routers. A MacIP gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. The MacIP gateway can also distribute IP addresses to AppleTalk computers on the network.

Note: Macintosh computers that have LocalTalk or EtherTalk selected in the MacTCP control panel, or "AppleTalk (MacIP)" selected in the TCP/IP control panel, must use the MacIP gateway to communicate with the Internet or any other IP network. Users should point their MacTCP or TCP/IP control panel to look in the LocalTalk zone for the MacIP server. Macintosh computers that have Ethernet selected in the MacTCP or TCP/IP control panel can do their own AppleTalk-IP conversions.

Setting up MacIP involves choosing MacIP dynamic address serving and then configuring that type. KIP forwarding is simply a method for distributing IP addresses to AppleTalk clients.

To go to the MacIP Setup screen, select MacIP/KIP Clients in the IP Address Serving screen from the Advanced Configuration menu.

Non-Small Office AppleTalk models only

- Select Serve Mac IP/KIP Clients and toggle to Yes, to enable MacIP/KIP address serving capability. This option is automatically enabled on Small Office models if AppleTalk and IP Address Serving are enabled.

Non-Small Office AppleTalk models only

- Select MacIP/KIP Static Options and press Return. The MacIP (KIP) Forwarding Setup screen tells the Netopia Router how many static addresses to allocate for MacIP/KIP clients. The addresses must fall within the address pool from the previous screen. You will need to enter the number of static MacIP addresses to reserve in this screen. Note that the address pool IP range will also be listed for your referral in this screen.

```
                    MacIP (KIP) Forwarding Setup

This screen tells the Netopia how many static addresses to allocate for
MacIP/KIP clients. The addresses must fall within the address pool from the
previous screen -- 163.176.56.90 to 163.176.56.94.

        Number of Static Addresses:        0

        First Static Client Address:       0.0.0.0


Reserve static MacIP addresses for KIP Forwarding here.
```

You have finished setting up IP Setup.

Chapter 5

IPX Setup

Internetwork Packet Exchange (IPX) is the network protocol used by Novell NetWare networks. This chapter shows you how to configure the Netopia Router for routing data using IPX. You also learn how to configure the router to serve IPX network addresses.

The Netopia Router supports the following IPX features:

- IPX RIP and SAP
- NetBIOS broadcast packet forwarding (IPX type 20)
- IPX packet filtering definable by source and destination IPX address and socket number, for added security
- IPX SAP filtering to aid in optimizing WAN bandwidth
- Dial-on-demand features:
  - Spoofing of IPX keep-alive, SPX, and server serialization packets
  - Configurable RIP/SAP timers on connection profiles

IPX Definitions

This section defines IPX-related protocols such as RIP, SAP and NetBIOS, in addition to other related terms. See the next section for setup instructions.

Internetwork Packet Exchange (IPX)

IPX is a datagram, connectionless protocol that Novell adapted from Xerox Network System's (XNS) Internet Datagram Protocol (IDP). IPX is dynamically routed, and the routing architecture works by "learning" network addressing automatically.

IPX address

An IPX address consists of a network number, a node number, and a socket number. An IPX network number is composed of eight hexadecimal digits. The network number must be the same for all nodes on a particular physical network segment. The node number is composed of twelve hexadecimal digits and is usually the hardware address of the interface card. The node number must be unique inside the particular IPX network. Socket numbers correspond to the particular service being accessed.

Socket

A socket in IPX is the equivalent of a port in TCP/IP. Sockets route packets to different processes within a single node. Novell has reserved several sockets for use in the NetWare environment:

Field Value	Packet Type	Description
00h	Unknown Packet Type	Used for all packets not classified by any other type
01h	Routing Information Packet	Unused for RIP packets
04h	Service Advertising Packet	Used for SAP packets
05h	Sequenced Packet	Used for SPX packets
11h	NetWare Core Protocol Packet	Used for NCP packets
14h	Propagated Packet	Used for Novell NetBIOS

Routing Information Protocol (RIP)

RIP, which was also derived from XNS, is a protocol that allows for the bidirectional transfer of routing tables and provides timing information (ticks), so that the fastest route to a destination can be determined. IPX routers use RIP to create and dynamically maintain databases of internetwork routing information. See the last section in this chapter for more information on routing tables.

Service Advertising Protocol (SAP)

SAP is a protocol that provides servers and routers with a method to exchange service information. Using SAP, servers advertise their services and addresses. Routers collect this information to dynamically update their routing tables and share it with other routers. These broadcasts keep all routers on the internetwork synchronized and provide real-time information on accessible servers on the internetwork.

The following is a list of common SAP server types:

Unknown	0000h
Print Queue	0003h
File Server	0004h
Job Server	0005h
Print Server	0007h
Archive Server	0009h
Remote Bridge Server	0024h
Advertising Print Server	0047h
Reserved Up To	8000h

NetBIOS

NetBIOS is a protocol that performs tasks related to the Transport and Session layers of the OSI model. It can operate over IPX, using a special broadcast packet known as "IPX Packet type 20" to communicate with IPX NetBIOS servers.

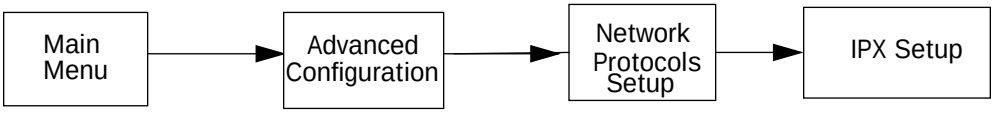
IPX Spoofing

Applicable only to ISDN switched lines

The Netopia has several IPX features designed to restrict the traffic on the ISDN link when the unit is not sending or receiving IPX data. When the link is idle and a user is logged into a Novell server, the server will send "keep alive" packets to ensure the user is still there. If the link is idle, the "keep alive" packets will be sent back to the server by the locally connected Netopia router as though they came back from the user without bringing up the ISDN link.

Similarly, "SPX keep alive" packets are treated in this manner. IPX RIP, and SAP messages will not be sent if the link is down. Together these features enable the user to remain connected to a Novell server or SPX peer without bringing up the ISDN link, except to send and receive actual user data.

IPX setup



The IPX Setup screen is where you configure the Ethernet side of the Netopia Router. The information you enter here controls how the Router routes IPX traffic.

Consult your network administrator for the IPX setup information you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia Router is reset.

To go to the IPX Setup screen, from the Main Menu select Advanced Configuration and then select Network Protocols Setup and then select IPX Setup.

Note: If you have completed Easy Setup, the information you have already entered will appear in the IP Setup options screen.

```
                              IPX Setup

        IPX Routing:                        On

        Ethernet Encapsulation...           802.3
        Ethernet Network Address:           00000000

        Ethernet Path Delay:                1
        Ethernet NetBios Forwarding:        No
        Ethernet Inbound SAP Filter Set... <<NONE>>


        Default Gateway Address:            00000000

        Filters and Filter Sets...

        IPX Wan Pool Base Address           00000000


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

1. To enable IPX routing, select IPX Routing, toggle it to Yes, and press Return.
2. To change Ethernet encapsulation from the commonly used 802.3 standard, select Ethernet Encapsulation and choose a different encapsulation method.
3. Select Ethernet Network Address and enter the network address of the IPX network connected to the Netopia Router's Ethernet port.

   Note: If the Ethernet network address is set to zero, the Router will attempt to learn the address from any configured IPX device on the Ethernet network or from the remote IPX network when a call is established.

4. To change the default path delay, select Ethernet Path Delay and enter a value (in ticks). This value is used to determine the port cost of using the Ethernet port in IPX RIP calculations.

5. To enable NetBIOS packet forwarding, select Ethernet NetBIOS Forwarding and toggle it to Yes. This parameter will determine whether "IPX Packet type 20" packets are forwarded on the Ethernet interface. These packets are used by NetBIOS and some other applications.

6. Select Ethernet Inbound SAP Filter Set to filter incoming IPX SAP advertisements on the Ethernet. By attaching an incoming SAP filter on the Ethernet, you can restrict the number of SAP entries learned on a large IPX network to only those required by remote users connecting to the Netopia Router. An Ethernet SAP filter *must* be used with networks that have so many servers advertised that the Netopia Router would otherwise exhaust its internal memory storing server entries.

   To attach a SAP filter set, first define the filter set using the Filters and Filter Sets option (see step 8 below). Then select the filter set from the Ethernet Incoming SAP Filter Set pop-up menu. To detach the filter set, select Detach Filter Set.

7. Select Default Gateway Address, and enter the network address of the IPX network to which all packets of unknown destination address should be routed.

   Note: The Default Gateway Address is usually set up to match the IPX Address in your network Connection Profile.

8. To configure filters and filter sets, select Filters and Filter Sets and go to the IPX filters and filter sets screens. For information on how to configure IPX filters and filter sets, see "IPX filters" on page 5-8.

9. Select IPX Wan Pool Base Address and enter the first IPX network address to be allocated to requesting IPX WAN clients. The base address you enter must not conflict with other IPX networks assigned to your IPX internet.

IPX in the answer profile

The answer profile can be configured to accept calls from remote IPX networks. To configure the answer profile to accept calls from remote IPX networks, go to the Default Answer Profile screen.

Note: The Default Answer Profile screen varies according to configuration.

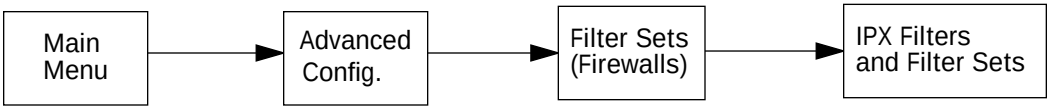
```
                    Default Answer Profile

Authentication...                 None

Force 56k on Answer:              No
Max. Receive Packet Size:         1500
Stac Data Compression...          None

Must Match a Defined Profile:     No

B Channel Usage...                1 B Channel
Idle Timeout:                     120

IP Enabled:                       Yes
IP Parameters...

IPX Enabled:                      Yes
IPX Parameters...

Configure values which may be used when receiving a call in this screen.
```

To enable IPX routing in the answer profile, select IPX Enabled and toggle it to Yes. When IPX Enabled is set to Yes, the item IPX Parameters appears below it.

To configure IPX routing in the answer profile, select IPX Parameters and go to the IPX Parameters (Default Answer Profile) screen. The items in this screen are similar to the IPX Profile Parameters items of the same name (see page 5-7).

```
                IPX Parameters (Default Answer Profile)

              NetBios Packet Forwarding:       Off

              Incoming Packet Filter Set...
              Outgoing Packet Filter Set...
              Incoming SAP Filter Set...
              Outgoing SAP Filter Set...

              Detach Filter Sets...

              Periodic RIP Timer:              60
              Periodic SAP Timer:              60

Configure IPX values to use when no matching Profile can be found.
```

IPX filters



IPX packet filters work very similarly to IP packet filters. They filter data traffic coming from or going to remote IPX networks. IPX filters can be set up to pass or discard IPX packets based on a number of user-defined criteria. Like IP filters, IPX filters must be grouped in sets that are applied to the answer profile or to connection profiles.

IPX SAP filters are used for filtering server entries not required to pass over the WAN links. When connecting to a large IPX network via ISDN, the transfer of large numbers of SAP entries can consume significant bandwidth on the WAN link.

Note: Using SAP filtering to prevent a server from being advertised does not provide security against that server being accessed—IPX packet filtering must be used for that purpose.

Setting up and using IPX filter sets is a four-step process:

1. Create the filters to use.
2. Create the filter sets to use.
3. Add filters to the filter sets.
4. Attach the filter sets to the answer profile or to connection profiles.

You can configure IPX filters and set up IPX filter sets from the IPX Filters and Filter Sets screen.

```
                        IPX Filters and Filter Sets

                    Show/Change IPX Packet Filters...
                    Add IPX Packet Filter...
                    Delete IPX Packet Filter...

                    Show/Change IPX Packet Filter Sets...
                    Add IPX Packet Filter Set...
                    Delete IPX Packet Filter Set...

                    Show/Change IPX Sap Filters...
                    Add IPX Sap Filter...
                    Delete IPX Sap Filter...

                    Show/Change IPX Sap Filter Sets...
                    Add IPX Sap Filter Set...
                    Delete IPX Sap Filter Set...

Define your filters 1st. IPX Filter Sets refer to, but don't contain, filters.
```

The items in the IPX Filters and Filter Sets screen are grouped into four areas:

- IPX packet filters
- IPX packet filter sets
- IPX SAP filters
- IPX SAP filter sets

The following sections explain the items in each of these areas.

IPX packet filters

For each IPX packet filter, you can configure a set of parameters to match on the source or destination attributes of IPX data packets coming from or going to the WAN.

Viewing and modifying packet filters

To display a view-only table of IPX packet filters, select Show / Change IPX Packet Filters in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, note the desired filter and press Return to go to the Change Packet Filter screen. The parameters in this screen are the same as the ones in the Add Packet Filter screen (see the next section).

Adding a packet filter

To add a new IPX packet filter, select Add IPX Packet Filter in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter screen.

```
                          Add Packet Filter

                Filter Name:               IPX Filter 1

                Source Network:            00000000
                Source Node Address:       000000000000
                Source Socket:             0000

                Destination Network:       00000000
                Destination Node Address:  000000000000
                Destination Socket:        0000

                     ADD FILTER NOW            CANCEL

Configure a new IPX Packet Filter. Finished?  ADD or CANCEL to exit.
```

By default, the filter's socket numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX data packet. You should configure the filter using criteria that meet your security needs.

1. Select Filter Name and enter a descriptive name for the filter.
2. To specify a source network for the filter to match on, select Source Network and enter an IPX network address.
3. To specify a source node for the filter to match on, select Source Node Address and enter an IPX node address.
4. To specify a source socket for the filter to match on, select Source Socket and enter an IPX source socket number.
5. To specify a destination network for the filter to match on, select Destination Network and enter an IPX network address.
6. To specify a destination node for the filter to match on, select Destination Node Address and enter an IPX node address.
7. To specify a destination socket for the filter to match on, select Destination Socket and enter an IPX destination socket number.
8. Select ADD FILTER NOW to save the current filter. Select CANCEL to exit the Add Packet Filter screen without saving the new filter.

Deleting a packet filter

To delete a packet filter, select Delete IPX Packet Filter in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX packet filter sets

Before the individual filters can be used, IPX packet filters must be grouped into sets. A filter can be part of more than one filter set.

Viewing and modifying packet filter sets

To display a table of IPX packet filter sets, select Show / Change IPX Packet Filter Sets in the IPX Filters and Filter Sets screen.

To modify any of the filter sets in the list, select the desired filter set and press Return to go to the Change Packet Filter Set screen. The parameters in this screen are the same as the ones in the Add Packet Filter Set screen (see the next section).

Adding a packet filter set

To add a new IPX packet filter set, select Add IPX Packet Filter Set in the IPX Filters and Filter Sets screen and press Return to go to the Add Packet Filter Set screen.

```
                        Add Packet Filter Set

               Filter Set Name:

               Show Filters/Change Action on Match...

               Append Filter...

               Detach Filter...

                    ADD FILTER SET NOW        CANCEL

Modify an IPX Packet Filter here. Changes are immediate.
```

Follow these steps to configure the new packet filter set:

1. Select Filter Set Name and enter a descriptive name for the filter set.
2. To change the forwarding action of filters in the filter set, select Show Filters / Change Action on Match and press Return to go to the Show Filters / Change Actions on Match screen.

```
                        Show Filters/Change Actions on Match

                    Filter Name--------------------Forward

                    Filter 1                       No

                    Filter 2                       No

                    <<NO MATCH>>                   Yes
Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the packet forwarding action to Yes (pass) or No (discard).

3. To add a filter to the filter set, select Append Filter to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward packets that match their criteria.

   To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select Detach Filter to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

5. Select ADD FILTER SET NOW to save the current filter set. Select CANCEL to exit the Add Packet Filter Set screen without saving the new filter set.

Deleting a packet filter set

To delete a packet filter set, select Delete IPX Packet Filter Set in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

IPX SAP filters

For each IPX SAP filter, you can configure a set of parameters to match on certain attributes of IPX SAP packet entries. The filters check IPX SAP packets for entries that match and then act on those entries. The SAP packets themselves are always allowed to continue after their entries are checked.

The purpose of filtering SAP packets is not to make your network more secure, but to add efficiency to network bandwidth use. Filtering SAP packets may reduce the size of SAP packets and SAP bindery tables by removing unwanted entries.

Viewing and modifying SAP filters

To display a table of IPX SAP filters, select Show/Change IPX SAP Filters in the IPX Filters and Filter Sets screen.

To modify any of the filters in the table, select the desired filter and press Return to go to the Change SAP Filter screen. The parameters in this screen are the same as the ones in the Add SAP Filter screen (see the next section).

Adding a SAP filter

To add a new IPX SAP filter, select Add IPX SAP Filter in the IPX Filters and Filter Sets screen and press Return to go to the Add SAP Filter screen.

```
                          Add SAP Filter

                Filter Name:

                Server Name:

                Socket:                    0000

                Type:                      0000

                IPX Network:               00000000
                IPX Node Address:          000000000000

                     ADD FILTER NOW            CANCEL

Configure a new IPX SAP Filter. Finished?  ADD or CANCEL to exit.
```

By default, the filter's socket and type numbers and network and node addresses are null (all zeros). This sets the filter to match on any IPX SAP packet entry. You should configure the filter using criteria that meet your needs.

Follow these steps to configure the new SAP filter:

1. Select Filter Name and enter a descriptive name for the filter.
2. To specify a server name for the filter to match on, select Server Name and enter the name of an IPX server. You can use the wildcard characters * (asterisk) and ? (question mark). Use * to match any string, including a null string (no characters), and ? to match any single character in the server's name. For example, the filter could match on the server name "FARALLON" with "FARA*", "FARAL?ON", and "FARALLON*".
3. To specify a socket for the filter to match on, select Socket and enter an IPX socket number.
4. To specify a type number for the filter to match on, select Type and enter an IPX type number.
5. To specify an IPX network address for the filter to match on, select IPX Network and enter an IPX network address.

6. To specify an IPX node address for the filter to match on, select IPX Node Address and enter an IPX node address.
7. Select ADD FILTER NOW to save the current filter. Select CANCEL to exit the Add SAP Filter screen without saving the new filter.

Deleting a SAP filter

To delete a SAP filter, select Delete IPX SAP filter in the IPX Filters and Filter Sets screen to display a table of filters. Select a filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

IPX SAP filter sets

Before IPX SAP filters can be used, they must be grouped into sets. A SAP filter can be part of more than one filter set.

Viewing and modifying SAP filter sets

To display a table of IPX SAP filter sets, select Show/Change IPX SAP Filter Sets in the IPX Filters and Filter Sets screen to display a list of filter sets.

To modify any of the filter sets in the list, select the desired filter set and go to the Change SAP Filter Set screen. The parameters in this screen are the same as the ones in the Add SAP Filter Set screen (see the previous section).

Adding a SAP filter set

To add a new IPX SAP filter set, select Add IPX SAP Filter Set in the IPX Filters and Filter Sets screen and go to the Add SAP Filter Set screen.

```
                        Add SAP Filter Set

                Filter Set Name:

                Show Filters/Change Action on Match...

                Append Filter...

                Detach Filter...

                     ADD FILTER SET NOW        CANCEL

Modify an IPX SAP filter here. Changes are immediate.
```

Follow these steps to configure the new SAP filter set:

1. Select Filter Set Name and enter a descriptive name for the filter set.
2. To change the forwarding action of filters in the filter set, select Show Filters/Change Action on Match and press Return to go to the Show Filters/Change Actions on Match screen.

```
                        Show Filters/Change Actions on Match

                    Filter Name--------------------Forward

                    Filter 1                       No

                    Filter 2                       No

                    <<NO MATCH>>                   Yes

Set whether filters forward or drop matching packets here.
```

Select a filter and toggle the entry forwarding action to Yes (pass) or No (discard).

3. To add a filter to the filter set, select Append Filter to display a table of filters. Select a filter from the table and press Return to add it to the filter set. The default action of newly added filters is to *not* forward (discard) packet entries that match their criteria.

   To exit the table without adding the filter, press the Escape key.

4. To remove a filter from the filter set, select Detach Filter to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press the Escape key.

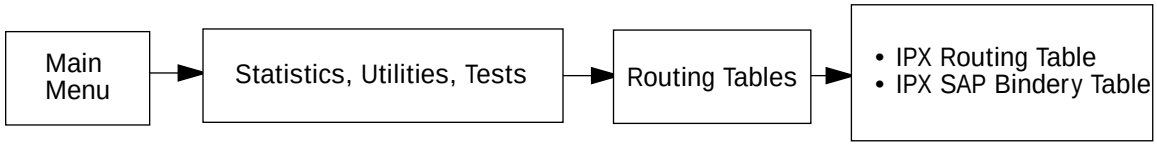
5. Select ADD FILTER SET NOW to save the current filter set. Select CANCEL to exit the Add SAP Filter Set screen without saving the new filter set.

Deleting a SAP filter set

To delete a SAP filter set, select Delete IPX SAP Filter Set in the IPX Filters and Filter Sets screen to display a list of filter sets. Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

Note: Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

IPX routing tables



IPX routing tables provide information on current IPX routes and services.

To go to the IPX Routing Table screen, select IPX Routing Table in the Routing Tables screen. This table shows detailed information about current IPX network routes.

```
                              IPX Routing Table

 Net Addr-Hops-Ticks-Type--Status-Interface-------------via Router------------
 ----------------------------------SCROLL UP-----------------------------------
00000020   2      3 RIP   Active Ethernet              00000120:00000c465c2f
00000030   2     12 RIP   Active Ethernet              00000120:00000c465c2f
00000033   4     14 RIP   Active Ethernet              000000120:00000c465c2f
00000100   2      7 RIP   Active Ethernet              00000120:00000c465c2f
00000110   1      1 RIP   Active Ethernet              00000120:00000c465c2f



--------------------------------SCROLL DOWN----------------------------
```

To go to the IPX SAP Bindery Table screen, select IPX SAP Bindery Table in the Routing Tables screen. This table shows detailed information about available IPX services and their location.

Chapter 6

AppleTalk Setup

This chapter discusses the concept of AppleTalk routing and how to configure AppleTalk Setup for a Netopia Router with AppleTalk capability. AppleTalk is available on the Netopia Router's 400 series which includes both the Small Office and Corporate models. This chapter will discuss both versions. Skip this chapter if this information does not apply to your particular Netopia model.

AppleTalk networks

A network is a communication system that connects computers together to share information using network services, such as electronic mail, print spoolers, and file servers. Information is transferred over a cabling system or WAN using a common set of protocols. You can think of the cabling system as an organization of cities, streets, and buildings and the protocols as the method of sending letters or packages, as illustrated on the following pages. A cable is the physical medium (for example, twisted pair or coaxial) over which information travels from one device to another.

AppleTalk is a protocol set for local area networks developed by Apple Computer. While initially applied to the LocalTalk cabling system for connecting Macintosh computers and LaserWriters, it has been expanded to use other cabling systems, such as Ethernet, as well as the dial-up telephone networks and packet switching systems. LocalTalk was originally known as the AppleTalk Personal Network system.

Each computer or peripheral device (printer, client, file server) connected to a network is called a node and has a unique node address, which can be any number from 1 to 254. Whenever you open the Chooser or any application that communicates with other computers on your network, your application compiles a list of all node names and addresses. All you see are the names --- for example, "Paul's Mac," "TechSportsWriter," or "2nd Floor AppleShare" --- but your application also knows the node addresses of all these devices.

When you send information, commands, or requests to a printer, server, or another workstation, your application formats the information into units known as packets. It then attaches the correct address to the packets and sends them to the AppleTalk software on your computer, which forwards the packets across the network. Packets also include a return address, so the receiver will know where to reply.

If the cabling of your network were a street system, then a node address would correspond to a building's street address. Node addresses are not permanent. Each AppleTalk device determines its node address at startup. Although a Macintosh that is starting up will try to use its previous address, the address will often be different every time you restart. This dynamic node addressing scheme prevents conflicts when devices are moved between networks and simplifies the administrative tasks of a network. If you have only one network, the node address alone is all the information AppleTalk needs to send a packet from one computer to another.

However, networks can be connected together through routers, such as the Netopia Router, into an internetwork (often shortened to internet). Because devices on different networks can have duplicate node numbers, AppleTalk tells them apart according to an additional part of their addresses: the network number.

The Router assigns a unique network number to each member network. In terms of the city street metaphor, the network number is similar to the name of the city. Putting a network number together with a node number fully specifies the address of a node on an internet.

To make the services on an internet manageable, groups of devices on a network can be grouped into zones. When this is done, selecting a network service (server, etc.) includes choosing a zone from which the service can be selected. Like network numbers, zone names are assigned by routers.

A routing table is maintained by each AppleTalk router. The table serves as a map of the internet, specifying the path and distance, in hops, between its router and other networks. The routing table is used to determine whether a router will forward a data packet and, if so, to which network.

You can use the information in the AppleTalk routing table to observe and diagnose the Netopia Router's current connections to other AppleTalk routers. To go to the AT Routing Table screen from the Netopia Router's console, select Statistics, Utilities, Tests from the Main Menu and then select Routing Tables and AppleTalk Routing Table.

```
                                AT Routing Table
-Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
 ----------------------------------SCROLL UP-------------------------
  1     --     Admin                  2    Good  46.131          0
  2     --     Admin                  2    Good  46.131          0
  3     --     Operations             2    Good  46.131          0
  4     --     Sales                  2    Good  46.131          0
  5     --     Marketing              2    Good  46.131          0
  6     --     Marketing              2    Good  46.131          1
  7     --     Customer Service       2    Good  46.131          1
  8     --     TechSports             2    Good  46.131          0
  10    --     R&D                    2    Good  46.131          0
  11    --     R&D                    2    Good  46.131          0
  12    --     R&D                    2    Good  46.131          0
  16    --     UNIX Services          2    Good  46.131          0
 *24    27     Operations             1    Good  46.131          79
  28    31     R&D                    1    Good  46.131          15
 ---------------------------------SCROLL DOWN------------------------
UPDATE'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

A router has multiple communications ports and is capable of forwarding information to other routers and devices on the internet. The router performs packet forwarding, network and device address maintenance, and other administrative functions required by the AppleTalk protocols. The distinction between routers and bridges is an important one:

- A true bridge, like a router, is used to join two cable segments and filter traffic between them. The result is still one expanded network rather than an internet. Bridges do not assign network numbers or zone names, nor do they maintain network maps.
- A router maintains the separate identities of the networks it connects; the result is an internet.

MacIP

When Macintosh computers encapsulate TCP/IP packets in AppleTalk, either because they are on LocalTalk or because, for administrative reasons, they must use the services of a MacIP gateway. This gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. Setting up MacIP involves enabling the feature and optionally setting up a range of addresses to be static.

See Chapter 4, "IP Setup." for more information on how to set up MacIP and other IP addressing schemes.

AURP

AppleTalk Update-Based Routing Protocol (AURP) allows AppleTalk networks to communicate across an IP network. Your local AppleTalk networks (connected to the Netopia Router) can exchange data with remote AppleTalk networks that are also connected to an AURP-capable router.

When two networks using AppleTalk communicate with each other through a network based on the Internet Protocol, they are said to be tunneling through the IP network. The Netopia Router uses AURP to allow your AppleTalk network to tunnel to designated AppleTalk partner networks, as well as to accept connections from remote AppleTalk networks tunneling to your AppleTalk LAN.

Routers and seeding

To configure AppleTalk networks, you must understand the concept of seeding. Seeding is the process by which routers (or more specifically, router ports) agree on what routing information is valid. AppleTalk routers that have been reset, for example, must decide what zones and network numbers are valid before they begin routing. In this case, a router may use the information it has stored, or use information it receives from another router, depending on how it has been configured.

To help ensure agreement between routers on a network, a seed router is configured with the correct information, and other routers obtain their information from that router when they are turned on or reset.

Routers commonly use one of three types of seeding procedures: hard seeding, soft seeding, and non-seeding.

Hard seeding: When a router that uses hard seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, and their information matches the router's own configuration information, the result is the same—the router uses the values in its own configuration. However, if other routers provide network numbers or zone names that conflict with those in the router's configuration, the router disables any of its own ports for which there are conflicts.

Soft seeding: When a router that uses soft seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, the router uses the information they provide, regardless of whether or not there are conflicts between the information received and its configured information. Once the soft seeding router begins to route, it can serve as a seed router, providing network number and zone name information to other routers upon request. The default state of the Netopia Router's AppleTalk ports is soft seeding.

Non-seeding: When a router that uses non-seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. For any network where no other routers reply, the non-seeding router will not have any active ports until the next reset.

You should set the Netopia Router's seeding action to work best in your particular network environment. These scenarios may guide you in deciding how to set the router's seeding:

- If the Netopia Router is the only router on your network, you must set it to either hard seeding or soft seeding. The default is soft seeding.
- If there is another active router on your network, and you want that router to configure the Netopia Router's EtherTalk or LocalTalk parameters, you can set the Netopia Router to non-seeding.
- If there is another active router on your network, you could set the Netopia Router to be soft seeding if you are unsure that the second router would always be available to configure the Netopia Router's EtherTalk or LocalTalk parameters.
- If you want the Netopia Router to configure the EtherTalk or LocalTalk parameters of other routers on your network, you must set it to hard seeding. In this case, the other routers must be soft seeding or non-seeding, and the Netopia Router must already be active when those other routers are rebooted.

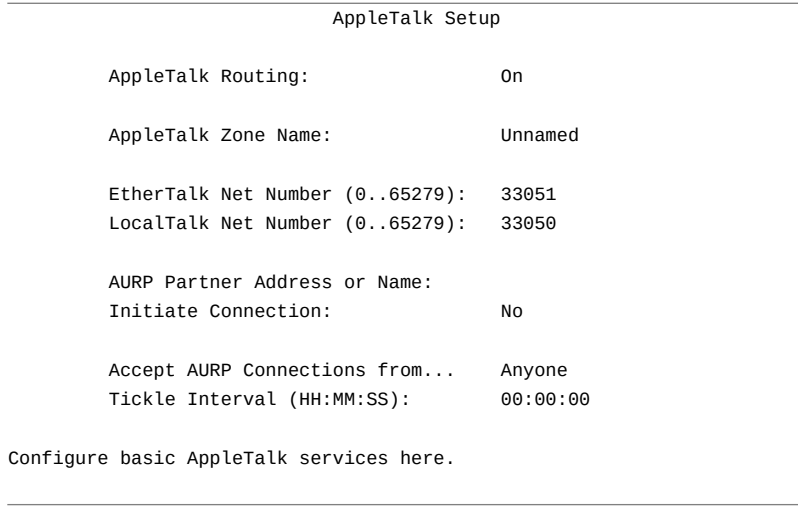
- If you want the Netopia Router and all other routers on your network to use only their own configurations, set the Netopia Router and all other routers to hard seeding. In this case, any router (including the Netopia Router) that is rebooted will not begin routing if it detects a routing conflict between itself and any other router. This last scenario could be useful for detecting and locating routing errors on your network.

For information on how to configure AppleTalk setup for Small Office models, see below. For information on how to configure AppleTalk setup for Corporate models, see “AppleTalk Setup for Corporate models” on page 6-9.

AppleTalk Setup for Small Office models

AppleTalk setup for Small Office Netopia Routers consists of configuring the options in the AppleTalk Setup screen.

To go to the AppleTalk Setup screen, select AppleTalk Setup in the Network Protocols Setup screen and press Return.



1. Select AppleTalk Routing and toggle to On.
2. Select AppleTalk Zone Name and enter a name of your choice (this will apply to both the EtherTalk and LocalTalk networks) to distinguish your network from the other facilities. The two different networks will appear in the same zone.
3. Observe EtherTalk Net Number. This value is the EtherTalk network number. You may type in a new network number, or leave the value as it originally appears.
4. Observe LocalTalk Net Number. This value is the LocalTalk network number. You may type in a new net number, or leave the value as it originally appears.
5. Select AURP Partner Address or Name and enter the AURP partner's IP address or domain name. If you do not know the remote network's IP address, enter its domain name. Domain names are the Internet addresses favored by people (for example: twain.gov, chagall.arts.edu, etc.). Domain names are matched to the IP addresses actually used by the router (for example: 163.7.8.202).
6. Once you enter the IP address or domain name of the remote AppleTalk network that you would like to connect to, an additional field appears. To initiate a connection with an AURP partner, select Initiate Connection and toggle it to Yes.

   Note: Small Office users can only create one AURP partner.
7. Select Accept AURP Connections and press Return. You have two choices for accepting AURP connections. A pop-up menu appears with the options Configured Partners Only or Anyone. Choosing Configured Partners Only will tell the Router to only accept a connection from the pre-defined partner. Choosing Anyone will allow any AURP machine to connect.
8. Select Tickle Interval (HH:MM:SS) and set the timer to indicate how often a tickle or 'are you still there' packet will be sent to the remote AppleTalk network.

   This parameter can be set between 0 and 100 hours. If this value is set to 0, the Netopia Router will never send out a tickle packet.

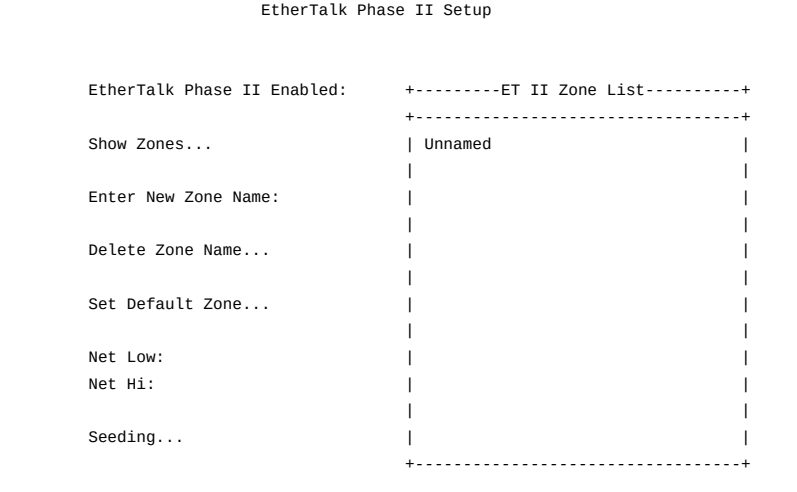
You have finished configuring AppleTalk Setup for the Small Office model.

AppleTalk Setup for Corporate models

AppleTalk setup for Corporate Netopia Routers consists of configuring EtherTalk, LocalTalk, and AURP.

EtherTalk Setup

To go to the EtherTalk Setup options screen, select Network Protocols Setup and then select AppleTalk Setup in the Advanced Configuration screen. Select EtherTalk Phase II Setup and press Return.



- If you are using EtherTalk Phase II on the Ethernet network connected to Netopia Router, select EtherTalk Phase II Enabled and toggle it to On.

- To view the zones available to EtherTalk Phase II, select Show Zones and press Return. You can dismiss the list of zones by pressing the Return or Escape key.
- Select Enter New Zone Name to enter a new zone name.

  Note: Your EtherTalk network number and zone name must match the values in use on the EtherTalk network.

  If another router is already present on the EtherTalk network that you will be connecting to the Netopia Router, use the zone name and network number used by that router for that EtherTalk network. Otherwise, your EtherTalk network may experience routing conflicts.

  As an alternative, you can set EtherTalk seeding to soft seeding and let the Netopia Router receive the zone name and network number from the other router.
- To remove zones from the list, select Delete Zone Name and press Return to see the zones list. Use the Up and Down Arrow keys to select the zone to delete. Press the Return key to delete it and exit the list. Press the Escape key to exit the list without deleting any zones.
- Select Set Default Zone to choose a different default zone. This is the zone where Netopia's EtherTalk Phase II port is visible to other AppleTalk nodes. The default zone is also where new AppleTalk nodes will appear. If you do not set a default zone, the first zone you create will be the default zone.
- You can also set the range of EtherTalk Phase II network numbers. Select Net Low and enter the lower limit of the network number range. Select Net High and enter the upper limit of the range.
- Select the Seeding pop-up menu and choose the seeding method for Netopia to use (see "Routers and seeding" on page 6-5).

You have finished configuring EtherTalk Phase II.

LocalTalk Setup

The Netopia Router can function as a LocalTalk-to-EtherTalk router. This means that a LocalTalk network can be connected to the Netopia Router's PhoneNET port.

Select LocalTalk Setup in the AppleTalk Setup screen and press Return to the LocalTalk Routing Setup screen.

```
                LocalTalk Routing Setup

        LocalTalk Enabled:        On

        LocalTalk Zone Name:      Unnamed

        LocalTalk Net Number:     0

        Seeding...:               Soft-Seeding

Use this screen to set up the LocalTalk Port Routing attributes.
```

- If you are using LocalTalk with the Netopia Router, select LocalTalk Enabled and make sure LocalTalk is set to On, which is the default.
- Select LocalTalk Zone Name and enter a new or existing zone name.

  Note: Your LocalTalk network may already have a zone and network number in place. For Netopia's LocalTalk port to be part of your LocalTalk network, it must have a network number and zone name that matches the values in use on the LocalTalk network.

  If another router is already present on the LocalTalk network that you will be connecting to the Netopia Router, use the zone name and network number used by that router for that LocalTalk network. Otherwise, your LocalTalk network may experience routing conflicts.

As an alternative, you can set LocalTalk seeding to soft seeding and let the Netopia Router receive the zone name and network number from the other router.

- Select LocalTalk Network Number and enter the desired network number.
- Select Seeding. From the pop-up menu, choose the type of seeding for the Netopia Router's LocalTalk port to use (see "Routers and seeding" on page 6-5).

You have finished configuring LocalTalk Setup.

AURP setup

To set up AURP, select AppleTalk Setup from the Network Protocols screen. Select AURP Setup and press Return.

```
                              AURP Setup

         AURP Enable:                            On

         Display/Change Partner...

         Add Partner...

         Delete Partner...


         Enter Free Trade Zone Name:

         Accept Connections From...              Anyone
         Restrict Guests to Free Trade Zone:     No

         Advanced Options...

AURP Allows you to connect remote AppleTalk Networks across IP.
```

- To activate AURP and enable connections to and from AURP partners, select AURP Enable and toggle it to On.

Viewing AURP partners

- To see a table of existing AURP partners, select Display/Show Partners and press Return.

  Note: The Netopia Router can define a total of 32 AURP partners.

Adding an AURP partner

- To add a new AURP partner, select Add Partner and press Return to go to the Add AURP Partner screen.

```
                        Add AURP Partner


        Partner IP Address or Domain Name:


        Initiate Connection:              No

        Restrict to Free Trade Zone:      No


        ADD PARTNER NOW                   CANCEL

Enter Information about new Partner.
```

- Select Partner IP Address or Domain Name and enter the new AURP partner's IP address. If you do not know the remote network's IP address, enter its domain name. Domain names are the Internet addresses favored by people (for example, chagall.arts.edu). Domain names are matched to the IP addresses actually used by IP routers (for example, 163.7.8.202).

- To initiate a connection with an AURP partner, select Initiate Connection and toggle it to Yes. This will open a connection to the remote AppleTalk network.
- To restrict the new AURP partner's access to your intranet, select Restrict to Free Trade Zone and toggle it to Yes. See "Restricting intranet access," below.
- To add the new AURP partner, select ADD PARTNER NOW. To discard the new AURP partner, select CANCEL.

Modifying an AURP partner

- To modify an AURP partner, select Display/Change Partner in the AURP Setup screen and press Return to display a table of existing partners.

  Use the Up and Down Arrow keys to select a partner, then press Return to go to the Change AURP Partner screen.

Deleting an AURP partner

- To delete an AURP partner, select Delete Partner in the AURP Setup screen and press Return to display a table of existing partners.

  Use the Up and Down Arrow keys to select an AURP partner, then press Return to delete it. Press the Escape key to exit without deleting a partner.

Restricting intranet access

- To restrict access to your Intranet by your AURP partners, establish a free trade zone. By creating this zone for AURP partners to access, you can confine all AURP traffic to and from the AppleTalk nodes residing within the free trade zone.

  Select Enter Free Trade Zone Name and enter the name of a zone to handle all AURP traffic. This zone may be one that does not yet exist.
- To restrict AURP access to and from the free trade zone, select Restrict Guests to Free Trade Zone and toggle it to Yes.

Receiving AURP connections

- To control the acceptance of incoming AURP tunnels, select Accept Connections From and choose Anyone or Configured Partners Only from the pop-up menu. If you choose Anyone, all incoming AURP connections will be accepted.

  The more secure option is Configured Partners Only, which only accepts connections from recognized AURP partners (the ones you have set up).

Configuring AURP Options

In the AURP Setup screen, select Advanced Options and go to the AURP Options screen. Using AURP can cause a problem when two networks, one local and one remote, have the same network number. This may cause network routing ambiguities than can result in routing errors.

```
                    AURP Options

Tickle Interval (HH:MM:SS):             00:00:00
Update Interval (HH:MM:SS):             00:00:30


Enable Network Number Remapping:        Yes

Remap into Range
            From:                       4096
            To:                         32768

Cluster Remote Networks:                No

Enable Hop-Count Reduction:             No
```

- Select Tickle Interval (HH:MM:SS) and set the timer to indicate how often a tickle or ‘are you still there’ packet will be sent to the remote AppleTalk Network.

The AURP tickle timer is a parameter that you can set anywhere between 0 and 100 hours. This parameter tells the AURP partners when to send out an AURP tickle packet. If this value is set to 0, the Netopia Router will never send out a tickle packet.

- Select Update Interval (HH:MM:SS) and set the timer to indicate how often a Routing Information Update (RI-Upd) packet will be sent to the remote router.

  The update timer is a parameter that you can set between 10 and 327270 seconds in 10-second increments. Values less than 10 will be rounded to 10. Values greater than 327270 will be rounded to 327270. Values in between 10 and 327270 will be rounded to the nearest multiple of 10.

- To enable network number remapping, select Enable Network Number Remapping and toggle it to Yes.

  You should enable network number remapping if you plan on using AURP. With remapping, Netopia will substitute network numbers not used by your network for the numbers of other remote networks. These safe numbers will only be used by local routers on your network; remote routers will not be aware of the remapping.

  When network number remapping is enabled, you *must* choose a safe range of network numbers as a destination for the remapping. A safe range of network numbers does not intersect your local AppleTalk network's range of network numbers.

- To choose a destination range for the remapping, select From under Remap into Range and enter a starting value. Then select To and enter an ending value. Make sure the range you choose is large enough to accommodate all expected incoming AURP network numbers.

- To improve the efficiency of remapping network numbers into a safe range, select Cluster Remote Networks and toggle it to Yes. This setting takes any number of remote networks being remapped and causes them to be remapped into a continuous range.

- To override the AppleTalk maximum limit of 15 hops, select Enable Hop-Count Reduction and toggle it to Yes. Hosts on a local AppleTalk network will then "see" AppleTalk destinations across the IP tunnel as being only one hop away.

  AppleTalk allows a packet up to 15 hops (going through 15 AppleTalk routers) to reach its destination. Packets that must reach destinations more than 15 hops away will not succeed, and tunneling from one large AppleTalk network to another could exceed that limit. In that case, hop count reduction would make that kind of packet transmission possible.

You have finished configuring AURP Setup.

Chapter 7

Security

The Netopia Router provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This chapter is divided into five main sections:

- "Suggested security measures" on page 7-2, lists actions for blocking potential security holes.
- "User accounts," beginning on page 7-2, shows you how to set up name/password combinations to protect the Netopia Router's configuration screens.
- "Telnet access" on page 7-5, shows you how to control access to the Netopia Router by those using the Telnet protocol.
- "About filters and filter sets," beginning on page 7-6, and "Working with IP filters and filter sets," beginning on page 7-16, have information on what filters are, how they work, how to customize them, and how to use them in sets. For information on IPX filters and filter sets, see "IPX filters," beginning on page 5-8.

Suggested security measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Netopia Router and your network more secure:

- If you will be using a PC Card modem for dial-up access through a telephone line, keep the phone number secure and be sure to set passwords to protect the configuration screens.
- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile, if you are using a switched line and CallerID.
- Where possible, insist on using PAP, CHAP, or secure authentication token card to authenticate connections to and from connection profiles.
- When using AURP, accept connections only from configured partners.
- Configure the Netopia Router through the serial or PC card console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia Router, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution! You are strongly encouraged to add protection to the configuration screens. Unprotected screens could allow an unauthorized user to compromise the operation of your entire network.

The following screens can be protected with a name/password combination:

- Main Menu
- Easy Setup
- Advanced Configuration
- Security Options (password only)
- Statistics, Utilities, Tests

Once user accounts are created, users who attempt to access protected screens will be challenged. Users who enter an incorrect name or password are returned to the Main Menu or to a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, select Security in the Main Menu and go to the Security Options screen.

```
                          Security Options

         Show Users...

         Add User...

         Delete User...

         Password for This Screen (11 chars max):
         Require Name and Password to Log On:              No

         Deny Telnet Access to SNMP Screens:               No
         Block Telnet Console Access:                      No

         Web Server Disabled (config):                     No

Set up configuration access options here.
```

Protecting the Security Options screen

The first screen you should protect is the Security Options screen, because it controls access to the configuration screens. Access to the Security Options screen can be protected with a password.

Select Password To Visit This Screen in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

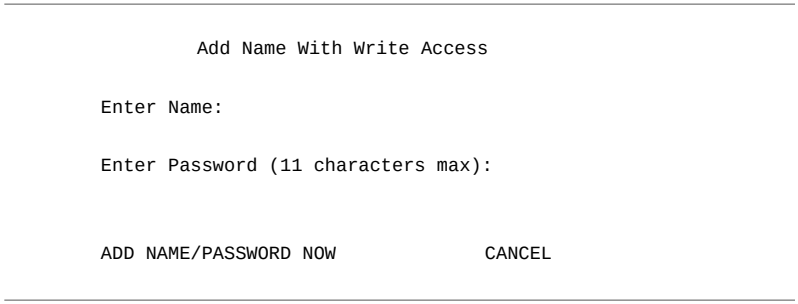
Protecting the configuration screens

You can protect the configuration screens with user accounts. You can administer the accounts from the Security Options screen.

A single user account allows access to the Easy Setup, Advanced Configuration, and Statistics, Utilities, Tests screens. You can create up to four accounts.

To display a view-only list of user accounts, select Show Users in the Security Options screen.

To add a new user account, select Add User in the Security Options screen and press Return to go to the Add Name With Write Access screen.



Follow these steps to configure the new account:

1. Select Enter Name and enter a descriptive name (for example, the user's first name).
2. Select Enter Password and enter a password.

3. To accept the new name/password combination, select ADD NAME/PASSWORD NOW. To exit the Add Name With Write Access screen without saving the new account, select CANCEL.

   Note: The Web server uses only the first configured Name/Password pair for configuration access.

To delete a user account, select Delete User to display a list of accounts. Select an account from the list and press Return to delete it. To exit the list without deleting the selected account, press the Escape key.

Protecting the Main Menu

The name/password combinations you created to protect the individual configuration screens can be extended to the Main Menu.

Select Require Name and Password to Log On in the Security Options screen and toggle it to Yes.

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia Router supports Telnet access to its configuration screens.

Caution! You should consider restricting Telnet access to the Netopia Router if you suspect there is a chance of tampering.

To restrict Telnet access, select Security in the Main Menu and go to the Security Options screen. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select Deny Telnet Access to SNMP Screens and toggle it to Yes. (See "SNMP traps" on page 9-20.)

To restrict Telnet access to all of the configuration screens, select Block Telnet Console Access and toggle it to Yes.

About filters and filter sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia Router's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can either be an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

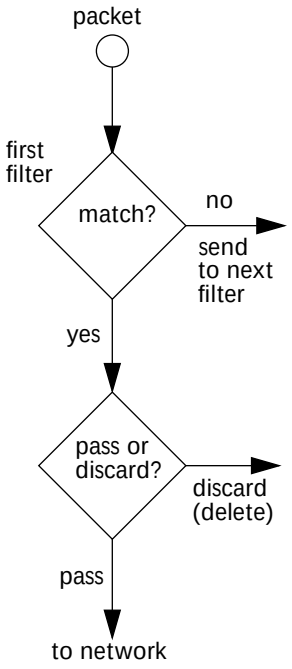
Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.

A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.

If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.



For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, and so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can pass or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither pass nor discard the packet (because it cannot match any criteria), the second filter has a chance to pass or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

Using filter sets

You use filter sets by linking them to particular connection profiles and the answer profile. When you create a connection profile or edit the answer profile, you can specify a filter set for that profile to use.

To learn how to link a filter set to a connection profile, see "Adding a Connection Profile" on page 2-16 or "Changing a Connection Profile" on page 2-15.

To learn how to link a filter set to the answer profile, see "How the default profile works for a permanent circuit" on page 2-45, or "How the default profile works for a permanent circuit" on page 2-45.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

A filter's actions

- Passes the packet to the local or remote network
- Blocks (discards) the packet
- Ignores the packet

A filter passes or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

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 Router:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd
+-------------------------------------------------------------------+
  1 199.211.211.17   0.0.0.0          TCP            23      Yes No
```

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The tables below show a few common services and their associated port numbers..

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to pass (forward) packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

```
+-#---Source IP Addr---Dest IP Addr----Proto-Src.Port-D.Port--On?-Fwd-+
| 1   192.211.211.17   0.0.0.0          TCP     0        23     Yes No  |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
+-----------------------------------------------------------------------+
```

The table's columns correspond to each filter's attributes:

#: The filter's priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if using those protocols.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays Yes when the filter is in effect or No when it is not.

Fwd: Shows whether the filter forwards (Yes) a packet or discards (No) it when there's a match.

Filtering example #1

Returning to our filtering rule example from above (see page 7-9), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:

   Block all Telnet attempts that originate from the remote host 199.211.211.17.

2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.

   - Source IP Addr = 199.211.211.17
   - Source IP address mask = 255.255.255.255
   - Dest IP Addr = 0.0.0.0
   - Destination IP address mask = 0.0.0.0

   Note: To learn about IP addresses and masks, see Appendix B, "Understanding IP Addressing."

3. Using the tables on page 7-10, find the destination port and protocol numbers (the *local* Telnet port):
   - Proto = TCP (or 6)
   - D. Port = 23
4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:
   - On? = Yes
   - Fwd = No

This four-step process is how we produced the following filter from the original rule:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd
+-------------------------------------------------------------------+
  1 199.211.211.17   0.0.0.0          TCP            23      Yes No
```

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:

```
+-#--Source IP Addr--Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd
+-------------------------------------------------------------------+
  1 200.233.14.0     0.0.0.0          0                     Yes No
```

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought should go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
  - passed if all the filters are configured to discard (*not* forward).
  - discarded if all the filters are configured to pass (forward).
  - discarded if the set contains a combination of pass and discard filters.

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.

- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the “must match” option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

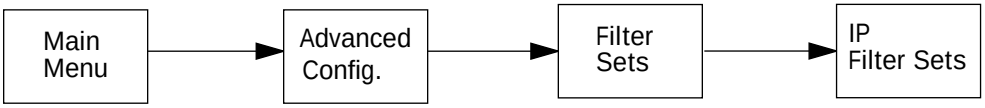
Each filter set you design will be based on one of the following approaches:

- That which is not expressly prohibited is permitted.
- That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

Working with IP filters and filter sets

This section covers IP filters and filter sets. For working with IPX filters and filter sets, see “IPX filters,” beginning on page 5-8.



To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section “About filters and filter sets,” beginning on page 7-6.

```
                                IP Filter Sets


                             Display/Change IP Filter Set...

                             Add IP Filter Set...

                             Delete IP Filter Set...


Return/Enter to configure and add a new Filter Set.
Set Up IP Filter Sets (Firewalls) from this and the following Menus.
```

The basic procedure for creating and maintaining filter sets is as follows:

1. Add a new filter set.
2. Create the filters for the new filter set.
3. View, change, or delete individual filters and filter sets.

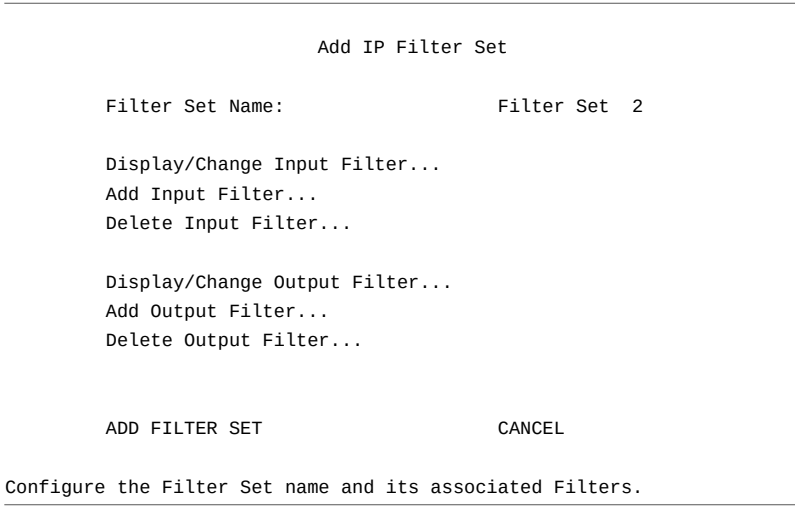
The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 16 output filters and up to 16 input filters.

To add a new filter set, select Add IP Filter Set in the IP Filter Sets screen and press Return to go to the Add Filter Set screen.

Note: There are two groups of items in the Add Filter Set screen, one for input filters and one for output filters. The two groups work in essentially the same way, as you'll see below.



Naming a new filter set

All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

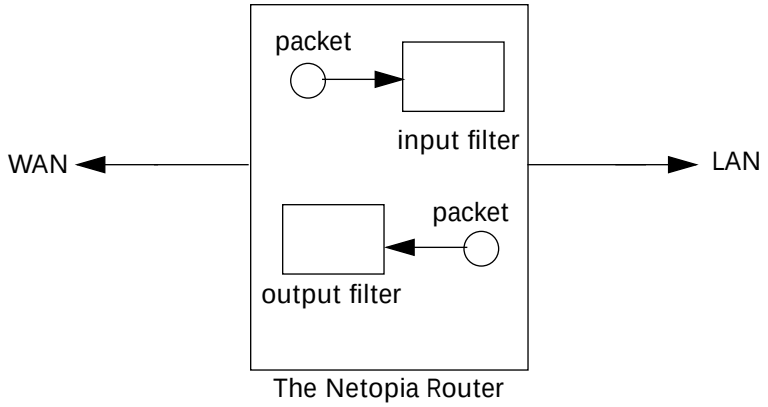
To give a new filter set a different name, select Filter Set Name and enter a new name for the filter set.

To save the filter set, select ADD FILTER SET. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see “Modifying filter sets” on page 7-24). Or you can add filters to your new set before saving it (see “Adding filters to a filter set” on page 7-20).

Select CANCEL to leave the Add Filter Set screen without saving the new filter set and return to the Filter Sets screen.

Input and output filters—source and destination

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet.



Packets in the Netopia Router pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to source and destination. From the perspective of an input filter, your local network is the destination of the packets it checks, and the remote network is their source. From the perspective of an output filter, your local network is the source of the packets, and the remote network is their destination.

Type of filter	"source" means	"destination" means
Input filter	the remote network	the local network
Output filter	the local network	the remote network

Adding filters to a filter set

In this section you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

To add an input filter, select Add Input Filter in the Add IP Filter Set screen and go to the Add Filter screen. (Select Add Output Filter to add an output filter.)

```
                        Add Filter

                Enabled:                    No
                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:              0

                Source Port Compare...      No Compare
                Source Port ID:             0
                Dest. Port Compare...       No Compare
                Dest. Port ID:              0

       ADD THIS FILTER NOW              CANCEL


Enter the IP specific information for this filter.
```

1. To make the filter active in the filter set, select Enabled and toggle it to Yes. If Enabled is toggled to No, the filter can still exist in the filter set, but it will have no effect.
2. If you want the filter to forward packets that match its criteria to the destination IP address, select Forward and toggle it to Yes. If Forward is toggled to No, packets matching the filter's criteria will be discarded.

3. Select Source IP Address and enter the source IP address this filter will match on. You can enter a subnet or a host address.
4. Select Source IP Address Mask and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
5. Select Dest. IP Address and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
6. Select Dest. IP Address Mask and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
7. Select Protocol Type and enter ICMP, TCP, UDP, Any, or the number of another IP transport protocol (see the table on page 7-12).

   Note: If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.
8. Select Source Port Compare and choose a comparison method for the filter to use on a packet's source port number. Then select Source Port ID and enter the actual source port number to match on (see the table on page 7-10).
9. Select Dest. Port Compare and choose a comparison method for the filter to use on a packet's destination port number. Then select Dest. Port ID and enter the actual destination port number to match on (see the table on page 7-10).
10. When you are finished configuring the filter, select ADD THIS FILTER NOW to save the filter in the filter set. Select CANCEL to discard the filter.

TCP filter. You can increase security on connections using TCP by filtering by protocol type and matching established TCP connections only. With this filter attached to an active connection profile, no TCP connections can be established from outside the firewall, increasing network security.

You can add a TCP filter to a filter set with the following steps:

1. In the Add Filter screen, toggle the Enabled field to Yes.
2. Select Forward and toggle it to Yes.
3. Select the Protocol Type field and type in TCP. Then press Return.
4. In the last field that appears, Established TCP Conns. Only, toggle the entry to Yes and press Return. This new field configures the filter to match TCP packets for established TCP connections only.
5. Select ADD THIS FILTER NOW and press Return.

With this filter in effect, users from outside the firewall cannot initiate TCP connections to devices on your network, including your FTP server, Web server, and Telnet. To provide limited access to your network, set up a filter to forward traffic to a specific port, such as the FTP server port, Web server port, or Telnet port, and to a specific IP address and mask, in addition to restricting all outside TCP connections.

Viewing filters

To display a view-only table of input (output) filters, select Display / Change Input Filters (Display / Change Output Filters) in the Add IP Filter Set screen.

Modifying filters

To modify a filter, select Display / Change Input Filter (Display / Change Output Filter) in the Add IP Filter Set screen to display a table of filters.

Select a filter from the table and press Return to go to the Change Filter screen. The parameters in this screen are the same as the ones in the Add Filter screen (see “Adding filters to a filter set” on page 7-20).

```
                    Change Filter

Enabled:                    No
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:              0

Source Port Compare...      No Compare
Source Port ID:             0
Dest. Port Compare...       No Compare
Dest. Port ID:              0


Enter the IP specific information for this filter.
```

Deleting filters

To delete a filter, select Delete Input Filter (Delete Output Filter) in the Add Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press the Escape key to exit the table without deleting the filter.

Viewing filter sets

To display a view-only list of filter sets, select Display / Change Filter Sets in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select Display / Change Filter Set in the Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to go to the Change IP Filter Set screen. The items in this screen are the same as the ones in the Add Filter screen (see “Adding filters to a filter set” on page 7-20).

```
                        Change IP Filter Set


        Filter Set Name:                    Basic Firewall

        Display/Change Input Filter...
        Add Input Filter...
        Delete Input Filter...


        Display/Change Output Filter...
        Add Output Filter...
        Delete Output Filter...
```

Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, you’ll have to note their configuration before deleting the current filter set and then recreate them.

To delete a filter set, select Delete Filter Set in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press the Escape key to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set, called Basic Firewall, which is part of the Netopia Router's factory configuration. You can add Basic Firewall to your connection profiles or the answer profile (see "Connection profiles for ISDN and Leased lines" on page 2-13 and "Default profile" on page 2-39).

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative "that which is not expressly permitted is prohibited" approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect as filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that wish to access servers on the WAN, not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See "Possible modifications," below, for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or 80 for WWW.

AURP tunnel. To allow an AURP tunnel between a remote AURP router with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243) and a local AURP router (including the Netopia Router itself), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: UDP
- Source Port Comparison: Equal
- Source Port ID: 387
- Dest. Port Comparison: Equal
- Dest. Port ID: 387

Chapter 8

Token Security Authentication

This chapter discusses how to configure and use security authentication on the Netopia Router.

Note: The security authentication feature only applies to Netopia Router models connecting over a dial-up ISDN line using the PPP-PAP-TOKEN or PPP-CACHE-TOKEN authentication protocol.

If you will not be using this feature, you can skip this chapter.

Securing network environments

Unauthorized tampering or theft of information on internal networks causes serious ramifications, given the reliance on information systems. Network abuse is a serious problem, complicated by the difficulty in detecting the source of the abuses. An unauthorized user can gain access to networks and copy information without leaving a trace.

Password protection is one solution, but static passwords are often insecure. They can be compromised, allowing unauthorized users to disguise themselves as authorized users and enter supposedly secure systems. However, a company called Security Dynamics™ has patented a security authentication technology to increase network security.

SecurID is a two-factor authentication process to protect against unauthorized access. This dynamic user authentication produces a randomly-generated security code mechanism that changes every 60 seconds. At login, authorized users enter their password and the code displayed on their SecurID token card. While a password may be compromised, the constantly changing access code, which requires the token card during system use, bars unauthorized users from entering the network.

Using the SecurID token card

Each SecurID token card is programmed with an algorithm that ensures every code displayed is valid only for that user at that particular time. The token card has a display that authorizes the individual user access to the computer. Through this authentication system, the user's identity is verified when the correct password and current code are entered from the user's token.

Personal identification number (PIN)

The user's password is called a personal identification number, or PIN. The user enters the secret PIN from a console connection, followed by the current code displayed on the token card. Then the access control module must authenticate the token's unique code in combination with the user's secret PIN before access is granted.

Key Security Authentication Features of the Netopia Router

As a remote device, the Netopia Router offers client/calling side security authentication. This feature allows the Netopia Router to call a server router and perform security card authentication. The router of the called server must have access to a server with ACE software loaded on it.

To perform security card authentication, each user must have a security authentication token card and a PIN. In addition, the user's identifying information must reside on the remote ACE servers for authentication negotiation to properly take place.

The Netopia Router supports the following user configurations for security authentication:

- Single user, calling a single destination (single session)
- Single user, calling multiple destinations (two simultaneous and separate sessions)
- Multiple users, calling a single destination (single session)
- Multiple users, calling multiple destinations (two simultaneous and separate sessions

Security authentication components

To properly identify and authenticate an authorized user, the following are required:

- A secret personal identification number (PIN) for each user.
- A security authentication token card.
- A Security Access Control Module (ACM).

Note: The Netopia Router currently only supports Ascend routers as ACMs.

- An external Netopia Router calling into a designated server. For example, a telecommuter dialing into a remote site from a Netopia Router interested in accessing personal email or file sharing services.

Note: The Netopia Router does not include a security authentication token card.

Configuring the Netopia Router for security authentication

To configure the Netopia Router to support security authentication, select an authentication method and set up a designated connection profile from the Advanced Configuration screen or your first connection profile from Easy Setup.

1. From the WAN Setup menu, select PPP / MP Options.

```
                              PPP/MP Options


        Data Compression...              +----------------+
                                         +----------------+
        Send Authentication...           | None           |
                                         | PAP            |
        Send User Name:                  | CHAP           |
        Send Password:                   | PAP-TOKEN      |
                                         | CACHE-TOKEN    |
        Receive User Name:               +----------------+
        Receive Password:

        B-Channel Usage...                 Dynamic

        BAP/BACP Enabled:                  Yes

        Maximum Packet Size:               1500



For PAP-TOKEN or CACHE-TOKEN -- Password protection is used.  Secure
Card needed to authenticate.
```

2. Select Send Authentication and press Return. From the pop-up menu, highlight PAP-TOKEN or CACHE-TOKEN. Your network administrator or the remote network administrator will tell you which method to select.

If you select PAP-TOKEN, select Send User Name and enter a name for your Netopia Router. You will not need to enter a Send Password for PAP-TOKEN. Press Return.

If you select CACHE-TOKEN, select Send User Name and enter a name for your Netopia Router. Then, select Send Password and enter a secret name or number. Press Return.

3. Set up a connection profile to use with your authentication method. See Chapter 2, for information on setting up a connection profile.

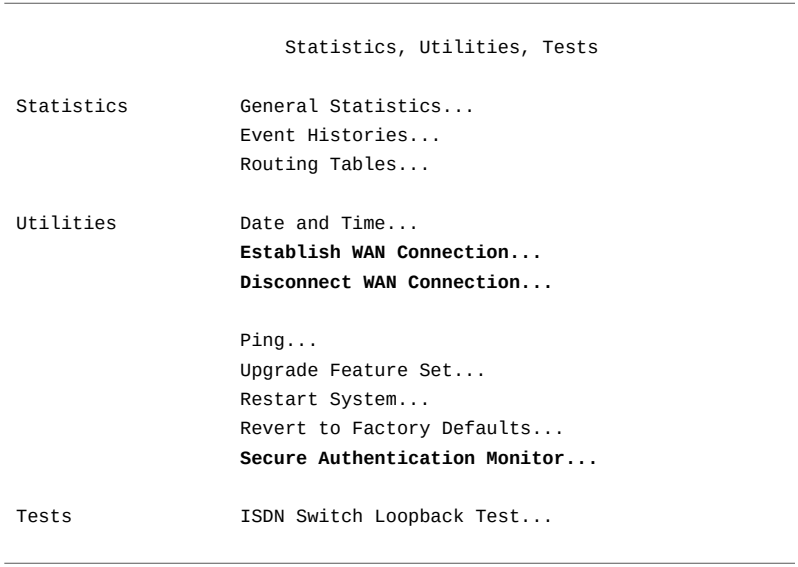
Note: If you are setting up your first connection profile, you can also enter your authentication information in the Easy Setup Connection Profile screen.

Initiating a connection call using security authentication

There are two ways to initiate a connection call using security authentication. You can either establish a dial-on-demand (DOD) connection or establish a manual connection.

Establishing a dial-on-demand (DOD) connection call

To establish a connection call using DOD, select Statistics, Utilities, Tests from the Main Menu and press Return.



1. Select Secure Authentication Monitor and press Return. The Secure Authentication Monitor screen appears.

Note: The Secure Authentication Monitor field will remain hidden if PAP-TOKEN or CACHE-TOKEN is not the selected authentication method in the connection profile.

2. Wait for the call to initiate.

```
                        Secure Authentication Monitor


                      Current ISDN Connection Status
Profile Name---State---%Use---Remote Address---Est.---More Info---



Status --- Passcode Required

For Connection Profile:  Easy Setup Profile

0-Challenge: Enter PASSCODE:
Passcode:                   123412345678
```

3. From the fields that appear, select Enter PASSCODE and press Return. Enter your PIN and the code displayed on your security authentication token card LED screen.
4. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one B-channel, you will be prompted for each B-channel being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN for a 2B-Channel call, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Establishing a manual connection call

To establish a Manual connection call, select the Statistic, Utilities, Tests from the Main Menu and press Return.

1. Select Establish WAN Connection from the Statistics, Utilities, Tests screen and press Return. The Establish WAN Connection screen displays a table of all of the connection profiles you have defined. Highlight the connection profile you wish to manually call. Press Return to initiate the call.

```
                              Call Status

                    Profile Name -- Easy Setup Profile
                    Connection State -- Dialing

                    Channel B1 State -- Acquiring

                    Channel B2 State --


 0-Challenge: Enter PASSCODE:
 Passcode:                    123412345678


Hit ESCAPE/RETURN/ENTER to return to previous menu.
```

2. From the fields that appear, select Enter PASSCODE and press Return. Enter your PIN and the code displayed on your security authentication token card LED screen.
3. Once the call is established, and you enter your passcode as prompted, PPP negotiation will continue. If the call is specified for PAP-TOKEN, and the session involves more than one B-channel, you will be prompted for each B-channel being brought up.

Note: When using CACHE-TOKEN, your passcode is valid for a time interval determined by the network administrator. When this time interval expires, you must provide a new passcode for the call negotiation.

When using PAP-TOKEN for a 2B-Channel call, your passcode is valid for one call negotiation. For a second call negotiation, you must enter the next passcode provided by the security authentication token card every 60 seconds.

You will be able to access information at the remote site that you are connecting to once authentication is successfully completed.

Troubleshooting

If the security authentication process did not negotiate properly, check for the following:

- If your security authentication token card is providing you with a passcode but is being rejected by the Radius server, your token card may be out of sync with the Radius server, or the server is not correctly configured to accept your account information.
- If your security authentication token card is not providing you with a passcode, the card may have expired or either the Netopia Router or Radius server is misconfigured.

For further information on how to troubleshoot these kinds of problems, contact the manufacturer of your security authentication software and hardware, or contact Farallon Technical Support.

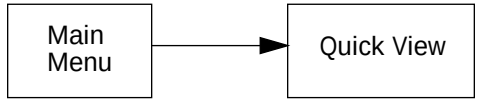
Chapter 9

Monitoring Tools

This chapter discusses the Netopia Router's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

Status overview

You can get a useful, overall status report from the Netopia Router in the Quick View screen. To go to the Quick View screen, select Quick View in the Main Menu.



The Quick View screen has three status sections:

- General status
- Current Status
- LED Status

The status sections vary according to the interface of your Netopia Router.

General Status

All interfaces

```
                                Quick View

Ethernet Address - 00-00-c5-ff-60-8d  Current Date - 5/30/97 03:49:52PM
Firmware Version - 3.0
WAN Line Rate - 64 Kbps

IP Address - 163.176.8.128            AppleTalk ET Address - 33051:150
IPX Network Address - 00000000        AppleTalk LT Address - 33050:149
```

Ethernet Address: The Netopia Router's hardware address.

Firmware Version: The version of the software that controls the Netopia Router. This number is useful if you call Farallon technical support and are asked for the firmware version running on the router. The firmware version number is also displayed on the Main Menu.

WAN Line Rate: The rate of the leased line connection. This field appears only on permanent leased lines.

Current Date: The current date. This can be set with the Date and Time utility (see "Setting the system date and time" on page 10-2).

IP Address: The Netopia Router's IP address, entered in the IP Setup screen.

IPX Network Address: The Netopia Router's IPX address, entered in the IPX Setup screen.

AppleTalk ET Address: The Netopia Router's AppleTalk address on its EtherTalk Phase II interface, entered in the EtherTalk Phase II Setup screen.

AppleTalk LT Address: The Netopia Router's AppleTalk address on its LocalTalk interface, entered in the LocalTalk Setup screen.

Current Status

The current status section is a table showing the current status of ISDN, the WAN, or Frame Relay.

Current ISDN Connection or WAN Status

ISDN only

```
                        Current ISDN Connection Status
---Profile Name------State---%Use-Remote Address----Est.-More Info----------
ISP                   CH1     10  IP 92.163.4.1      Lcl  NAT 192.163.100.6
```

Leased line with PPP or HDLC enabled only

```
                             Current WAN Status
---Profile Name------State---%Use-Remote Address----Est.-More Info----------
ISP                   CH1     10  IP 92.163.4.1      Lcl  NAT 192.163.100.6
```

Profile Name: Lists the name of the connection profile being used, if any. This field will also indicate if the B-channel is in use for a POTS call.

State: Lists the channels in use for this connection.

%Use: Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.

Remote Address: Shows the IP address of the connected remote network if the connection is using IP. Otherwise, shows the IPX address of the connected remote network, if using IPX. For ISDN POTS calls, it shows the called DN if locally originated, otherwise the calling DN (if available).

Est: Indicates whether the connection was locally or remotely established.

More Info: Indicates, 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).

Current Frame Relay Status

Leased line with Frame Relay enabled only

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

DLCIs In Use: Indicates the number of data link connection identifiers currently in use.

Bytes Rx: Indicates the total number of bytes received on the WAN link.

Bytes Tx: Indicates the total number of bytes sent on the WAN link.

Frames Rx: Indicates the total number of frames received on the WAN link.

Frames Tx: Indicates the total number of frames sent on the WAN link.

FECNs+BECNs: Indicates congestion of frames. The forward explicit congestion notification (FECN) indicates too much data at too high a speed is being received. The backward explicit congestion notification (FECN) indicates too much data at too high a speed is being sent.

LED Status

This section shows the current real-time status of the Netopia Router's LEDs. It is useful for remotely monitoring the router's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

All interfaces

```
                                  LED Status
-----ETHERNET------+--CH1-----MGMT----CH2---+-CARD-+-PWR +-------LEDS--------
 LNK LNK TX COL AUI    RX LNK  RDY TX  RX LNK              |'-'= Off 'E'= Error
  -   -   -   -   -     -  -    -   -   -  -      -     O  |'O' = On '*'= Blink
```

Each LED representation can report one of four states:

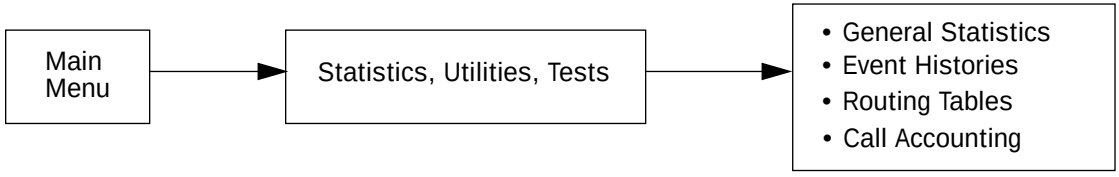
–: A dash means the LED is off.

*: An asterisk means the LED is blinking.

O: The letter “O” means the LED is on (solid).

E: The letter “E” means the LED is reporting an error.

Statistics



When you are troubleshooting your Netopia Router, the Statistics screens provide insight into the recent event activities of the Router.

Go to the Statistics, Utilities, Tests and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select General Statistics in the Statistics, Utilities, Tests screen.

General Statistics

```
---Type--------------Rx---------Tx--+-Type-------------------------------------
   IP Pkts            0          0  | EN Rx Packets                        0
   IPX Pkts           0          2  | EN Rx Errors                         0
   ET II Pkts         0         36  | EN Collisions                        0
                                    | FEBE/NEBE Err                      0/0
   LT Packets         0         36  | LT Bad Packets                       0
```

General Statistics displays information about data traffic on the Netopia Router's PhoneNet and Ethernet ports. This information is useful for monitoring and troubleshooting your LAN.

The left side of the screen lists total packets received and total packets transmitted for the following protocols:

- IP (IP packets on the Ethernet)
- IPX (IPX packets on the Ethernet)
- ET II (AppleTalk packets on Ethernet, using EtherTalk Phase II)
- LT (LocalTalk on the PhoneNET)

The right side of the table lists the total number of occurrences of each of five types of communication statistics:

EN Rx Packets: The number of Ethernet packets received.

EN Rx Errors: The number of bad Ethernet packets received.

EN Collisions: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN.

ISDN only

FEBE/NEBE Errors: The number of bad FEBE/NEBE packet errors. FEBE (Far End Bit Errors) is a counter of bad packets coming from the ISDN switch to the Router. NEBE (Near End Bit Errors) is a counter of bad packets coming from the Router to the ISDN switch.

LT Bad Pkts: An error occurring when unacceptable LocalTalk packets are received by the Netopia Router.

WAN Connection Statistics

ISDN only

```
----------------------WAN Connection Statistics----------------------
Ch.---Bytes Rx----Bytes Tx--Packets Rx--Packets Tx--Remote Network-----
1            0           0           0           0
2            0           0           0           0
D            0           0           0           0
```

Leased line with PPP or HDLC enabled only

```
----------------------WAN Connection Statistics----------------------
Ch.---Bytes Rx----Bytes Tx--Packets Rx--Packets Tx--Remote Network-----
1            0           0           0           0
```

Leased line with Frame Relay enabled only

```
----------------------WAN Connection Statistics----------------------
---------Bytes Rx-----Bytes Tx-----Frames Rx----Frames Tx----FECNs-------BECNs
              0           0           0           0           0           0
```

The WAN Connection Statistics give the following information about each channel of the point-to-point interface:

- The number of bytes and packets received through the channel
- The number of bytes and packets transmitted through the channel

Not applicable with Frame Relay enabled

- The IP address of the remote network to which the Netopia Router is connected through the channel
- The congestion notifications (FECNs and BECNs) indicating too much data at too high a speed begin received (FECN) or sent (BECN)

Frame Relay LMI Statistics

Models with Frame Relay enabled only

```
    ----------------------Frame Relay LMI Statistics----------------------
    LMI Status Pkts Rx             0  | LMI Status Enq's Tx              0
```

Interfaces using Frame Relay also include the Frame Relay LMI Statistics. This section displays how many local management interface (LMI) packets have been received and how many LMI enquiries have been sent.

DLCI Traffic Statistics

Models with Frame Relay enabled only

```
                                DLCI Statistics

 DLCI----Remote IP Addr--IPX Net----Frames Rx--Frames Tx---Bytes Rx---Bytes Tx
 ---------------------------------SCROLL UP-----------------------------------
16               --        --            0          0          0          0
17               --        --            0          0          0          0
18               --        --            0          0          0          0

 --------------------------------SCROLL DOWN---------------------------------

Select a DLCI and hit Return/Enter for more information.
```

Interfaces using Frame Relay also offer the DLCI Traffic Statistics field. By selecting DLCI Traffic Statistics in the General Statistics screen and pressing Return, you can view the DLCI Statistics table.

The table provides the following information for each DLCI:

DLCI: Lists the data link connection interfaces.

Remote IP Addr: The IP address of the destination node for that DLCI.

IPX Net: The IPX address of the node sending that DLCI.

Frames Rx: The number of frames received on that DLCI.

Frames Tx: The number of frames sent with on DLCI.

Bytes Rx: The number of bytes received with on DLCI.

Bytes Tx: The number of bytes sent with on DLCI.

If the DLCI statistics table exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select the SCROLL UP item at the top of the list and press the Return key. To scroll down, select the SCROLL DOWN item at the bottom of the list and press Return.

To obtain more information about any DLCI listed in the table, select the DLCI and press Return. A dialog box containing more information about the selected DLCI will appear. Press Return or the Escape key to dismiss the dialog box.

Event Histories

The Netopia Router records 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 ISDN or leased line.

Note: Netopia Router's built-in battery backup prevents loss of event history from a shut down or reset.

The Router's event histories are structured to display most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk.

To go to the Event Histories screen, select Event Histories in the Statistics, Utilities, Tests screen.

Device Event History

The Device Event History screen lists port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

To go to the Device Event History screen, select Device Event History in the Event Histories screen.

```
                          Device Event History
                                        Current Date --   6/4/98 09:23:53 AM
 -Date-----Time-----Event-------------------------------------------------------
 ---------------------------------SCROLL UP-------------------------------------
 06/04/97 08:56:13   AppleTalk initialization complete
 06/04/97 08:56:06   IPX initialization complete
 06/04/97 08:56:06   IP address server initialization complete
 06/04/97 08:56:06 --BOOT: Cold start v3.2-------------------------------------
 06/04/97 08:52:28   AURP initialization complete
 --------------------------------SCROLL DOWN-----------------------------------

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

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select the SCROLL UP item at the top of the list and press the Return key. To scroll down, select the SCROLL DOWN item at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or the Escape key to dismiss the dialog box.

To clear the Device Event History, select Clear Device Event History in the Event Histories screen.

WAN Event History

The WAN Event History screen lists events on the ISDN or leased line. The most recent events appear at the top.

To go to the WAN Event History screen, select WAN Event History in the Event Histories screen.

```
                              WAN Event History
                                                Current Date --   6/4/97 04:36:11 PM
 -Date-----Time-----Event-----------------------------------------------------------
 ---------------------------------SCROLL UP---------------------------------
 06/04/97 16:35:44   PPP: IPXCP negotiated, session 1
 06/04/97 16:35:44   PPP: IPCP negotiated, session 1, rem: 192.173.119.1
 06/04/97 16:35:43   PPP: MP negotiated, session 1
 06/04/97 16:35:43   PPP: PAP  remote accepted us, Channel 1
 06/04/97 16:35:43   PPP: NCP up, session 1, Channel 1
 06/04/97 16:35:41   PPP: Channel 1 up, Dialout
 06/04/97 16:35:41   Received Connect Ind. for DN: 915105551111
 06/04/97 16:35:41 >>Issued 64Kb Setup Request from our DN: 5105771234
 06/04/97 16:34:57   Received Clear Confirm for our DN: 5105771234
 06/04/97 16:34:56   Requested Disc. from DN: 915105551111, Cause: 16
 06/04/97 16:34:56   PPP: Channel 1 down
 06/04/97 16:34:56 * PPP: PAP  authentication failed, Channel 1
 06/04/97 16:34:54   PPP: Channel 1 up, Dialout
 06/04/97 16:34:54   Received Connect Ind. for DN: 915105551111
 06/04/97 16:34:53 >>Issued 64Kb Setup Request from our DN: 5105771234
 ---------------------------------SCROLL DOWN---------------------------------

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

Each entry in the list contains the following information:

Time: Time of the event.

Date: Date of the event.

Event: A brief description of the event.

Models on switched circuits only

Ch.: The channel involved in the event.

Models on switched circuits only

Dir. Number: The directory number (number dialed) involved in the event.

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select the SCROLL UP item at the top of the list and press the Return key. To scroll down, select the SCROLL DOWN item at the bottom of the list and press the Return key.

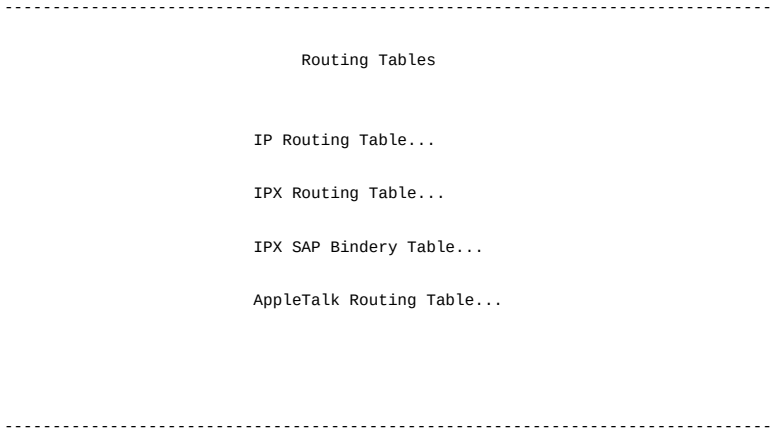
To get more information about any event listed in the WAN Event History, select the event and then press the Return key. A dialog box containing more information about the selected event will appear. Press Return or the Escape key to dismiss the dialog box. Also see Appendix D, “ISDN, DDS/ADN, and T1 Events” for explanations of the possible events.

To clear the WAN Event History, select Clear WAN Event History in the Event Histories screen.

Routing Tables

You can view all of the IP, IPX and AppleTalk routes in the Netopia Router’s IP, IPX and AppleTalk routing tables, respectively.

To go to the Routing Tables screen, select Routing Tables in the Statistics, Utilities, Tests screen.



IP routing table

The IP routing table displays all of the IP routes currently known to the Netopia Router.

To display the IP Routing Table screen, select IP Routing Table in the Routing Tables screen and go to the IP Routing Table screen.

IPX routing table

The IPX routing table displays all of the IPC routes currently known to the Netopia Router.

To display the IPX Routing Table screen, select IPX Routing Table in the Routing Tables screen and go to the IPX Routing Table screen.

IPX Sap Bindery table

The IPX Sap Bindery table displays all of the IPX Sap Bindery routes currently known to the Netopia Router.

To display the IPX Sap Bindery table screen, select IPX Sap Bindery table in the Routing Tables screen and go to the IPX Sap Bindery table screen.

AppleTalk routing table

The AppleTalk routing table displays information about the current state of AppleTalk networks connected to the Netopia Router, including remote AppleTalk networks connected with AURP. This information is gathered from other active AppleTalk routers.

To go to the AT Routing Table screen, select AppleTalk Routing Table in the Routing Tables screen.

```
                                AT Routing Table

 -Net---Range--(Def) Zone Name---------Hops-State-Next Rtr Addr.--Pkts Fwded---
 ----------------------------------SCROLL UP-----------------------------------
  1     --     Admin                   2    Good  46.131          2
  2     --     Admin                   2    Good  46.131          0
  3     --     Operations              2    Good  46.131          1
  4     --     Sales                   2    Good  46.131          0
  5     --     Marketing               2    Good  46.131          1
  6     --     Marketing               2    Good  46.131          2
  7     --     Customer Service        2    Good  46.131          1
  8     --     TechSports              2    Good  46.131          0
  10    --     R&D                     2    Good  46.131          0
  11    --     R&D                     2    Good  46.131          0
  12    --     R&D                     2    Good  46.131          1
  16    --     UNIX Services           2    Good  46.131          0
 *24    27     Operations              1    Good  46.131          186
  28    31     R&D                     1    Good  46.131          36
 --------------------------------SCROLL DOWN---------------------------------
 UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

Each row in the AppleTalk routing table corresponds to an AppleTalk route or network range. If the list of routes shown exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select the SCROLL UP item at the top of the table and press the Return key. To scroll down, select the SCROLL DOWN item at the bottom of the table and press the Return key.

The table has the following columns:

Net: Displays the starting network number supplied by the AppleTalk router in the ‘Next Rtr Addr. Column’. If a network number is preceded by an asterisk (*), it has multiple zones. To display the zones, select the network entry and press Return.

Range: Displays the ending network number for the extended network.

(Def) Zone Name: Displays the zone or zones associated with the specified network or network range. The zone name shown is either the only zone for a non extended network (e.g.:LocalTalk networks), or the default zone name for an extended network. To see the complete list of zones for an extended network with multiple zones, select the entry in the table and press the Return key. Press the Return key again to close the list of zones.

Hops: Displays the number of routers between the Netopia Router and the specified network.

State: Displays the state of the specified route, based on the frequency of Routing Table Maintenance Protocol (RTMP) packets received for the route. The state can be Good, Suspect, or Bad. AppleTalk routers regularly exchange RTMP packets to update AppleTalk routing information.

Next Rtr Addr.: Displays the DDP or IP address of the next hop for the specified route. A DDP address is displayed if the router shown is on the local AppleTalk network. DDP address means that a connection to the next hop router is by a native AppleTalk network (e.g.: LocalTalk or EtherTalk Phase II). An IP address is displayed if the Netopia Router is connected to the router shown using AURP. IP address means a connection transports over AURP (AppleTalk encapsulated IP).

Pkts Fwded: The number of packets sent to the router shown.

The AppleTalk routing table updates automatically when you first display this screen, but not while you are viewing it. To update the AppleTalk routing table, select UPDATE (near the bottom left-hand side of the screen) and press Return.

Call Accounting

The Netopia Router offers system-wide call accounting to track first minutes (an ISDN tariff factor) and additional minutes, for initiated data and voice calls.

To go to the Call Accounting screen, select Call Accounting in the Statistics, Utilities, Tests screen.

```
                          Call Accounting

        Enable Call Accounting:           On

        Day for auto-reset of timers:     12

        Maximum connect time (HH:MM):     12:00


                          RESET MINUTE COUNTERS


-------- Call Accounting Statistics ---------------------------------

        Total First Minutes:              0
        Total Additional Time (HH:MM):    0:00
        Remaining Time (HH:MM):           10:25
        Trigger Date(MDY):                1/1/98
```

To enable call accounting, follow these steps:

1. Select Enable Call Accounting and toggle it to On.
2. Select Day for auto-reset of timers and enter the day of the month for the Router to reset the Call Accounting Statistics.
3. Select Maximum connect time (HH:MM) and enter the total amount of time to allow for outbound calls, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.
4. Select RESET MINUTE COUNTERS and press Return to manually reset the Call Accounting Statistics.

Under Call Accounting Statistics:

- Total First Minutes displays the total number of first minutes of outbound calls placed during the recording interval.
- Total Additional Minutes (HH:MM) displays the total remaining time of all outbound calls placed during the recording interval.

- Remaining Time (HH:MM) displays how much time is left in the recording interval. If call accounting is not enabled, the message will read, Call Accounting Disabled.
- Trigger Date (MDY) displays the date, in month, day, year format, when the call accounting begins.

SNMP

The Netopia Router includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

The Netopia Router supports the following Management Information Base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- AppleTalk MIB-I (RFC 1243)
- Frame Relay DTE MIB (RFC 1315)
- Farallon Netopia MIB

These MIBs are on the Netopia Router CD included with the Netopia Router. You should load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

sysObjectID and sysDescr

The value returned by the Netopia Router SNMP agent for sysObjectID is 1.3.6.1.4.1.304.2.2.*x*, where *x* is dependent upon your model number and defined in the table below:

Netopia Model no.	*x*	Netopia Model no.	*x*
420	16	620	17
430	5	630	3
435	6	635	10
440	2	640	4
450	8	650	12
455	9	655	13
460	14	660	15

The value returned by the Netopia Router SNMP agent for sysDescr is Netopia PN*yyy*, where *yyy* is your particular Netopia Router model number. For some models, *yyy* also includes a suffix to the model number. See the table below.

Non-North American ISDN Netopia Routers	yyy-(two-character country code)-1S
SA Netopia Routers	yyy-SA
T1 Netopia Routers	yyy-T1
DDS Netopia Routers	yyy-DDS

The SNMP Setup screen

To go to the SNMP Setup screen, select SNMP in the Advanced Configuration screen.

```
                              SNMP Setup


        System Name:
        System Location:
        System Contact:


        Read-Only Community String:        public
        Read/Write Community String:       private

        Authentication Traps Enable:       Off

        IP Trap Receivers...


Configure optional SNMP parameters from here.
```

Follow these steps to configure the first three items in the screen:

1. Select System Name and enter a descriptive name for the Netopia Router's SNMP agent.
2. Select System Location and enter the router's physical location (room, floor, building, etc.).
3. Select System Contact and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia Router SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB-II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The Read-Only Community String and the Read/Write Community String are like passwords that must be used by an SNMP manager querying or configuring the Netopia Router. An SNMP manager using the Read-Only Community String can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the Read/Write Community String can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to "public" and "private," respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Caution! Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia Router through SNMP.

For more information on security issues, see "Suggested security measures" on page 7-2.

SNMP traps

An SNMP trap is an informational message sent from an SNMP agent (in this case, the Netopia Router) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

Standard traps generated by the Netopia Router include the following:

- An authentication failure trap is generated when the router detects an incorrect community string in a received SNMP packet. Auth. Traps Enable must be On for this trap to be generated.
- A cold start trap is generated after the router is reset.

- An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia Router sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia Router. Up to eight receivers can be set. You can also review and remove IP traps.

Go to the IP Trap Receivers screen by selecting IP Trap Receivers in the SNMP Setup screen.

```
                          IP Trap Receivers


                    Display/Change IP Trap Receiver...

                    Add IP Trap Receiver...

                    Delete IP Trap Receiver...


Return/Enter to modify an existing Trap Receiver.
Navigate from here to view, add, modify and delete IP Trap Receivers.
```

Setting the IP trap receivers

1. Select Add IP Trap Receiver.
2. Select Receiver IP Address or Domain Name. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select Community String if you enabled one in the SNMP Setup screen, and enter the appropriate password.
4. Select Add Trap Receiver Now and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select Display / Change IP Trap Receiver in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select Display / Change IP Trap Receiver in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the Change IP Trap Receiver screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select Delete IP Trap Receiver in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select Cancel and press Return.

Chapter 10

Utilities and Tests

A number of utilities and tests are available for system diagnostic and control purposes:

- Setting system date and time (see page 10-2)
- Establishing and disconnecting WAN connections (see Chapter 2)
- Running a ping test (see page 10-3)
- Counting the number of routers between the Netopia Router and a given destination (see page 10-7)
- Upgrading feature sets and WANlets (see page 10-8)
- Restarting the system (see page 10-8)
- Reverting to factory default settings (see page 10-9)
- Monitoring secure authentication (see Chapter 2)
- Running an ISDN loopback test (see page 10-9)
- Configuring the console (see page 10-11)
- Transferring configurations and firmware files (see page 10-12 and page 10-17)

Note: These utilities and tests are accessible only through the console-based management screens. If you used Web-based management to configure your Router, see Chapter 4, “Installing the Netopia Router,” of the *Getting Started Guide* for information on accessing the console-based management screens.

Some utilities and tests may not be available on some Netopia Router models, depending on the switch type and data encapsulation method. See the following sections for more information.

Setting the system date and time

You can set the system's date and time in the Set Date and Time screen.

Select Date and Time in the Statistics, Utilities, Tests screen and press Return to go to the Set Date and Time screen.

```
                        Set Date and Time


System Date Format:                MM/DD/YY
Current Date (MM/DD/YY):           1/1/1998

System Time Format:                AM/PM
Current Time:                      09:40
AM or PM:                          AM
```

Follow these steps to set the system's date and time:

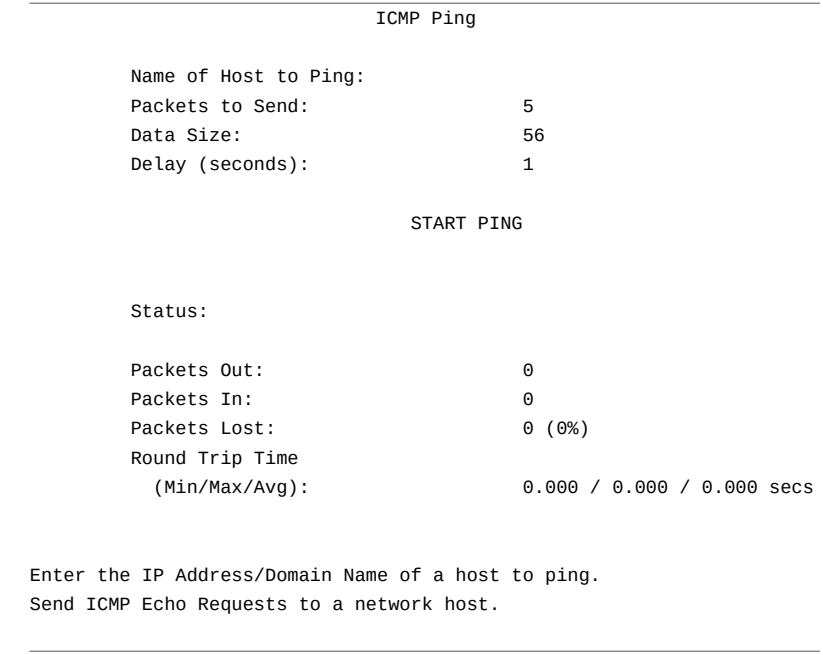
1. Select System Date Format and choose how the date will be displayed. DD represents the day, MM represents the month, and YY represents the year.
2. Select Current Date and enter the date in the appropriate format. Use one- or two-digit numbers for the month and day, and the last two digits of the current year. The date's numbers must be separated by forward slashes (/).
3. Select System Time Format and choose the 12-hour clock (AM/PM) or the 24-hour clock (24hr).
4. Select Current Time and enter the time in the format HH:MM, where HH is the hour (using either the 12-hour or 24-hour clock) and MM is the minutes.
5. Select AM or PM and choose AM or PM. The AM or PM item appears only if the time is in the 12-hour clock format.

Ping

The Netopia Router includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Netopia Router. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

To use the Ping utility, select Ping in the Statistics, Utilities, Tests screen and press Return to go to the Ping screen.



To configure and initiate a Ping test, follow these steps:

1. Select Name of Host to Ping and enter the destination domain name or IP address.

2. Select Packets to Send to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you may change it to any value from 1 to 4,294,967,295.
3. Select Data Size to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you may change it to any value from 0 (only header data) to 1664.
4. Select Delay (seconds) to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you may change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately one after another.
5. Select START PING and press Return to begin the Ping test. While the test is running, the START PING item becomes STOP PING. To manually stop the Ping test, select STOP PING and press Return or the Escape key.

While the Ping test is running, and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

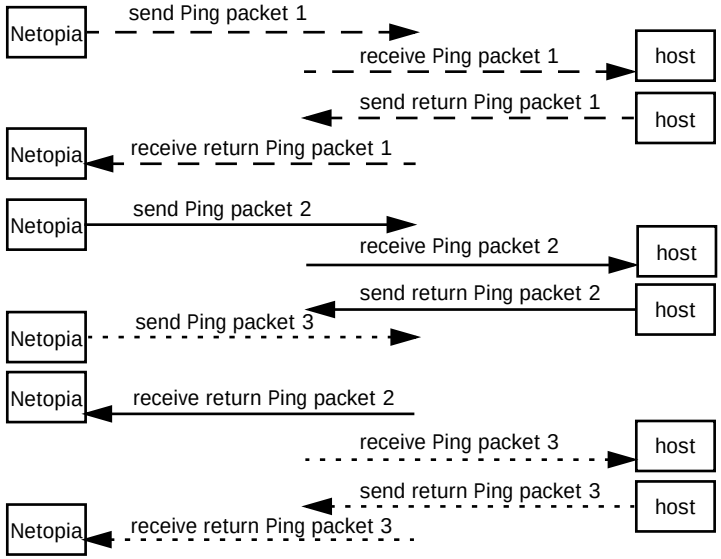
Status: The current status of the Ping test. This item can display the following messages:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name-style name
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the router with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered "on time," return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the Packets In count.

In the example below, a Netopia Router is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Netopia Router before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between Packets Out and Packets Lost, and Packets In is noticeably lagging behind Packets Out, the destination is probably unreachable. In this case, use STOP PING.

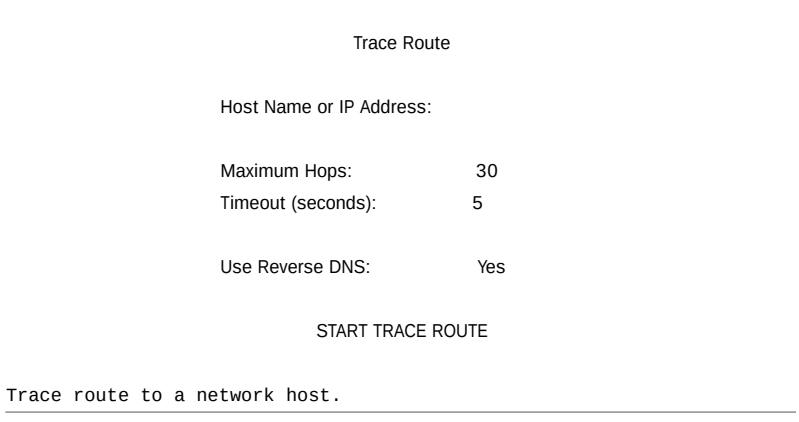
Round Trip Time (Min / Max / Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia Router is 255, the maximum allowed. The TTL value defines the number of IP routers that the packet can traverse. Ping packets that reach their TTL value are dropped, and a “destination unreachable” notification is returned to the sender (see the table above). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group’s ipDefaultTTL object.

Tracing a route

You can count the number of routers between your Netopia Router and a given destination with the Trace Route utility.

Select Trace Route in the Statistics, Utilities, Tests screen and press Return to go to the Trace Route screen.



To trace a route, follow these steps:

1. Select Host Name or IP Address and enter the name or address of the destination you want to trace.
2. Select Maximum hops (1..64) to set the maximum number of routers to count between the Netopia Router and the destination router, up to 64. The default is 30 hops.

3. Select Timeout per probe (1..10 sec) to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.
4. Select Use Reverse DNS to learn the names of the routers between the Netopia Router and the destination router. The default is Yes.
5. Select START TRACE ROUTE and press Return. The screen will be replaced by a scrolling screen, listing the destination, the number of hops, the IP addresses of each hop, and the DNS names, if selected.
6. Cancel the trace by pressing Esc. Return to the Trace Route screen by pressing Esc twice.

Upgrading the Netopia Router

You can upgrade your Netopia Router by adding new feature sets through the Upgrade Feature Set utility.

See the release notes that came with your router or visit the Farallon web site at www.farallon.com for information on new feature sets, how to obtain them, and how to install them on your Netopia Router.

Restarting the system

You can restart the system by selecting the Restart System item in the Statistics, Utilities, Tests screen.

You must restart the system whenever you reconfigure the Netopia Router and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions.

Factory defaults

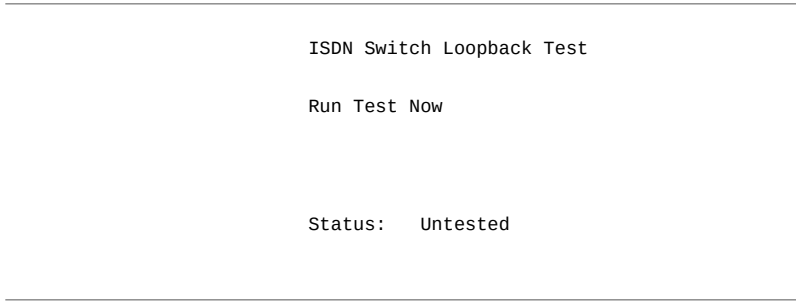
You can reset the Netopia Router to its factory default settings. Select the Revert to Factory Defaults item in the Statistics, Utilities, Tests screen and press Return. Select CONTINUE in the dialog box and press Return. The Netopia Router settings will return to the factory defaults, deleting your configurations.

The ISDN loopback test

The ISDN loopback test is designed to confirm the existence of a working ISDN line and the proper configuration of certain Netopia Router parameters. This test is available only on switched ISDN lines.

Using the first B-channel, the test calls the Netopia Router on the second B-channel, creating a call loop back to the unit.

To run the ISDN loopback test, select ISDN Switch Loopback Test in the Statistics, Utilities, Tests screen and press Return to go to the ISDN Switch Loopback Test screen.



Select Run Test Now and press Return. The loopback test is executed immediately.

Note: Make sure neither B-channel is in use before you execute the loopback test.

The Status item reports one of three results:

Untested: The loopback test has not yet been run.

Loopback Test FAILED: The loopback test has failed. See "If the loopback test fails," below, for troubleshooting suggestions.

Loopback Test PASSED. The loopback test was successful. The line is working properly, and the directory numbers (the ISDN phone numbers associated with each B-channel) are correct. If a SPID is associated with the first B-channel, its correctness is also confirmed. If a SPID is associated with the second B-channel, its correctness is confirmed.

Note: SPIDs are applicable to certain North American ISDN switch protocols.

If the loopback test fails

Follow these suggestions to track down the reason behind the loopback test's failure:

- Check that the WAN Ready LED is solid green.
- Check the ISDN event log and get more information about events that seem relevant to the failure.
- Check the B-channel usage in the Quick View screen to make sure there were no active calls when the loopback test was performed.
- Check the accuracy of the directory numbers, SPIDs, and switch protocol you entered in the ISDN Line Configuration screen (compare them with the information you received from your ISDN service provider).
- Verify termination of the S/T bus.
- Contact your ISDN service provider to have the line checked.
- Check that your line is not provisioned for voice only (Circuit Switched Voice).

Console configuration

In the *Getting Started Guide*, it was suggested that you set the communications parameters in your terminal emulation software to match the Netopia Router's default settings. However, you can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select Console Configuration in the Advanced Configuration screen.

```
                        Console Configuration


                Baud Rate...              9600

                Bits per Character...     8

                Stop Bits...              1

                Parity...                 No Parity

        SET CONFIG NOW                    CANCEL
```

Follow these steps to change a parameter's value:

1. Select the parameter you want to change.
2. Select a new value for the parameter. Return to step 1 if you want to configure another parameter.
3. Select SET CONFIG NOW to save the new parameter settings. Select CANCEL to leave the parameters unchanged and exit the Console Configuration screen.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia Router's console or PC Card (PCMCIA) port.

To go to the PC Card Config/Firmware Transfer screen, select PC Card Config/Firmware Transfer in the Advanced Configuration screen.

```
                    PC Card Config/Firmware Transfer


                Send Firmware to Netopia...

                Send Config to Netopia...

                Receive Config from Netopia...


       PC Card Modem Init String:    AT&F&C1&D2E0S0=1\J0\Q3
```

The transfer you initiate will occur through the port from which you initiate it. If you are connected to the Netopia Router through its console port, the transfer will occur through that port. If you are connected through the PC Card port, the transfer will occur through that port.

Using the console port

Using the Netopia Router's screens through the console port. involves using either a PC or Macintosh computer with a terminal emulation program that supports XMODEM file transfers.

See the *Getting Started Guide* for directions on how to configure your terminal emulation program.

Using the SmartPort

Follow these steps to prepare to use the SmartPort (PC Card port):

1. Connect a standard PC Card modem to the port. See "Connecting a modem to the SmartPort" on page 1-4 for more information.

   The modem will be initialized using the default string contained in the PC Card Modem Init String item in the PC Card Config/Firmware Transfer screen. Consult your modem's user's guide and edit the default string it includes commands not supported by your modem. You may choose to substitute equivalent commands.

2. Connect a standard, working analog telephone line (*not* an ISDN line) to the modem.

3. Call the modem from another site using a computer, a modem, and a terminal emulation program (like the one used with the console port). The terminal emulation program should be configured as specified in the *Getting Started* guide.

Once you connect to the Netopia Router's modem, you should see the configuration screens. Press Ctrl-L if you connect but are unable to see the screens.

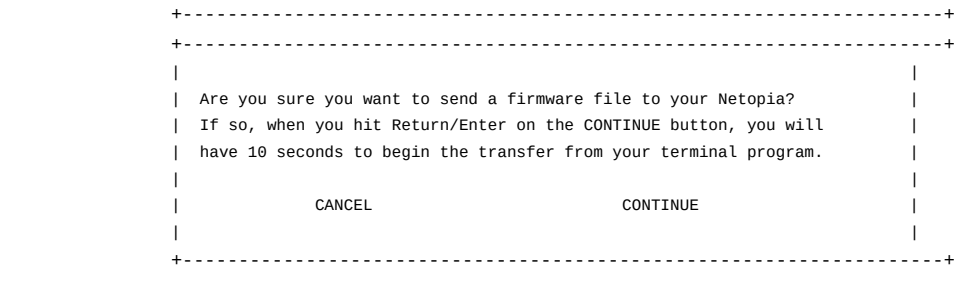
Updating firmware

Firmware updates may be available periodically from Farallon or from a site maintained by your organization's network administration.

The procedure below applies whether you are using the console or the PC Card port.

Follow these steps to update the Netopia Router's firmware:

1. Make sure you have the firmware file on disk and know the path to its location.
2. Select Send Firmware to Netopia and press Return. The following dialog box appears:



3. Select CANCEL to exit without downloading the file, or select CONTINUE to download the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the firmware file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution! Do not manually reset the Netopia Router while it is automatically resetting or it could be damaged.

Downloading configuration files

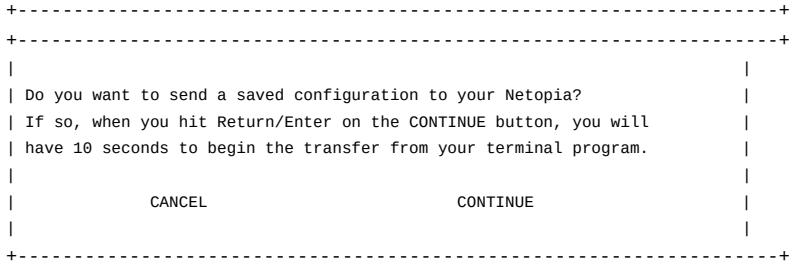
The Netopia Router can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

The procedure below applies whether you are using the console or the PC Card port.

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select Send Config to Netopia and press Return. The following dialog box appears:



3. Select CANCEL to exit without downloading the file, or select CONTINUE to download the file.

If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

The system will reset at the end of a successful file transfer to put the new configuration into effect.

Uploading configuration files

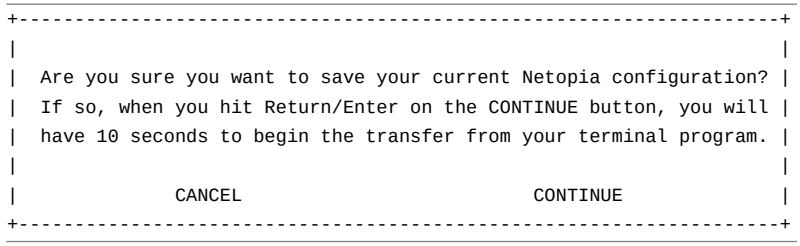
A file containing a snapshot of the Netopia Router's current configuration can be uploaded from the Router to disk. The file can then be downloaded by a different Netopia Router to configure its parameters (see "Downloading configuration files" on page 10-15). This is useful for configuring a number of Routers with identical parameters, or for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia Router by Farallon or your network administrator.

The procedure below applies whether you are using the console or the PC Card port.

To upload a configuration file:

1. Decide on a name for the file and a path for saving it.
2. Select Receive Config from Netopia and press Return. The following dialog box appears:



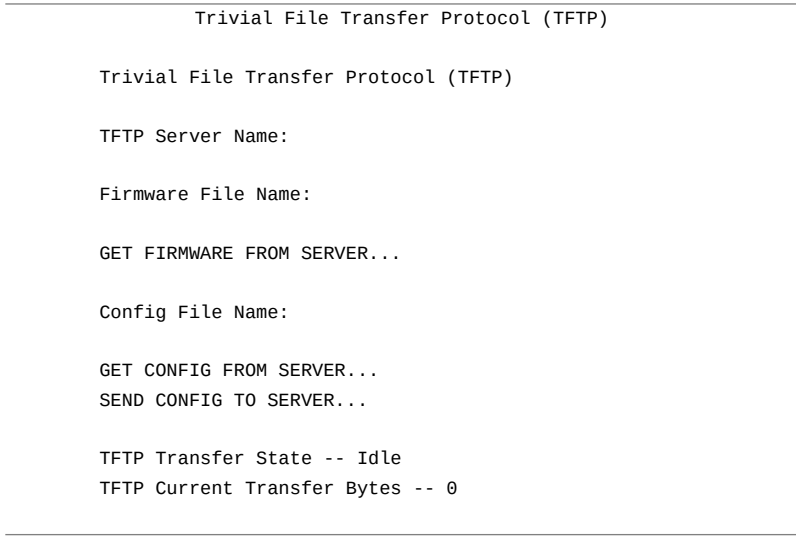
3. Select CANCEL to exit without uploading the file, or select CONTINUE to upload the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the Router as the client. To use the Router as a TFTP client, a TFTP server must be available.

To use TFTP, select Trivial File Transfer Protocol (TFTP) in the Advanced Configuration screen and press Return to go to the Trivial File Transfer Protocol (TFTP) screen.



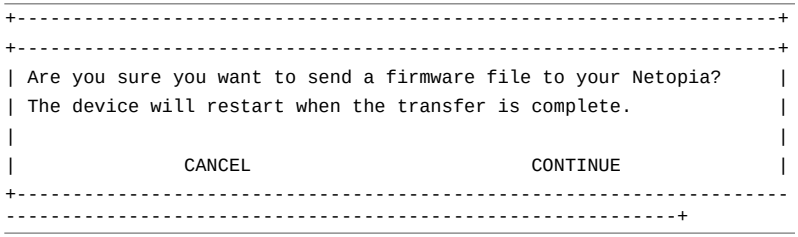
The sections below describe how to update the Router's firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Farallon or from a site maintained by your organization's network administrator.

To update the Router's firmware, follow these steps:

1. Select TFTP Server Name and enter the DNS name or IP address of the TFTP server you will use. The DNS name or IP address is available from the site where the server is located.
2. Select Firmware File Name and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
3. Select GET FIRMWARE FROM SERVER and press Return. You will see the following dialog box:



   Select CANCEL to exit without downloading the file, or select CONTINUE to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution! Do not manually reset the Netopia Router while it is automatically resetting or it could be damaged.

4. If you choose to download the firmware, the TFTP Transfer State item will change from Idle to Reading Firmware. The TFTP Current Transfer Bytes item will reflect the number of bytes transferred.

Downloading configuration files

The Router can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the Router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

1. Select TFTP Server Name and enter the DNS name or IP address of the TFTP server you will use. The DNS name or IP address is available from the site where the server is located.
2. Select Config File Name and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
3. Select GET CONFIG FROM SERVER and press Return. You will see the following dialog box:

```
+-------------------------------------------------------------------+
+-------------------------------------------------------------------+
| Are you sure you want to send a saved configuration to your Netopia? |
|                                                                   |
|                                                                   |
|              CANCEL                        CONTINUE               |
+-------------------------------------------------------------------+
```

   Select CANCEL to exit without downloading the file, or select CONTINUE to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.

4. If you choose to download the configuration file, the TFTP Transfer State item will change from Idle to Reading Config. The TFTP Current Transfer Bytes item will reflect the number of bytes transferred.

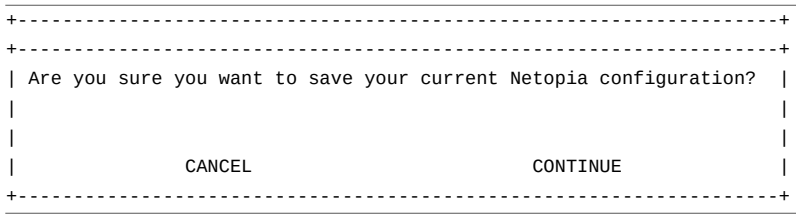
Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the Router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia Router unit to configure its parameters (see "Downloading configuration files" on page 10-19). This is useful for configuring a number of Routers with identical parameters, or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Netopia Router unit by Farallon or your network administrator.

To upload a configuration file, follow these steps:

1. Select TFTP Server Name and enter the DNS name or IP address of the TFTP server you will use. The DNS name or IP address is available from the site where the server is located.
2. Select Config File Name and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select SEND CONFIG TO SERVER and press Return. You will see the following dialog box:



Select CANCEL to exit without uploading the file, or select CONTINUE to upload the file. The system will reset at the end of the file transfer to put the new configuration into effect.

4. The TFTP Transfer State item will change from Idle to Writing Config. The TFTP Current Transfer Bytes item will reflect the number of bytes transferred.

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while using the Netopia Router. It also includes information on how to contact Farallon Technical Support.

Important information on these problems may be found in the event histories kept by the Netopia Router. These event histories can be accessed in the Statistics, Utilities, Tests screen.

Power outages

If you suspect that power was restored after a power outage, and the Netopia Router is connected to a remote site, you may need to switch the Netopia Router off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the Router should reestablish the connection.

Configuration problems

If you reconfigure the Netopia Router and the reconfigured settings do not seem to be taking effect, reset (restart) the system. You can reset the system by switching the Netopia Router off and back on.

Resetting the system will cause new configuration settings to take effect.

Console connection problems

Can't see the configuration screens (nothing appears)

- Check the cable connection from the Netopia Router's console port to the computer being used as a console.
- Check that the terminal emulation software is accessing the correct port on the computer that's being used as a console.
- Try pressing Ctrl-L or Return several times to refresh the terminal screen.
- Check that flow control on serial connections is turned off.

Junk characters appear on the screen

- Check that the terminal emulation software is configured correctly.
- Check the baud rate.

Characters are missing from some of the configuration screens

- Try changing the Netopia Router's default speed of 9.6 kbps and setting your terminal emulation software to match the new speed.

ISDN problems

The WAN Ready LED is blinking red

This is an indication that the Netopia Router cannot detect the ISDN switch at your ISDN service provider's central office.

- Check that the cable you are using for ISDN is not a 10Base-T cable, which can look similar to an ISDN cable.
- Check that you have plugged the correct cable into the Netopia Router's ISDN port, and not one of its EtherWave ports.

The WAN Ready LED is solid red

This is an indication that the Netopia Router is unable to synchronize with the switch at your ISDN service provider's central office.

- Confirm that you have entered the correct directory numbers when configuring the Router.
- Confirm that you have configured the Router with the correct ISDN switch protocol. The protocol selected should match the one used on your ISDN line.
- Check the ISDN event history to see what error it reports. You can select any event shown in the history and press Return to see more information on that event.

The WAN Ready LED is off

- The initial call made or received on the ISDN line may activate the WAN Ready LED. You can also activate the LED by using the ISDN loopback test. See "The ISDN loopback test" on page 10-9 for more information on using the ISDN loopback test.

Calls do not go through

If the Ready LED is glowing solid green and the ISDN loopback test is successful, calls you make with the Netopia Router should go through. There may be several reasons why a particular call does not go through:

- The number being dialed is wrong.
- The connection profile being used has the Dial On Demand parameter (in the Telco Options screen) set to No. It should be set to Yes, or you must manually initiate the call.
- The connection profile being used has the Dial parameter (in the Telco Options screen) set to Dial In Only. It should be set to Dial In/Out or Dial Out Only.
- The IP address is not set to 0.0.0.0 in the connection profile.

If you are trying to call an ISP, confirm the following:

- The ISP's directory number
- The authorization method you use (PAP, CHAP, or none) to access your ISP account
- If using PAP or CHAP, the name and password/secret you were given and their case (uppercase or lowercase)
- The ISP's IP address

Check the ISDN event history for more information.

Frame Relay problems

- Check the LMI to see if the Router is communicating over Frame Relay.
- Make sure the Router is auto-detecting the DLCI.
- Make sure the Router is using inverse ARP for the remote IP address, or the manually entered remote IP address is correct.
- Verify the port speed, CIR, B_c, and B_e.

Network problems

This section contains tips on ways you can troubleshoot a networking problem.

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway's IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia Router's ping utility, in the Statistics, Tests, Utilities screen, and try to ping local and remote hosts. See "Ping" on page 10-3 for instructions on how to use the ping utility. If you can successfully ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.farallon.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia Router (use ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN Statistics and LAN Statistics screens to see more specific information on data traffic flow and address serving.
- If you are using MacIP subnetting, make sure Transmit RIP is On (see the IP Options screen).

Internal termination switch

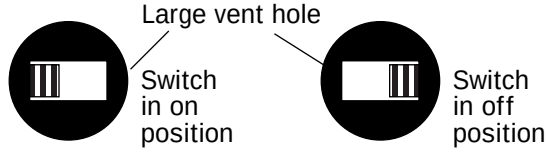
Non-North American models only

The Netopia Router includes an internal termination switch for terminating the S/T bus. The S/T bus is the connection from the Router to the NT1 or wall jack on your ISDN line. The S/T bus must be properly terminated to avoid ISDN communications errors.

The Netopia Router ships with its internal termination switch set to the off position. This means that you should already have S/T bus termination. If you are unsure of whether you have S/T bus termination, contact your ISDN service provider.

If you do not have S/T bus termination, you should set the internal termination switch to the on position.

The switch is located just inside a rear-panel ventilation hole that is visibly larger than the other holes, as shown in the following illustration:



The Netopia Router's opening for accessing the internal termination switch.

Use a pointed object, such as a pen, to carefully reach inside the correct ventilation hole and slide the switch to the left. This is the on position, with termination in effect.

Technical support

Farallon Communications is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Farallon

Look in this guide and in the accompanying *Getting Started* guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting technical support.

Environment profile

- Locate the Netopia Router's model number, product serial number, and firmware version. The serial number is on the bottom side of the Router, along with the model number. The firmware version appears in the Netopia Router's Main Menu screen.

  Model number:_____

  Serial number: _____

  Firmware version: _____

- What kind of local network(s) do you have, with how many devices?

  Ethernet

  LocalTalk

  EtherTalk

  TCP/IP

  IPX

  Other: _____

How to reach us

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact us by telephone, please be ready to supply Farallon Technical Support with the information you used to configure the Netopia Router. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

When you are prepared, contact Farallon Customer Service by e-mail, telephone, fax, or post:

Internet: techsports@farallon.com (for technical support)
info@farallon.com (for general information)

Phone: 1 510-814-5000
Fax: 1 510-814-5023

Farallon Communications, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Farallon Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Farallon World Wide Web server via http://www.farallon.com
Internet via anonymous FTP to ftp.farallon.com/pub
AppleLink (Third Parties A-G)

FAX-Back

This service provides technical notes which answer the most commonly asked questions, and offer solutions for many common problems encountered with Farallon products.

FAX-Back: +1 510-814-5040

Local service

If you are not located in the United States or Canada, you can get service locally by contacting your nearest Farallon reseller or distributor. For a worldwide list of our distributors, see our AppleLink bulletin board or contact Farallon directly.

Appendix B

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia Router and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way, to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts, instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.9.200.3 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations who request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1-127	127	16,777,214	net.host.host.host	97.3.14.250
B	128-191	16,384	65,534	net.net.host.host	140.100.10.11
C	192-223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits, in order to leave room for

the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses, and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation, like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network, when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia Router.

Note: If you receive an IP address from an ISP, there must be a mask associated with that IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

Suppose that your organization has a total of 25 IP hosts situated on three different floors of your office building, and that you are in charge of designing the network that will connect them. You obtain a Class C network number, 199.14.17.0, since you expect that your organization will always have fewer than 254 IP hosts. All your IP hosts will use IP addresses of the form 199.14.17.x, where x represents the eight bits that can be used for subnet numbers and individual host numbers.

How many of the final eight bits of the IP address should you reserve for hosts, and how many should you use for subnet numbers? The answer depends on how many subnets you expect to need, and how many hosts you expect to put on each subnet. All 25 of your hosts could certainly coexist on one network that does not use subnetting. However, you are fortunate enough to have two IP routers on hand, so you decide to lower traffic levels and simplify troubleshooting by setting up three subnets, one for each floor. The following table lists how many subnets and how many hosts you may have for a Class C network, depending on how many bits you allocate to the subnet numbers.

Subnetting options for a Class C IP network			
Subnet mask chosen	Number of bits for subnet number	Number of subnets possible	Number of hosts possible on each subnet
11111111.11111111.11111111.10000000 or 255.255.255.128	1	0	126
11111111.11111111.11111111.11000000 or 255.255.255.192	2	2	62
11111111.11111111.11111111.11100000 or 255.255.255.224	3	6	30
11111111.11111111.11111111.11110000 or 255.255.255.240	4	14	14
11111111.11111111.11111111.11111000 or 255.255.255.248	5	30	6
11111111.11111111.11111111.11111100 or 255.255.255.252	6	62	2
11111111.11111111.11111111.11111110 or 255.255.255.254	7	126	0
11111111.11111111.11111111.11111111 or 255.255.255.255	8	254	0

As you can see, subnet masks that allocate one, seven, or eight bits to subnets are useless for a Class C network. This is because binary host addresses or subnet addresses that are composed of all zeros or all ones are reserved for broadcasting (see "Broadcasts" on page B-16). Class A or Class B networks, on the other hand, would still have many host numbers available if the network manager chose a subnet mask that allocated seven or eight bits to subnets.

1. Decide on a subnet strategy

Your 25 IP hosts are arranged as follows: 10 on the third floor, eight on the fourth floor, and seven on the fifth floor. Since you will need at least ten host addresses per subnet, the preceding table indicates that you must choose a subnet mask that allocates four or fewer bits to the subnet address. You decide to use a subnet mask

that allocates five bits to the host address and three to the subnet address. This gives you a potential of six subnets of 30 machines each.

2. Determine the subnet mask

You can find the subnet mask associated with your subnetting choice in the table above. IP does not specify which bits are to be used for the subnet numbers and which for the host numbers, but it is conventional to use the left-most bits for the subnet numbers. This allows you to use an unbroken series of host numbers on each subnet, although there will be big gaps between your subnet numbers.

Now you can calculate the legal range of host numbers you can use on each of your subnets, the legal subnet numbers you can use, and the combined totals to use when setting up each host with its own IP address.

3. Find the actual host numbers

First, determine which host numbers are legal. In this example, host numbers are five bits long, meaning that values can range from 00000 to 11111 in binary notation. Remember that 00000 and 11111 are reserved for broadcasts. Actual host numbers, therefore, would be 00001 through 11110 in binary notation, or 1 through 30 in decimal notation.

4. Find the actual subnet numbers

Next, determine which subnet numbers are legal. In this example, the subnet numbers could be any eight bits that meet two constraints. The first constraint is that the five least significant digits must be zero, as these bits are allocated to the host number and cannot be used in the subnet number. The second constraint is that the three most significant bits must not be all zeros or all ones, as these values are reserved for broadcasting. So the legal subnet numbers are 00100000, 01000000, 01100000, 10000000, 10100000, and 11000000. When translated into decimal notation, these possible subnet numbers are 32, 64, 96, 128, 160, and 192. You decide to use 32, 64, and 96 as the subnet numbers for your three subnets: 32 for the third floor, 64 for the fourth floor, and 96 for the fifth floor.

5. Determine the host addresses

Finally, combine your subnet numbers with your host numbers to determine the actual IP addresses you may use for your 25 hosts. The first three bytes of the address will always be 199.14.17, as assigned to you by InterNIC. The final byte will be the sum of the subnet number and the host number. The following table shows the ranges of IP addresses you can choose from when you configure each host.

Subnet location	Subnet number	Smallest host number	Largest host number	Smallest combined total	Largest combined total	IP address range
3rd floor	32	1	30	33	62	199.14.17.33 to 199.14.17.62
4th floor	64	1	30	65	94	199.14.17.65 to 199.14.17.94
5th floor	96	1	30	97	126	199.14.17.97 to 199.14.17.126

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don't need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you may obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP's network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you

must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages to this situation is the greater ease and lower cost of obtaining a subnet from an ISP rather than a full Class C address.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia Router, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia Router automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia Router. Using the Router in this way allows it to function as an address server.

One reason to use the Netopia Router as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You only need to enter information once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia Router as an address server is that it will only distribute addresses to hosts that need to use them. If there is a shortage of addresses, the address server will automatically take an address away from a host that has stopped using it and give it to a host that is requesting one. If you do not possess enough addresses for every host on your network to have one at all times, using address serving to distribute them is one solution. However, this is not an efficient solution because a host without an IP address will be forced to wait until a host with one is turned off or gives up its IP address for some other reason.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. A network administrator's computer, a computer dedicated to communicating with the Internet, and routers are appropriate candidates for a static address.

Using address serving

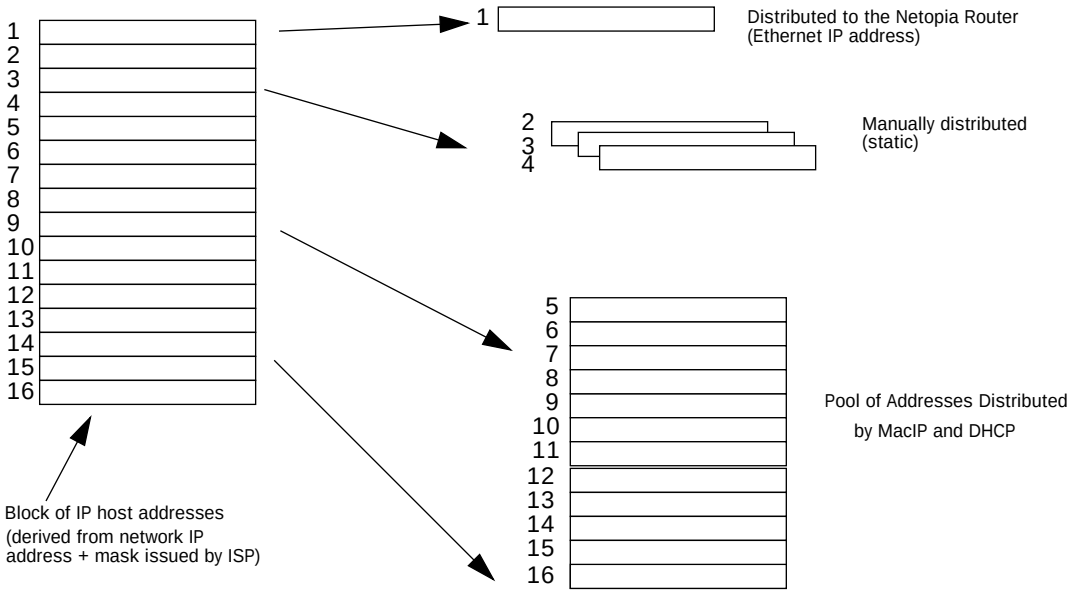
The Netopia Router provides two ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. MacIP is provided with the Netopia Internet Software Starter Kit.

The Netopia Router can use both DHCP and MacIP. Whether you use one or both will depend on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you will need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.

- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

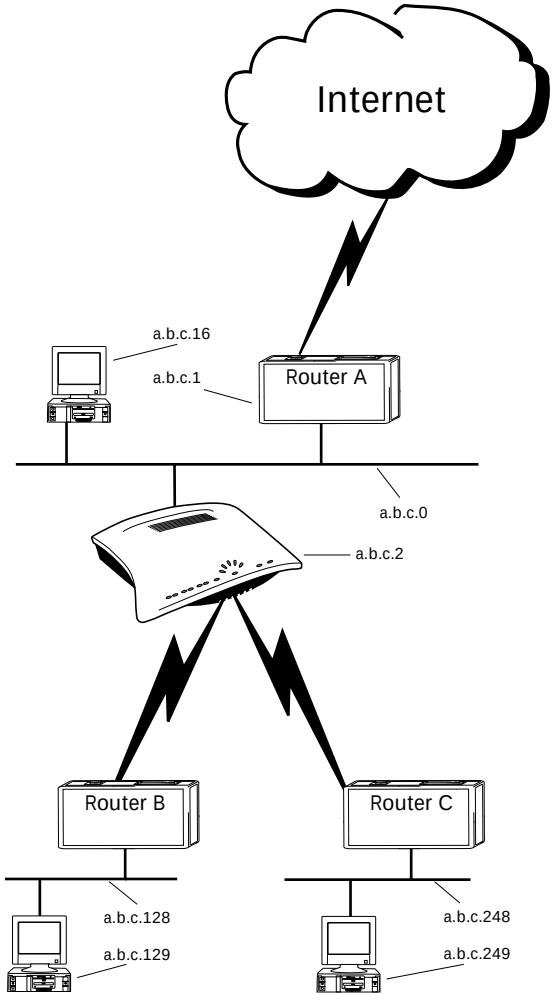
The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BOOTP, MacIP, and WAN clients, even though BOOTP and static MacIP clients might not be considered served.

- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32, and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter "10" in the DHCP Setup screen's Number of Addresses to Allocate item. Then, in the same screen's First Address item, enter the first address in the sub-block to allocate such that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).



Nested IP subnets

Under certain situations, you may wish to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses avaiilable to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia Router), a Netopia Router, and a number of other hosts. Router A maintains a link to the Internet, and may be used as the default gateway.

Routers B and C (which could also be Netopia Routers) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia Router with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
for Router B	a.b.c.128	255.255.255.192	7
for Router C	a.b.c.248	255.255.255.248	3

The Netopia Router's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

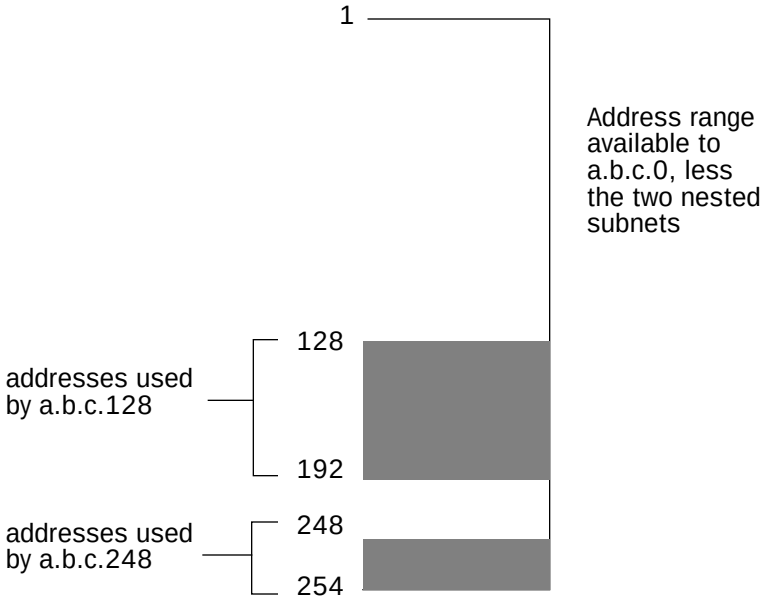
```
                          IP Routing Table

 Network Address-Subnet Mask-----via
Router------Port--Age--------Type------
 ---------------------------------SCROLL
UP-------------------------------
 0.0.0.0         0.0.0.0           a.b.c.1      WAN   3719
Management
 127.0.0.1       255.255.255.255   127.0.0.1    lp1   6423       Local
 a.b.c.128       255.255.255.192   a.b.c.128    WAN   5157       Local
 a.b.c.248       255.255.255.248   a.b.c.248    WAN   6205       Local




--------------------------------SCROLL
DOWN-------------------------------
 UPDATE
```

Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia Router, which examines its destination IP address.

The Netopia Router compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia Router uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network, if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork, if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. When you install and configure the Netopia Router to be an AppleTalk–IP gateway, you must specify whether it should use Ethernet or 802.3. If you do not know which to use, see the documentation provided with your IP computers, or talk with your IP network manager or the vendor of your IP equipment. By default, the Netopia Router uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

Appendix C

ISDN Configuration Guide

This appendix contains supplemental ISDN configuration information.

Definitions

The following terms are used in this appendix:

Directory number: The actual phone number associated with the ISDN line you order. Depending on the type of switch protocol used on your line, there may be one directory number for both B-channels, or one for each B-channel.

SPID: The Service Profile ID generally looks like the directory number with some extra digits (the TID) appended to it. SPIDs are used only in North America. The number of SPIDs received from your ISDN service provider can vary from none to two.

TID (Terminal ID): This one- or two-digit number is associated with the SPID. It's usually 1 or 01 for the first SPID and 2 or 02 for the second SPID, but it can vary in form. You may need to add a TID to each SPID you use when you configure the Netopia Router.

If you encounter other unfamiliar terms, check the glossary.

About SPIDs

Depending on the type of ISDN switch protocol you use, you may be required to enter SPIDs in the ISDN Line Configuration screen. Generally, SPIDs are used with North American (United States and Canada) switch protocols.

The exact format of ISDN SPIDs is sometimes a point of confusion. This is because several formats exist, and some formats allow variations.

The table below displays the general SPID formats for the types of North American ISDN switch protocols supported by the Netopia Router. The formats shown are a subset of possible SPID formats, but in most cases they should work.

In the following table, xxxxxxx represents the directory number assigned to your ISDN line, and yyy represents your area code.

Switch	SPID format
AT&T 5ESS custom (multipoint)	01xxxxxxx0
Northern Telecom DMS-100 custom	yyyxxxxxxx1 and yyyxxxxxxx2 or yyyxxxxxxx01 and yyyxxxxxxx02
National ISDN-1 on AT&T 5ESS (multipoint)	01xxxxxxx000
National ISDN-1 on Northern Telecom DMS-100	yyyxxxxxxx100 and yyyxxxxxxx200 or yyyxxxxxxx0100 and yyyxxxxxxx0101

Note: AT&T 5ESS custom point-to-point switches have no SPIDs and are not represented in the table above. However, this type of switch configuration is supported by the Netopia Router.

Example SPIDs

If your ISDN line is controlled by a DMS-100 switch using National ISDN-1, and your directory numbers are given as (415)234-5678 and (415)234-5679, your SPIDs are 4152345678010 and 4152345679020. Alternately, your SPIDs can be 41523456780100 and 41523456790200.

Second directory number

The Add Connection Profile screen in the WAN Setup (Advanced Configuration) now contains the item Optional Second Number. This item should be filled in when the remote network (the network router being called) has a separate directory number for each B-channel.

Switch-specific uses

In general, if the remote network has an ISDN line with an AT&T 5ESS® switch, only one directory number is needed. However, the remote network may be set up to require incoming calls to use separate directory numbers for each B-channel. In this case, enter the second directory number in the Optional Second Number item.

If the remote network has an ISDN line with a DMS-100 switch and is not in a hunt group, it should have one directory number for each B-channel. Both directory numbers are required by the Netopia Router to make a connection to that network using two B-channels. In this case, enter the second directory number in the Optional Second Number item. If only one directory number is available in this case, only one B-channel can be used when connecting to that network.

Backup number

Another use for the Optional Second Number item is for storing a backup number in case a connection cannot be made using the primary number. For example, if calling the primary number returns a busy signal, the Netopia Router will attempt to use the secondary number stored in Optional Second Number. If a connection also cannot be made using the secondary number, see the event history to determine the problem and its solution. See Appendix E, "Leased line and ISDN Events", for more information.

If the remote network's directory number is part of a hunt group, a second directory number may not be necessary to make a successful connection using two B-channels.

Dynamic B-channel usage

If the B-Channel Usage item in a connection profile's PPP/MP Options screen is set to Dynamic or 2 B, Pre-emptible, one or both B channels may be in use at any time during a call made with that connection profile. Use of the second B-channel depends on traffic volume.

In addition, one of the B-channels may be relinquished if there is an incoming call, or if a second outgoing connection is made using another connection profile.

The ability to allow incoming calls when both B-channels are in use depends on the type of switch protocol on the local ISDN line, and how that line is provisioned (configured). Some types of switch protocols never allow incoming calls when both B-channels are in use. Switch protocols that do allow incoming calls must have the additional call offering (ACO) parameter turned on for data. ACO for data is off by default.

The table below shows which supported switch types can allow an incoming call when ACO for data is on.

Type of switch:	Incoming call allowed?
AT&T 5ESS custom	N/A
AT&T 5ESS National ISDN-1	Yes
DMS-100 custom	Yes*
DMS-100 National ISDN-1	Yes*

* Must have two directory numbers assigned.

This table may not be a complete list of switch protocols that support ACO. To find out if your switch protocol supports ACO, or to turn ACO on, contact your ISDN service provider.

Other incoming call restrictions

A B-channel will not be relinquished to admit an incoming call if a connection profile has B-Channel Usage set to 2 B-Channels.

A B-channel will not be relinquished to admit an incoming call when there are two separate concurrent calls. Incoming calls are automatically allowed in when there is at least one B-channel free.

Appendix D

ISDN, DDS/ADN, and T1 Events

This appendix is a complete list of the leased line and ISDN events that can appear in the Netopia Router's event histories. The text that appears in a history is shown in bold, followed by a brief explanation and the parameters associated with the event.

You can display more information about any event simply by selecting it in the Event History and pressing Return. See the example Event History shown below.

```
                          Device Event History
                                        Current Date --   6/4/97 09:23:53 AM
 -Date-----Time-----Event-----------------------------------------------------
 ----------------------------------SCROLL UP-----------------------------------
 06/04/97 08:56:13   AppleTalk initialization complete
 06/04/97 08:56:06   IPX initialization complete
 06/04/97 08:56:06   IP address server initialization complete
 06/04/97 08:56:06 --BOOT: Cold start-----------------------------------------
 06/04/97 08:52:28   AURP initialization complete
 --------------------------------SCROLL DOWN-----------------------------------

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

For example, if you selected a Disconnect Requested event that occurred at 19:43:01 and pressed Return, the following screen would appear:

```
+-----------------------EVENT DETAILS---------------------+
+-----------------------------------------------------------+
|                                                           |
| 19:40:04 on Friday, July 23, 1999                         |
| Disconnect Requested                                      |
| Called #: 914152270188; Cause: 16                         |
|                                                           |
|                                                           |
+-----------------------------------------------------------+
```

Leased line events

WAN data link activated at X Kbps: Indicates leased line is active at the specified speed (X).

WAN data link deactivated: Indicates leased line is not active.

ISDN events

ISDN Port Init: ISDN port has been initialized.

ISDN Line Active: ISDN L1 active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

SPID Initialized: SPID accepted by switch. Associated parameter: directory number associated with SPID.

SPID Failed: SPID rejected/removed by switch. Associated parameter: directory number associated with SPID.

ISDN Line Deactivated: ISDN L1 not active - L1 not ready to carry L2 data. Associated parameter: switch type or protocol.

Received Clear Confirmation for our DN: Received clear confirmation from switch. Associated parameter: called directory number.

Received Clear Ind. from DN: Received clear indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Connection Confirmed to our DN: Received connect confirmation for Connect Request sent to the switch. Associated parameter: called directory number.

Received Connect Ind. for DN: Received connect indication for Call Request sent to the switch. Associated parameter: called directory number.

Received Disc. Ind. from DN: Received disconnect indication from switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

Received Setup Ind. from DN: Received call indication from switch. Associated parameter: called directory number.

Issued Setup Request from our DN: Call request was sent to switch. Associated parameter: called directory number.

Requested Connect to our DN: Connect request for the received call was sent to the switch. Associated parameter: called directory number.

Issued Clear Request for our DN: Clear request was sent to the switch. Associated parameter: called directory number.

Issued Clear Response to DN: Clear response was sent to the switch. Associated parameter: called directory number.

Disconnect Reqested: Disconnect request was sent to switch. Associated parameter: called directory number. Secondary associated parameter: cause code.

ISDN event cause codes

These codes appear as associated (secondary) parameters in some of the ISDN events.

Cause No. 1: unallocated (unassigned number). This cause indicates that the destination requested by the calling user cannot be reached because, although the number is in a valid format, it is not currently assigned (allocated).

Cause No. 2: no route to specified transit network. This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular network, while it does exist, does not serve the equipment that is sending this cause.

This cause is supported on a network-dependent basis.

Cause No. 3: no route to destination. This cause indicates that the called user cannot be reached because the network through which the call has been routed does not serve the destination desired.

This cause is supported on a network-dependent basis.

Cause No. 6: channel unacceptable. This cause indicates that the channel used in this call is not acceptable to the sending entity.

Cause No.7: call awarded and being delivered in an established channel. This cause indicates that the user is receiving an incoming call, which is being connected to a channel already used by that user for similar calls (e.g., packet-mode X.25 virtual calls).

Cause No. 16: normal call clearing. This cause indicates that the call is being cleared because one of the users involved in the call has requested that the call be cleared.

Under normal situations, the source of this cause is not the network.

Cause No. 17: user busy. This cause is used when the called user has indicated the inability to accept another call.

It is noted that the user equipment is compatible with call.

Cause No. 18: no user responding. This cause is used when a user does not respond to a call establishment message with either an alerting or connect indication within the prescribed period of time allocated (defined in Recommendation Q.931 by the expiry of either timer T303 or T310).

Cause No. 19: no answer from user (user alerted). This cause is used when a user has provided an alerting indication but has not provided a connect indication within a prescribed period of time.

This cause is not necessarily generated by Q.931 procedures but may be generated by internal network timers.

Cause No. 21: call rejected. This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible.

Cause No. 22: number changed. This cause is returned to a calling user when the called party number indicated by the calling user is no longer assigned. The new called party number may optionally be included in the diagnostic field. If a network does not support this capability, cause No. 1, unassigned (unallocated) number, shall be used.

Cause No. 26: non-selected user clearing. This cause indicates that the specified user has not been awarded the incoming call.

Cause No. 27: destination out of order. This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term "not functioning correctly" indicates that a signaling message was unable to be delivered to the remote user: e.g., a physical layer or data link layer failure at the remote user, user equipment off-line, etc.

Cause No. 28: invalid number format (address incomplete). This cause indicates that the called user cannot be reached because the called party number is not a valid format or is not complete.

Cause No. 29: facility rejected. This cause is returned when a facility requested by the user cannot be provided by the network.

Cause No. 30: response to STATUS INQUIRY. This cause is included in the STATUS message when the reason for generated the STATUS message was the prior receive of a STATUS INQUIRY message.

Cause No. 31: normal, unspecified. This cause is used to report a normal even only when no other cause in the normal class applies.

Cause No. 34: no circuit/channel available. This cause indicates that there is no appropriate circuit/channel presently available to handle the call.

Cause No. 38: network out of order. This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time: e.g., immediately reattempting the call is not likely to be successful.

Cause No. 41: temporary failure. This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time: e.g., the user may wish to try another call attempt almost immediately.

Cause No. 42: switching equipment congestion. This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Cause No. 43: access information discarded. This cause indicates that the network could not deliver access information to the remote user as requested: i.e., user-to-user information, low layer compatibility, high layer compatibility, or a sub-address as indicated in the diagnostic.

It is noted that the particular type of access information discarded is optionally included in the diagnostic.

Cause No. 44: requested circuit/channel not available. This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.

Cause No. 47: resource unavailable, unspecified. This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.

Cause No 49: Quality of Service not available. This cause is used to report that the requested Quality of Service, as defined in Recommendation X.213, cannot be provided (e.g., throughput or transit delay cannot be supported).

Cause No. 50: requested facility not subscribed. This cause indicates that the requested supplementary service could not be provided by the network because the user has not completed the necessary administrative arrangements with its supporting networks.

Cause No 57: bearer capability not authorized. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause that the user is not authorized to use.

Cause No. 58: bearer capability not presently available. This cause indicates that the user has requested a bearer capability implemented by the equipment that generated this cause which is not available at this time.

Cause No 63: service or option not available, unspecified. This cause is used to report a service or option not available event only when no other cause in the service or option not available class applies.

Cause No. 65: bearer capability not implemented. This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Cause No. 66: channel type not implemented. This cause indicates that the equipment sending this cause does not support the channel type requested.

Cause No. 69: requested facility not implemented. This cause indicates that the equipment sending this cause does not support the requested supplementary service.

Cause No. 70: only restricted digital information bearer capability is available. This cause indicates that a device has requested an unrestricted bearer service but the equipment sending this cause only supports the restricted version of the requested bearer capability.

Cause No. 79: service or option not implemented, unspecified. This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.

Cause No. 81: invalid call reference value. This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.

Cause No. 82: identified channel does not exist. This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.

Cause No. 83: a suspended call exists, but this call identify does not. This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).

Cause No. 84: call identity in use. This cause indicates that the network has received a call suspend request. The call suspend request contained a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.

Cause No. 85: no call suspended. This call indicates that the network has received a call resume request. The call resume request contained a call identity information element that presently does not indicate any suspended call within the domain interfaces over which calls may be resumed.

Cause No. 86: call having the requested call identity has been cleared. This cause indicates that the network has received a call resume request. The call resume request contained a call identity information element that once indicated a suspended call; however, that suspended call was cleared while suspended (either by network timeout or by remote user).

Cause No. 88: incompatible destination. This cause indicates that the equipment sending this cause has received a request to establish a call that has a low layer compatibility, high layer compatibility, or other compatibility attributes (e.g., data rate) that cannot be accommodated.

Cause No. 91: invalid transit network selection. This cause indicates that a transit network identification of an incorrect format as defined in Annex C/Q.931 was received.

Cause No. 95: invalid message, unspecified. This cause is used to report an invalid message event only when no other cause in the invalid message class applies.

Cause No. 96: mandatory information element is missing. This cause indicates that the equipment sending this cause has received a message that is missing an information element that must be present in the message before that message can be processed.

Cause No. 97: message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined but not implemented by the equipment sending this cause.

Cause No. 98: message not compatible with call state or message type non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message such that the procedures do not indicate that this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.

Cause No. 99: information element non-existent or not implemented. This cause indicates that the equipment sending this cause has received a message that includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause No. 100: invalid information element contents. This cause indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more of the fields in the information element are coded in a way that has not been implemented by the equipment sending this cause.

Cause No 101: message not compatible with call state. This cause indicates that a message has been received that is incompatible with the call state.

Cause No. 102: recovery on timer expiry. This cause indicates that a procedure has been initiated by the expiry of a timer in association with Q.931 error handling procedures.

Cause No. 111: protocol error, unspecified. This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Cause No. 127: interworking, unspecified. This cause indicates there has been interworking with a network that does not provide causes for actions it takes; thus, the precise cause for a message being sent cannot be ascertained.

Appendix E

Further Reading

Angell, David. *ISDN for Dummies*, Foster City, CA: IDG Books Worldwide, 1995. Thorough introduction to ISDN for beginners.

Black, Uyless. *Emerging Communications Technologies*, Englewood Cliffs, New Jersey: PTR Prentice Hall, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay operate and where they fit in a computer/communications network.

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*, Sebastopol, CA: O'Reilly & Associates, 1995. Dense and technical, but Chapter 6 provides a basic introduction to packet filtering.

Chapman, D. Brent. "Network (In)Security Through IP Packet Filtering," paper available from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041

Garfinkel, Simson. *PGP: Pretty Good Privacy*, Sebastopol, CA: O'Reilly & Associates, 1991. A guide to the free data encryption program PGP and the issues surrounding encryption.

Levine, John R. and Carol Baroudi. *The Internet for Dummies*, Foster City, CA: IDG Books Worldwide, 1993. Covers all of the most popular Internet services, including e-mail, newsgroups, and the World Wide Web. Also has information on setting up individual workstations with TCP/IP stacks.

Miller, A. Mark. *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)*, M&T Books: A Division of MIS: Press, 1994. An intermediate/advanced reference on Frame Relay technologies.

Siyan, Karanjit. *Internet Firewall and Network Security*, Indianapolis: New Riders Publishing, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip. *Frame Relay Principles and Applications*, Addison-Wesley Publishing Company, 1996. Covers information on Frame Relay, including the pros and cons of the technology, description of the theory and application, and an explanation of the standardization process.

Glossary

Access Line: A communications line (e.g. circuit) interconnecting a frame-relay-compatible device (DTE) to a frame-relay switch (DCE). See also *Trunk Line*.

Access Rate (AR): The data rate of the user access channel. The speed of the access channel determines how rapidly (maximum rate) the end user can inject data into a frame relay network.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *Comite Consultatif International Telegraphique et Telephonique (CCITT*).

AppleTalk: A comprehensive network system designed and developed by Apple Computer, Inc. AppleTalk allows many different types of computer systems, printers, and servers to communicate on a variety of cabling schemes, including LocalTalk and Ethernet cabling. In this manual, AppleTalk refers especially to the protocols or rule sets that govern this communication.

AppleTalk address: A unique identifier for each device using AppleTalk that allows information to be sent and received correctly. An AppleTalk address always includes a network number wherever two or more AppleTalk networks are connected together by routers.

AUI (Attachment Unit Interface): Usually refers to 15-pin D connectors associated with Ethernet transceivers.

AURP (Apple Update-based Router Protocol): An enhanced AppleTalk routing protocol. AURP provides improved support for AppleTalk over wide area networks (WANs) and tunneling through non-AppleTalk (IP) networks. AURP features include network number remapping, clustering of remote network numbers, and hop count reduction.

backbone: A network topology consisting of a single length of cable with multiple network connection points.

Bandwidth: The range of frequencies, expressed in Kilobits per second, that can pass over a given data transmission channel within a frame relay network. The bandwidth determines the rate at which information can be sent through a channel - the greater the bandwidth, the more information that can be sent in a given amount of time.

baud rate: The rate of the signaling speed of a transmission medium.

Be (Excess Burst Size): The maximum amount of uncommitted data (in bits) in excess of Bc that a frame relay network can attempt to deliver during a time interval Tc. This data (Be) generally is delivered with a lower probability than Bc. The network treats Be data as discard eligible. See also *Committed Burst Size* (*Bc*).

BECN (Backward Explicit Congestion Notification): A bit set by a frame relay network to notify an interface device (DTE) that congestion avoidance procedures should be initiated by the sending device.

bit: A binary digit; the smallest unit of data in the binary counting system. A bit has a value of either 0 or 1.

bits per second (bps): A measure of the actual data transmission rate. The bps rate may be equal to or greater than the baud rate depending on the modulation technique used to encode bits into each baud interval. The correct term to use when describing modem data transfer speeds.

bps: See *bits per second*.

branch: A length of cable in a star network that goes from the center of the star to a wall jack.

Bridge: A device that supports LAN-to-LAN communications. Bridges may be equipped to provide frame relay support to the LAN devices they serve. A frame-relay-capable bridge encapsulates LAN frames in frame relay frames and feeds those frame relay frames to a frame relay switch for transmission across the network. A frame-relay-capable bridge also receives frame relay frames from the network, strips the frame relay frame off each LAN frame, and passes the LAN frame on to the end device. Bridges are generally used to connect local area network (LAN) segments to other LAN segments or to a wide area network (WAN). They route traffic on the Level 2 LAN protocol (e.g., the Media Access Control address), which occupies the lower sub layer of the LAN OSI data link layer. See also Router.

broadcast: A network transaction that sends data to all hosts connected to the network.

Burstiness: In the context of a frame relay network, data that uses bandwidth only sporadically; that is, information that does not use the total bandwidth of a circuit 100 percent of the time. During pauses, channels are idle; and no traffic flows across them in either direction. Interactive and LAN-to-LAN data is bursty in nature, because it is sent intermittantly, and in between data transmission the channel experiences idle time waiting for the DTEs to respond to the transmitted data user's input of waiting for the user to send more data.

byte: A group of bits, normally eight, which represent one data character.

CallerID: See *CND.*

CCITT (Comite Consultatif International Telegraphique et Telephonique): International Consultative Committee for Telegraphy and Telephony, a standards organization that devises and proposes recommendations for international communications. See also *ANSI (American National Standards Institute)*.

Channel: Generically refers to the user access channel across which frame relay data travels. Within a given T1 or E1 physical line, a channel can be one of the following, depending on how the line is configured.

Unchannelized

The entire T1/E1 line is considered a channel, where:

- The T1 line operates at speeds of 1.536 Mbps and is a signle channel consisting of 24 T1 time slots.
- The E1 line operates at speeds of 1.984 Mbps and is a single channel consisting of 20 E1 time slots.

Channelized

The channel is any one of N time slots within a given line, where:

- The T1 line consists of any one or more channels. Each channel is any one of 24 time slots. The T1 line operates at speeds in multiples of multiples of 56/64 Kbps to 1.536 Mbps, with aggregate speed not exceeding 1.536 Mbps.
- The E1 line consists of one or more channels. Each channel is any one of 31 time slots. The E1 line operates at speeds in multiples of 64 Kbps to 1.984 Mbps, with aggregate speed not exceeding 1.984 Mbps.

Fractional

The T1/E1 channel is one of the following groupings of consecutively or nonconsecutively assigned time slots:

- N T/1 time slots (NX56/64Kbps where N=1 to 23 T1 time slots per Ft1 channel).
- N E1 time slots (NX64Kbps, where N = 1 to 30 time slots per E1 channel).

Channel Service Unit (CSU): An ancillary device needed to adapt the V.35 interface on a Frame Relay DTE to the T1 (or E1) interface on a frame relay switch. The T1 (or E1) signal format on the frame relay switch is not compatible with the V.35 interface on the DTE: therefore, a CSU or similar device, placed between the DTE and the frame relay switch, is needed to perform the required conversion.

CHAP (challenge handshake protocol): A method for ensuring secure network access and communications.

Class A, B, and C networks: The values assigned to the first few bits in an IP network address determine which class designation the network has. In decimal notation, Class A network addresses range from 1.X.X.X to 126.X.X.X, Class B network addresses range from 128.1.X.X to 191.254.X.X, and Class C addresses range from 192.0.1.X to 223.255.254.X. For more information on IP network address classes, see *Appendix C, "Understanding IP Addressing."*

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

clustering: A feature that clusters remapped network numbers into a range of sequential network numbers.

CNA (Calling Number Authentication): A security feature that will reject an incoming call if it does not match the Calling Number field in one of the Netopia ISDN Router's Connection Profiles.

CND (Calling Number Delivery): Also known as caller ID, a feature that allows the Called Customer Premises Equipment (CPE) to receive a calling party's directory number during the call establishment phase.

Committed Burst Size (Bc): The maximum amount of data (in bits) that the network agrees to transfer, under normal conditions, during a time interval Tc. See also *Excess Burst Size (Be)*.

Committed Information Rate (CIR): The committed rate (in bits per second) at which the ingress access interface trunk interfaces, and egress access interface of a frame relay network transfer information to the destination frame relay end system under normal conditions. The rate is averaged over a minimum time interval Tc.

Committed Rate Measurement Interval (Tc): The time interval during which the user can send only a Bc-committed amount of the traffic. Tc is computed (from the subscription parameters of CIR and Bc) as Tc = Bc/CIR. Tc is not a periodic time interval. Instead, it is used only to measure incoming data, during which it acts like a sliding window. Incoming data triggers the Tc interval, which continues until it completes its commuted duration. See also *Committed Information Rate (CIR)* and *Committed Burst Size (Bc)*.

community strings: Sequences of characters that serve much like passwords for devices using SNMP. Different community strings may be used to allow an SNMP user to gather device information or change device configurations.

CRC (Cyclic Redundancy Check): A computational means to ensure the accuracy of frames transmitted between devices in a frame relay network. The mathematical function is computed, before the frame is transmitted at the originating device. Its numerical value is computed based on the content of the frame. This value is compared with a recomputed value of the function at the destination device. See also *FCS (Frame Check Sequence)*.

CSV (Circuit Switched Voice): Also know as Data-Over-Voice, a feature that allows data calls to be placed or answered using ISDN speech grade bearer capabilities.

DCE (Data Communications Equipment): Term defined by both frame relay and X.25 committees, that applies to switching equipment and is distinquished from the devices that attach to the network (DTE). Also see *DTE*.

DDP (Datagram Delivery Protocol): Defines socket-to-socket delivery of datagrams over an AppleTalk internet.

DE (Discard Eligibility): A user-set bit indicating that a frame may be discarded in preference to other frames if congestion occurs, to maintain the committed quality of service within the network. Frames with the DE bit set are considered Be excess data. See also *Excess burst Size (Be)*.

DTE (Data Terminal Equipment): Term defined by both frame relay and X.25 committees that applies to switching equipment and is distinguished from the devices that attach to the DCE because pins 2 and 3 are reversed. Also see *DCE*.

default zone: When a Phase II EtherTalk network includes more than one zone, all routers on that network must be configured to assign one of these zones as a default zone. The default zone is temporarily assigned to any Phase II EtherTalk node that hasn't chosen a zone. The user may choose another zone by opening the Network Control Panel, selecting the correct physical connection, and then choosing a zone in the scrolling field displayed.

DHCP (Dynamic Host Configuration Protocol): A service that lets clients on a LAN request configuration information, such as IP host addresses, from a server.

DLCI (Data Link Control Identifier): A unique number assigned to a PVC end point in a frame relay network. Identifies a particular PVC endpoint within a user's access channel in a frame relay network.

DNS (Domain Name Service): A TCP/IP protocol for discovering and maintaining network resource information distributed among different servers.

download: The process of transferring a file from a server to a client.

E1: Transmission rate of 2.048 Mbps on E1 communications lines. An E1 facility carries a 2.048 Mbps digital signal. See also *T1* and *channel*.

Egress: Frame Relay frames leaving a frame relay network in the direction toward the destination device. Contrast with Ingress.

Encapsulation: A process by which an interface device places an end devices protocol-specific frames inside a frame relay frame. The network accepts only frames formatted specifically for frame relay; hence, interface devices acting as interfaces to a frame relay network must perform encapsulation. See also *Interface device* or *Frame-Relay-Capable Interface Device*.

End-Device: The ultimate source or destination of data flowing through a frame relay network sometime referred to as a Data Terminal Equipment (DTE). As a source device, it sends data to an interface device for encapsulation in a frame relay frame. As a destination device, it receives de-encapsulated data (i.e., the frame relay frame is stripped off, leaving only the user's data) from the interface device. Also see DCE. NOTE: An end device can be an application program or some operator-controlled device (e.g., workstation). In a LAN environment, the end device could be a file server or host.

Ethernet: A networking protocol that defines a type of LAN characterized by a 10 Mbps (megabits per second) data rate. Ethernet is used in many mainframe, PC, and UNIX networks, as well as for EtherTalk.

Ethernet address: Sometimes referred to as a hardware address. A 48-bits long number assigned to every Ethernet hardware device. Ethernet addresses are usually expressed as 12-character hexadecimal numbers, where each hexadecimal character (0 through F) represents four binary bits. Do not confuse the Ethernet address of a device with its network address.

EtherTalk: Apple's data-link software that allows an AppleTalk network to be connected by Ethernet cables. EtherTalk is a protocol within the AppleTalk protocol set. Two versions of EtherTalk are in common use, designated as Phase I and Phase II EtherTalk.

extended network: A network using AppleTalk Phase II protocols; EtherTalk 2.0 and TokenTalk are extended networks. LocalTalk networks are compatible with Phase II but are not extended because a single LocalTalk network cannot have multiple network numbers or multiple zone names.

FCS (Frame Check Sequence): The standard 16-bit cyclic redundancy check used for HDLC and frame relay frames. The FCS detects bit errors occurring in the bits of the frame between the opening flag and the FCS, and is only effective in detecting errors in frames no larger than 4096 octets. See also *CRC (Cyclic Redundancy Check*.

FECN (Forward Explicit Congestion Notification): A bit set by a frame relay network to notify an interface device (DTE) that congestion avoidance procedures should be initiated by the receiving device. See also *BECN*.

Filer Server: In the context of a frame relay network supporting LAN-to-LAN communications, a device connecting a series of workstations within a given LAN. The device performs error recovery and flow control functions as well as end-to-end acknowledgement of data during data transfer, thereby significantly reducing overhead within the frame relay network.

firmware: System software stored in a device's memory that controls the device. The Netopia ISDN Router's firmware can be updated.

Frame-Relay-Capable Interface Device: A communications device that performs encapsulation. frame-Relay-capable reouters and bridges are examples of interface devices used to interface the customer's equipment to a frame relay network. See also *Inteface Device and Encapsulation*.

Frame Relay Frame: A variable-length unit of data, in frame-relay format that is transmitted through a frame relay network as pure data. Contrast with Packet. See also *Q.922A*.

Frame Relay Network: A telecommunications network based on frame relay technology. Data is multiplexed. In contrast with a Packet-Switching Network.

gateway: A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

hard seeding: A router setting. In hard seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information and the information provided by another router, it disables the router port for which there is a conflict. See also *non-seeding, seeding*, *seed router,* and *soft seeding*.

HDLC (High Level Data Link Control): A generic link-level communications protocol developed by the International Organization for Standardization (ISO). HDLC manages synchronous, code-transparent, serial information transfer over a link connection. See also *SDLC (Synchronous Data Link Control).*

header: In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

hop: A single trunk line between two switches in a frame relay network. An established PVC consists of a certain number of hops, spanning the distance from the ingress access interface to the egress access interface within the network.

hop count: The number of routers a packet has gone through. If there are six routers between source and destination nodes, the hop count for the packet will be six when it arrives at its destination node. The maximum allowable hop count is usually 15.

hop count reduction: A feature of AURP supported by the Netopia ISDN Router. Tunnels and point-to-point links over WANs can often exceed the maximum allowable hop count of 15 routers. Network administrators can use the hop count reduction feature to set up tunnels and point-to-point links that exceed the 15-router limit.

host: A single, addressable device on a network. Computers, networked printers, and routers are hosts.

Host Computer: A communications device that enables users to run applications programs to perform such functions as text editing, program execution, access to data bases, etc.

Ingress: Frame Relay frames from an access device toward the frame relay network. Contrast with Egress.

Interface Device: Provides the interface between the end device(s) and a frame relay network by encapsulating the user's native protocol in frame relay frames and sending the frames across the frame relay backbone. See also *Encapsulation* and *Frame-Relay-Capable Interface Device*.

internet: A set of networks connected together by routers. This is a general term, not to be confused with the large, multi-organizational collection of IP networks known as the Internet. An internet is sometimes also known as an internetwork.

internet address, IP address: Any computing device that uses the Internet Protocol (IP) must be assigned an internet or IP address. This is a 32-bit number assigned by the system administrator, usually written in the form of 4 decimal fields separated by periods, e.g., 192.9.200.1. Part of the internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address. See also *Class A, B, and C networks*.

IP (Internet Protocol): A networking protocol developed for use on computer systems that use the UNIX operating system. Often used with Ethernet cabling systems. In this manual, IP is used as an umbrella term to cover all packets and networking operations that include the use of the Internet Protocol. See also *TCP/IP*.

IP address, IP host address, IP network address: See *internet address*.

IP broadcast: See *broadcast*.

IP tunneling: See *AURP*.

IPX (Internet Package Exchange): A protocol used by Novell Netware networks.

ISDN (Integrated Services Digital Network): A method of transmitting data digitally over telephone lines.

ISP (Internet service provider): A company that provides Internet-related services. Most importantly, an ISP provides Internet access services and products to other companies and consumers.

LAPB (Link Access Procedure Balanced): The balanced-mode, enhanced version of HDLC. Used in X.25 packet-switching networks. Contrast with LAPD.

LAPD (Link Access Procedure on the D-channel: A protocol that operates at the data link layer (layer 2) of the OSI architecture. LAPD is used to convey information between layer 3 entities across the frame relay network. The D-channel carries signaling information for circuit switching. Contrast with LAPB.

LAN (Local Area Network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

LAN Protocols: A range of LAN protocols supported by a frame relay network, including Transmission Control Protocol/Internet Protocol (TCP/IP), AppleTalk, Xerox Network System (XNS), Internetwork Packet Exchange (IPX), and Common Operating System used by DOS-based PCs.

LAN Segment: In the context of a frame relay network supporting LAN-to-LAN communications, a LAN linked to another LAN by a bridge. Bridges enable two LANs to function like a single, large LAN by passing data from one LAN segment to another. To communicate with each other, the bridged LAN segments must use the same native protocol. See also *Bridge*.

LocalTalk: The cabling specification for AppleTalk running at a speed of 230.4 kbps (kilobits per second).

MacIP: A protocol in which IP packets are encapsulated within AppleTalk headers, for transmission over AppleTalk networks. MacIP requires the presence of at least one AppleTalk–IP gateway. MacIP is usually used to allow an AppleTalk computer to communicate with an IP computer.

MacIP client: A Macintosh computer that is using the MacIP protocol to communicate with an IP computer.

MIB (Management Information Base): A standardized structure for SNMP management information.

modem: A device used to convert digital signals from a computer into analog signals that can be transmitted across standard analog (not ISDN) telephone lines. Modem is a contraction of modulator-demodulator.

NAT (Network Address Translation): A feature that allows communication between the LAN connected to the Netopia ISDN Router and the Internet using a single IP address, instead of having a separate IP address for each computer on the network.

NetBIOS: A network communications protocol used on PC LANs.

network: A group of computer systems and other computer devices that communicate with one another.

network administrator: A person who coordinates the design, installation, and management of a network. A network administrator is also responsible for troubleshooting and for adding new users to the network.

network log: A record of the names of devices, location of wire pairs, wall-jack numbers, and other information about the network.

network number: A unique number for each network in an internet. AppleTalk network numbers are assigned by seed routers, to which the network is directly connected. An isolated AppleTalk network does not need a network number.

network number remapping: Resolves network number conflicts when two or more AppleTalk networks that may have duplicate network numbers are connected together. The Netopia ISDN Router lets you set up a range of network numbers into which remote AppleTalk network numbers are remapped.

network range: A unique set of contiguous numbers associated with an extended network; each number in a network range can be associated with up to 253 node addresses.

node: See *host*.

non-seeding: A router setting that causes it to request network number and zone information from any other routers on the network connected to the non-seeding port. If it receives this information, it begins to route packets through that port. See also *hard seeding, seeding*, *seed router,* and *soft seeding*.

NT1: Local ISDN equipment that terminates an ISDN line. In most countries, the NT1 is built into the ISDN wall jack. In the United States and Canada, users must provide the NT1. See also *S/T interface*, *U interface*.

packet: A group of fixed-length binary digits, including the data and call control signals, that are transmitted through an X.25 packet-switching network as a composite whole. The data, call control signals, and possible error control information are arranged in a predetermined format. Packets do not always travel the same pathway but are arranged in proper sequence at the destination side before forwarding the complete message to an addressee. Contrast with Frame Relay Frame.

Packet-Switching Network: A telecommunications network based on packet-switching technology, wherein a transmission channel is occupied only for the duration of the transmission of the packet. Contrast with Frame Relay Network.

PAP (PPP authentication protocol): A method for ensuring secure network access.

Parameter: A numerical code that controls an aspect of terminal and/or network operation. Parameters control such aspects as page size, data transmission speed, and timing options.

PC Card: A removable device, such as a modem or network interface card, approximately the size of a credit card. Designed to fit into a PC Card slot. Formerly called a PCMCIA card. See *PC Card slot*.

PC Card slot: The slot designed to hold PC Cards. Formerly called a PCMCIA slot. The Netopia ISDN Router has a PC Card port with two PC Card slots.

PCMCIA: See *PC Card*.

PVC (Permanent Virtual Circuit): A frame relay logical link, whose endpoints and class of service are defined by network management. Analogous to an X.25 permanent virtual circuit, a PVC consists of the originating frame relay network element address, originating data link control identifier, terminating frame relay network element address, and termination data link control identifier. Originating refers to the access interface from which the PVC is initiated. Terminating refers to the access interface at which the PVC stops. Many data network customers require a PVC between two points. Data terminating equipment with a need for continuous communications use PVCs. See also *DLCI (Data Link Connection Identifier*.

port: A location for passing data in and out of a device, and, in some cases, for attaching other devices or cables.

port number: A number that identifies a TCP/IP-based service. Telnet, for example, is identified with TCP port 23.

POTS (Plain Old Telephone Service): A service that connects analog devices such as telephones, facsimile machines, or modems to the Netopia ISDN Router and communicate over the ISDN line.

PPP (Point to Point Protocol): A protocol for framing IP packets and transmitting them over a serial line.

protocol: A set of rules for communication, sometimes made up of several smaller sets of rules also called protocols. AppleTalk is a protocol that includes the LocalTalk, EtherTalk, and TokenTalk protocols.

Q.922 A (Q.922 Annex A): The international draft standard that defines the structure of frame relay frames. Based on the Q.922A frame format developed by the CCITT. All frame relay frames entering a frame relay network automatically confiorm to this structure. Contrast with LAPB (Link Access Procedure Balanced).

Q.922 A Frame: A variable-length unit of data, formatted in frame-relay (Q.922A) format, that is transmitted through a frame relay network as pure data (i.e., it contains no flow control information). Contrast with Packet. See also *Frame Relay Frame*.

remapping: See *network number remapping*.

RFC (Request for Comment): A series of documents used to exchange information and standards about the Internet.

RIP (Routing Information Protocol): A protocol used for the transmission of IP routing information.

RJ-11: A telephone-industry standard connector type, usually containing four pins.

RJ-45: A telephone-industry standard connector type usually containing eight pins.

router: A device that supports LAN-to-LAN communications. A router can connect identical network types, such as LocalTalk-to-LocalTalk, or dissimilar network types, such as LocalTalk-to-Ethernet. However—unless a gateway is available—a common protocol, such as AppleTalk, must be used over both networks. Routers may be equipped to provide frame relay or ISDN line support to the LAN devices they serve. A frame-relay-capable router encapsulates LAN frames in frame relay frames and feeds those frames to a frame relay switch for transmission across the network. See also *Bridge* and *gateway*.

router port: A physical or logical connection between a router and a network. Where a network only allows the use of one protocol, each physical connection corresponds to one logical router port. An example is the Netopia ISDN Router's LocalTalk port. Where a network allows the use of several protocols, each physical connection may correspond to several logical router ports—one for each protocol used. Each router port has its own network address.

routing table: A list of networks maintained by each router on an internet. Information in the routing table helps the router determine the next router to forward packets to.

seeding: A method for ensuring that two or more routers agree about which physical networks correspond to which network numbers and zone names. There are three options: non-seeding, soft seeding, and hard seeding. Seeding can often be set separately for each router port. See also *hard seeding*, *non-seeding, seed router,* and *soft seeding*.

seed router: A router that provides network number and zone information to any router that starts up on the same network. See also *hard seeding*, *non-seeding, seeding,* and *soft seeding*.

serial port: A connector on the back of the workstation through which data flows to and from a serial device.

server: A device or system that has been specifically configured to provide a service, usually to a group of clients.

SNMP (Simple Network Management Protocol): A protocol used for communication between management consoles and network devices. The Netopia ISDN Router can be managed through SNMP.

soft seeding: A router setting. In soft seeding, if a router that has just been reset detects a network number or zone name conflict between its configured information for a particular port and the information provided by another router connected to that port, it updates its configuration using the information provided by the other router. See also *hard seeding*, *non-seeding, seeding,* and *seed router*.

Statistical Multiplexing: Interleaving the data input of two or more devices on a single channel or access line for transmission through a frame relay network. Interleaving of data is accomplished using the DLCI.

S/T interface: The interface on local ISDN equipment where the connection to an NT1 or a properly terminated ISDN line is made. The Netopia ISDN Router models 440-S/T and 430-S/T have S/T interfaces. See also *NT1*, *U interface*.

subnet: A network address created by using a subnet mask to specify that a number of bits in an internet address will be used as a subnet number rather than a host address.

subnet mask: A 32-bit number to specify which part of an internet address is the network number, and which part is the host address. When written in binary notation, each bit written as 1 corresponds to 1 bit of network address information. One subnet mask applies to all IP devices on an individual IP network.

SDLC (Synchronous Data Link Control): A link-level communications protocol used in an International Business Machines (IBM) Systems Network Architecture (SNA) network that manages synchronous, code-transparent, serial information transfer over a link connection. SDLC is a subset of the more generic HDLC (High-Level Data Link Control) protocol developed by the International Organization for Standardization (ISO).

T1: Transmission rate of 1.544 Mbps on T1 communications lines. A T1 facility carries a 1.544 Mbps digital signal. Also referred to as DS-1 (Digital Signal Level 1). See also *E1* and *channel*.

TCP/IP (Transmission Control Protocol/Internet Protocol): An open network standard that defines how devices from different manufacturers communicate with each other over one or more interconnected networks. TCP/IP protocols are the foundation of the Internet, a worldwide network of networks connecting businesses, governments, researchers, and educators.

telephone wall cable: 2-pair, 4-pair, or 8-pair, 22- or 24-gauge solid copper wire cable. Telephone wall cable is sometimes called telephone station cable or twisted-pair cable.

TFTP (Trivial File Transfer Protocol/Internet Protocol): A protocol used to transfer files between IP nodes. TFTP is often used to transfer firmware and configuration information from a UNIX computer acting as a TFTP server to an IP networking device, such as the Netopia ISDN Router.

thicknet: Industry jargon for 10Base-5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base-2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

Trunk Line: A communications line connecting two frame relay switches to each other.

UDP (User Datagram Protocol): A TCP/IP protocol describing how packets reach applications in destination nodes.

U interface: The interface on local ISDN equipment where the connection to the ISDN line is made. The Netopia ISDN Router's U interface is its ISDN (WAN) port.

wall jack: A small hardware component used to tap into telephone wall cable. An RJ-11 wall jack usually has four pins; an RJ-45 wall jack usually has eight pins.

WAN (wide area network): A network that consists of nodes connected by long-distance transmission media, such as telephone lines. WANs can span a state, a country, or even the world.

WAN IP: In addition to being a router, the Netopia ISDN Router is also an IP address server. There are four protocols it can use to distribute IP addresses over the WAN which include: DHCP, BOOTP, IPCP and MacIP. WAN IP is a feature for both the Small Office and Corporate Netopia ISDN Router models.

wiring closet: A central location where a building's telephone and network wiring is connected. Multi-story buildings often have a main wiring closet in the basement and satellite wiring closets on each floor.

zone: An arbitrary subset of nodes within an AppleTalk internet. Creating multiple zones makes it easier for users to locate network services. The network administrator defines zones when he or she configures routers. Isolated networks have no zones. LocalTalk and EtherTalk Phase I networks may have no more than one zone each. EtherTalk Phase II and TokenTalk networks may have more than one zone each. Several networks of any AppleTalk type may share a zone name.

Index

Limited Warranty and Limitation of Remedies

Farallon warrants to you, the end user, that the Netopia™ ISDN Router (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. Farallon's entire liability and your sole remedy under this warranty during the warranty period is that Farallon shall, at its option, either repair the Product or refund the original purchase price of the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Farallon Customer Service within the warranty period to obtain a Return Materials Authorization ("RMA") number.
2. Return the defective Product and proof of purchase, shipping prepaid, to Farallon with the RMA number prominently displayed on the outside of the package.

If you are located outside of the United States or Canada, please contact your dealer in order to arrange for warranty service.

THE ABOVE WARRANTIES ARE MADE BY FARALLON ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. FARALLON AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, FARALLON AND ITS LICENSOR(S) DO NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATION REGARDING THE USE OR THE RESULTS OF THE USE OF THE PRODUCT IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, CURRENTNESS, OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT IS ASSUMED BY YOU. THE EXCLUSION OF IMPLIED WARRANTIES IS NOT PERMITTED BY SOME STATES OR JURISDICTIONS, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT CASE, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY OF THE PRODUCT. THERE MAY BE OTHER RIGHTS THAT YOU MAY HAVE WHICH VARY FROM JURISDICTION TO JURISDICTION.

REGARDLESS OF WHETHER OR NOT ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL FARALLON, ITS LICENSOR(S) AND THE DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS OF ANY OF THEM BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, AND THE LIKE) ARISING OUT THE USE OR INABILITY TO USE THE PRODUCT EVEN IF FARALLON OR ITS LICENSOR(S) HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. FARALLON AND ITS LICENSOR(S) LIABILITY TO YOU FOR ACTUAL DAMAGES FROM ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF THE ACTION (WHETHER IN CONTRACT, TORT [INCLUDING NEGLIGENCE], PRODUCT LIABILITY OR OTHERWISE), WILL BE LIMITED TO $50.

v.697