NETOPIA™ D-SERIES DSL DSUs

D3100-I	**IDSL**
D3232	**IDSL**
D7100	**SDSL**
D7171	**SDSL**

User's Reference Guide
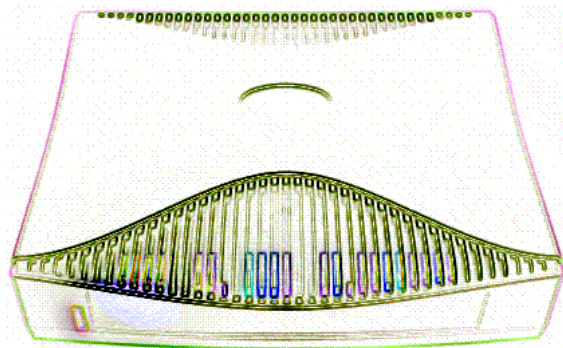
Copyright

Part Number

For additional copies of this electronic manual, order Netopia part number 6161076-PF-02.

Printed Copies

For printed copies of this manual, order Netopia part number TED-DSU/Doc
(P/N 6161076-00-02).

Contents

Glossary

Limited Warranty and Limitation of Remedies

Index

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia D-Series DSL DSUs are Digital Service Units or intelligent Ethernet filtering bridges for SDSL or IDSL connections. They feature the ability to sense the connection type (Frame Relay or RFC 1483 DSL) and automatically configure themselves for use as a DSU to Ethernet bridge. In either configuration the Netopia D-Series offers management features available locally or remotely, either in-band or out-of-band. The DSU mode offers a convenient way to migrate existing DDS or T1 service that uses an external CSU/DSU to connect to SDSL or IDSL. In the intelligent Ethernet bridge mode, the Netopia D-Series includes packet filtering for enhanced security on the LAN and efficient use of the DSL link.

■   The Netopia D7100 and D7171 use an SDSL link to a Copper Mountain DSLAM for the WAN connection.

■   The Netopia D3100-I and D3232 use an ISDN Digital Subscriber Line (IDSL) to provide remote users dedicated, digital access, even if they are connected to a central office via a digital loop carrier (DLC) system or an ISDN repeater.

■   The Netopia D3232 and D7171 use DSL bonding technology, as available through Copper Mountain DSLAMs, to effectively double or quadruple the bandwidth of the DSL link.

In DSU mode the Auxiliary port functions as a Synchronous serial port supplying a V.35 DCE interface for connection to another router. In bridging mode the Ethernet hub bridges traffic as a proxy for the MAC address supplied by the remote end of the DSL link.

The MAC address, or Media Access Control address is the physical address of a device connected to a network, expressed as a 48-bit hexadecimal number. Sometimes this is called the hardware address, and is a unique number assigned to each device by the manufacturer.

The Netopia D-Series provides an auto-sensing function that determines if the Auxiliary port or the hub is associated with the DSL connection. In either case you can manage the device via the hub using Telnet or SNMP, or via the serial console.

The hub effectively has two Ethernet MAC addresses in bridging mode: the proxied address that the remote end supplied and a local IP address for management purposes.

This section covers the following topics:

■   "Features and capabilities" on page 1-12

■   "About DSL Bonding" on page 1-12

■   "How to use this guide" on page 1-13

Features and capabilities

The Netopia D-Series DSL DSUs all provide the following features:

■ Status lights (LEDs) for easy monitoring and troubleshooting.

■ Support for console-based management over Telnet or serial cable connection.

■ Wall-mountable, bookshelf (side-stackable), or desktop-stackable design for efficient space usage.

In DSU mode

■ DSU mode (Frame Relay): Copper Mountain DSL to V.35 for connection to an external router using RFC1490 Frame Relay protocol.

■ Industry-standard V.35 interface for connection to external router.

■ Management Access: Password protected access to management tools with up to four user names and passwords.

In Ethernet filtering bridge mode

■ Ethernet bridge or LAN extension mode (RFC 1483): Copper Mountain DSL to Ethernet for direct connection to a LAN using RFC 1483 protocol.

■ Inter-operates with Copper Mountain Networks Copper Edge™ access concentrator with integrated management.

■ Connectivity to Ethernet LANs via built-in 8 port 10Base-T hub with uplink port.

■ Security Features (Intelligent bridge mode):
Packet Filters (8 user definable filter sets using up to 255 rules): IP and MAC layer packet filtering; Filter packets on source or destination address, service or protocol; filter incoming packets for security, or outgoing packets for more efficient use of DSL bandwidth.
Management Access: Password protected access to management tools with up to 4 user names and passwords.

About DSL Bonding

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

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

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

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

How to use this guide

This guide is designed to be your single source for information about your Netopia D-Series DSL DSU. It is intended to be viewed on-line, using the powerful features of the Adobe Acrobat Reader. The information display has been deliberately designed to present the maximum information in the minimum space on your screen. You can keep this document open while you perform any of the procedures described, and find useful information about the procedure you are performing.

If you prefer to work from hard copy rather than on-line documentation, you can also print out all of the manual, or individual sections. The pages are formatted to print on standard 8 1/2 by 11 inch paper. We recommend that you print on three-hole punched paper, so you can put the pages in a binder for future reference. For your convenience, a printed copy can be purchased from Netopia. Order part number TED-DSU/Doc.

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

Use the guide's table of contents and index to locate informational topics.

Chapter 2

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia D-Series DSL DSU. This section covers the following topics:

Find a location

When choosing a location for the Netopia D-Series, consider:

- Available space and ease of installation

- Physical layout of the building and how to best use the physical space available for connecting your Netopia D-Series to the LAN or router

- Available wiring and jacks

- Distance from the point of installation to the next device (length of cable or wall wiring)

- Ease of access to the front of the unit for configuration and monitoring

- Ease of access to the back of the unit for checking and changing cables

- Cable length and network size limitations when expanding networks

What you need

Locate all items that you need for the installation.

Included in your Netopia D-Series package are:

- The Netopia D-Series DSL DSU

- A power adapter and cord with a mini-DIN8 connector

- Two RJ-45 10Base-T Ethernet or Line cables

- A dual DE-9 and mini-DIN8 to DE-9 console cable (for a PC or a Macintosh)

- An HD-15 to V.35 DCE interface cable

- Two splitters (D3232 only)

- The CustomerCare CD containing an Internet browser, Adobe Acrobat Reader for Windows and Macintosh, ZTerm terminal emulator software and NCSA Telnet for Macintosh, and documentation

You will need:

■ A Windows 95-, 98-, 2000-, or NT–based PC or a Macintosh computer with Ethernet connectivity for configuring the Netopia D-Series. This may be built-in Ethernet or an add-on card, with TCP/IP installed and configured. See Chapter 4, "Configuring TCP/IP."

■ An SDSL or IDSL wall outlet wired for a connection to a Competitive Local Exchange Carrier (CLEC) that supports Digital Subscriber Line connections.

Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia D-Series cables.

The figure below displays the back of the Netopia D-Series DSL DSU.

Netopia D-Series DSL DSU back panel
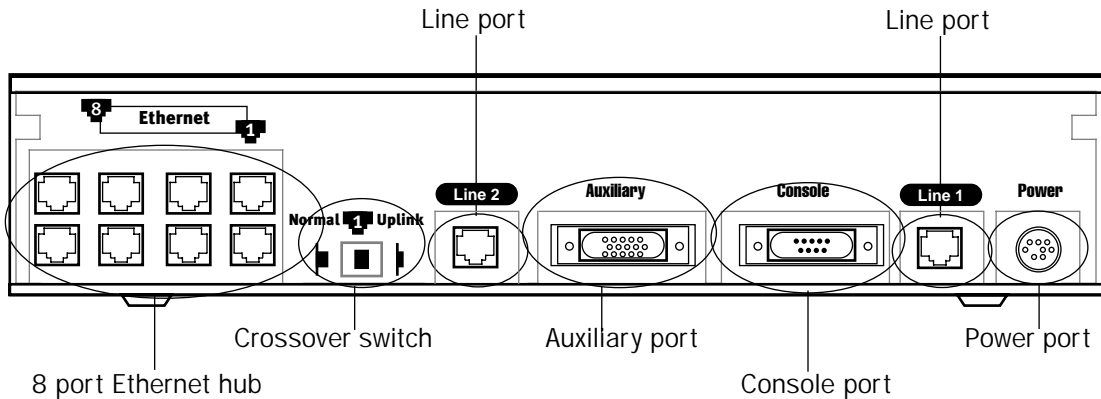
Filtering Bridge mode

1. Connect the mini-DIN8 connector from the power adapter to the power port, and plug the other end into an electrical outlet.

2. Connect one end one of the RJ-45 cables to the Line 1 port, and the other end to your SDSL or IDSL wall outlet.

3. Connect one end of one of the RJ-45 Ethernet cables to any of the Ethernet ports on the Netopia D-Series and the other end to your computer or to your network.

   (If you are connecting the Netopia D-Series to an existing Ethernet hub, use Ethernet port #1 on the Netopia D-Series and set the crossover switch to the **Uplink** position.)

   You should now have: the power adapter plugged in; the Ethernet cable connected between the Netopia D-Series and your computer or network; and the SDSL or IDSL cable connected between the Netopia D-Series and the SDSL or IDSL wall outlet.

DSU mode

1. Connect the mini-DIN8 connector from the power adapter to the power port, and plug the other end into an electrical outlet.

2. Connect one end one of the RJ-45 cables to the Line 1 port, and the other end to your SDSL or IDSL wall outlet.

3. Connect one end of one of the RJ-45 Ethernet cables to any of the Ethernet ports on the Netopia D-Series and the other end to your computer or to your network.

    (If you are connecting the Netopia D-Series to an existing Ethernet hub, use Ethernet port #1 on the Netopia D-Series and set the crossover switch to the **Uplink** position.) This connection will provide management access to the Netopia D-Series.

4. Connect the HD-15 end of the supplied V.35 interface cable to the Auxiliary port and the other end to your external Frame Relay router. The unit will auto-detect filtering bridge mode or DSU mode, based on which cables are connected and traffic on the lines.

Connect Line ports to mutiple DSL lines (D3232 only)

On the Netopia D3232 DSU, you can connect the Line ports to up to 4 DSL lines using the splitters provided with your equipment.

1. Connect one end of one of the RJ-45 cables to the Line 1 port, and the other end to the port on the single end of the splitter.

2. Connect one end of another RJ-45 cable to either of the ports on the double end of the splitter, and the other end of the RJ-45 cable to one of your SDSL or IDSL wall outlets.

3. Connect one end of another RJ-45 cable to the second port on the double end of the splitter, and the other end of the RJ-45 cable to another of your SDSL or IDSL wall outlets.

4. Repeat steps 1-3 with the Line 2 port, the second splitter, and a third and fourth SDSL or IDSL wall outlets.

Netopia D-Series DSL DSU back panel ports

The following table describes all the Netopia D-Series DSL DSU back panel ports.

Port	Description
Power port	A mini-DIN8 power adapter cable connection.
Line port 1 and 2	Two RJ-45 telephone-style jacks labelled Line 1 and Line 2 for your SDSL or IDSL connections.
Console port	A DE-9 console port for a direct serial connection to the console screens. You can use this if you are an experienced user. See "Connecting a console cable to your Netopia D-Series" on page 5-36.
Auxiliary port	An HD-15 auxiliary port for attaching the V.35 interface cable to an external Frame Relay router in DSU mode. In Filtering Bridge mode you can connect an external modem to this port for remote out-of-band management. This application requires separate purchase of the Async cable (Part TE6/DB25).
Crossover switch	A crossover switch with Normal and Uplink positions. If you use Ethernet Port #1 for a direct Ethernet connection between a computer and the Netopia D-Series, set the switch to the **Normal** position. If you are connecting the Netopia D-Series to an Ethernet hub, use Ethernet port #1 on the Netopia D-Series and set the switch to the **Uplink** position.

Port	Description
8-port Ethernet hub	Eight 10Base-T Ethernet jacks. You will use one of these to configure the Netopia D-Series. For a new installation, use the Ethernet connection. Alternatively, you can use the console connection to run console-based management using a direct serial connection. You can either connect your computer directly to any of the Ethernet ports on the Netopia D-Series, or connect both your computer and the Netopia D-Series to an existing Ethernet hub on your LAN.

Netopia D-Series DSL DSU status lights

The figure below represents the Netopia D-Series status light (LED) panel.

Netopia D-Series LED front panel
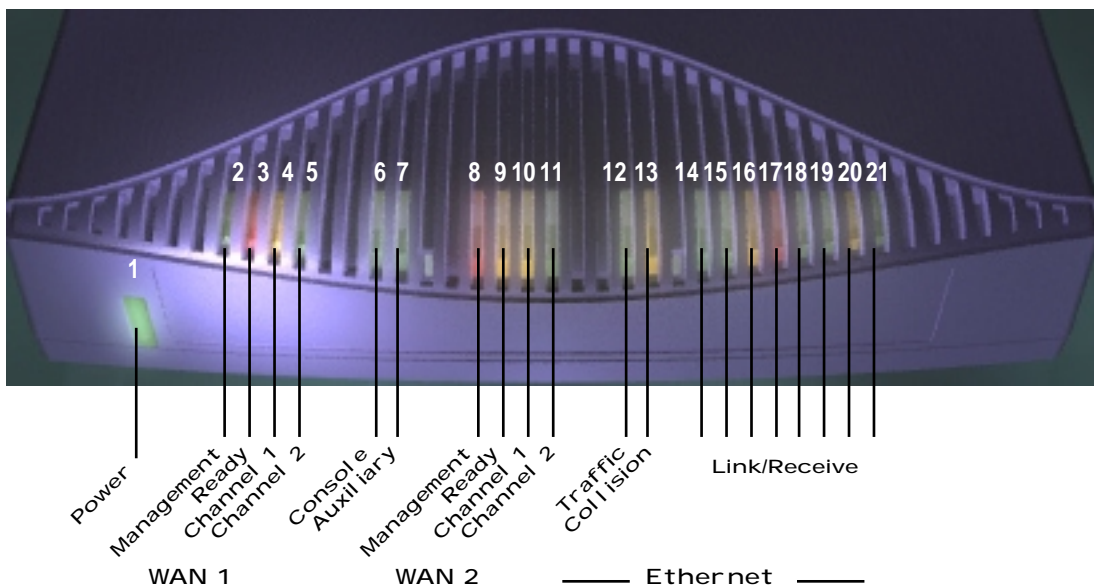
The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
The corresponding line passes supervisory traffic between the Digital Subscriber Line Access Multiplexer (DSLAM) and the Netopia D-Series	2 or 8 flashes **yellow**.
The WAN interface is operational	3 or 9 is **green**.
The line is unavailable	3 or 9 flashes **red**.
The WAN on Channel 1 has carrier	4 or 10 is **green**.
Data is transmitted or received on the WAN on Channel 1	4 or 10 flashes **yellow**.
The WAN on Channel 2 has carrier	5 or 11 is **green**. (D3232 only)

When this happens...	the LEDs...
Data is transmitted or received on the WAN on Channel 2	5 or 11 flashes **yellow**. (D3232 only)
Console cable is attached and has carrier	6 and 7 are **green**.
Data is transmitted or received	6 and 7 flash **yellow**.
Data is transmitted or received by the ethernet controller	12 flashes **yellow**.
The Ethernet interface detects a collision	13 flashes **red**.
Link is detected	14 though 21 are **solid green**.
Data are received on their respective ports	14 though 21 **flash green**.
Note: Console carrier (6) is ignored if the console is not configured for a remote modem.	

Chapter 3

Connecting to Your Local Area Network

This chapter describes how to physically connect the Netopia D-Series to your local area network (LAN). Before you proceed, make sure the Netopia D-Series is properly configured. You can customize the Netopia D-Series's configuration for your particular LAN requirements using console-based management (see "Console-Based Management" on page 5-35).

This section covers the following topics:

- "Netopia D-Series Configuration Modes" on page 3-21
- "Readying computers on your local network" on page 3-23
- "Connecting to an Ethernet network" on page 3-24

Netopia D-Series Configuration Modes

The Netopia D-Series DSL DSU can be used in either of two ways:

- as an intelligent Ethernet filtering bridge for DSL connections, or
- as a Digital Service Unit

When the appropriate cables are connected, it senses the connection type (Frame Relay or ATM FUNI) and automatically configures itself for use as a DSU or a DSL to Ethernet bridge.

See the following sections for suggestions on how to connect the Netopia D-Series to different types of networks.

Filtering bridge mode

The following figure shows a typical configuration for the filtering bridge mode:
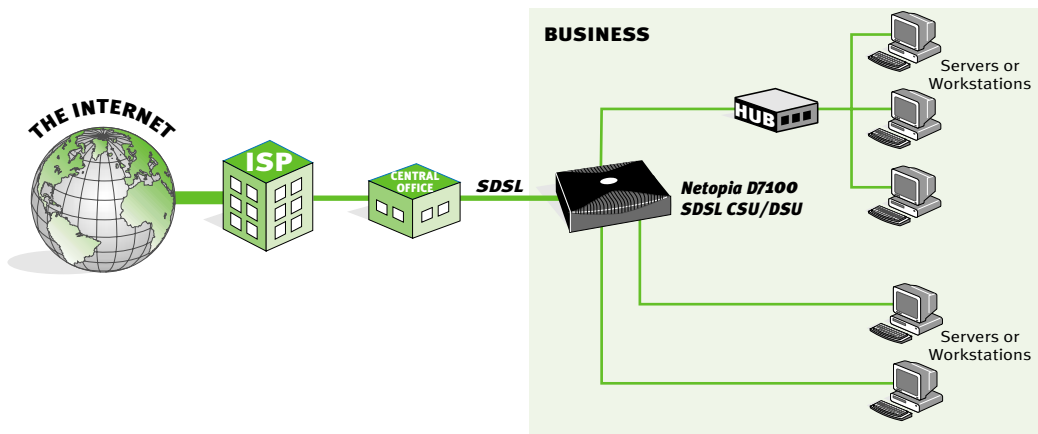
In bridge mode the Netopia D-Series performs a simple algorithm. When the Netopia D-Series receives a packet on the Ethernet hub, the packet is examined for its destination Media Access Control (MAC) address.

The MAC address is the physical address of a device connected to a network, expressed as a 48-bit hexadecimal number. Sometimes this is called the hardware address, and is a unique number assigned to each device by the manufacturer.

If the destination MAC address is the Netopia D-Series's MAC address, based on its serial number, and it is for management purposes (Telnet or SNMP) or is an ICMP that needs response, it is accepted. If it is the MAC address that is being proxied (supplied by the DSLAM) it is encapsulated in ATM FUNI and transmitted over the DSL connection. A packet received from the DSL connection will be de-encapsulated and its MAC address examined. Either it is management traffic for the Netopia D-Series, or it is encapsulated for Ethernet and transmitted over the hub.

DSU mode

The DSU behavior is similar, except that the datalink encapsulation on the WAN is Frame Relay, and the destination for packets from the WAN is the Auxiliary port. The Ethernet hub is only available for management (Telnet or SNMP).

A special male HD-15 to female V.35 cable supports the Netopia D-Series as a DCE connecting the Auxiliary port to a Frame Relay Access Device (FRAD) such as a sync serial router.

The following figure shows a typical configuration for the DSU mode:
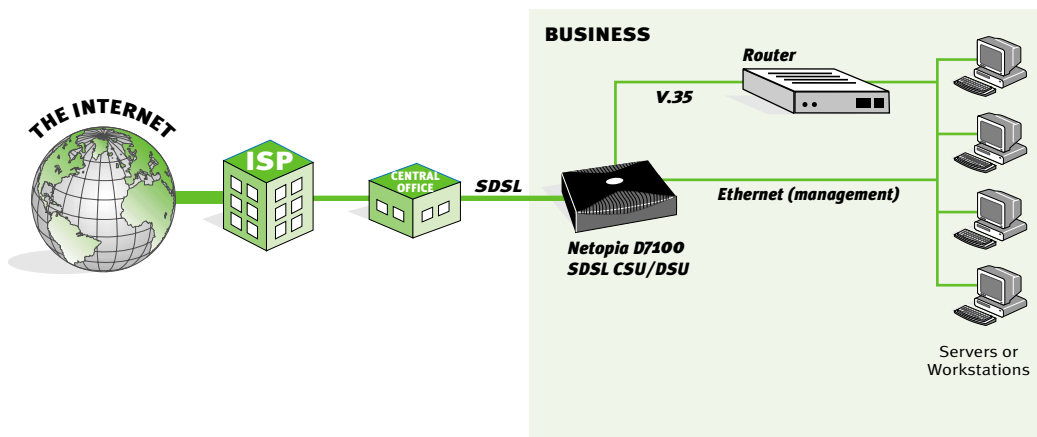
The sections that follow refer to the filtering bridge mode only.

Readying computers on your local network

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

```
                    ┌──────────────────────────────────┐
                    │      Application software        │
                    ├──────────────────────────────────┤
                    │         TCP/IP stack             │
                    ├──────────────────────────────────┤
                    │        Ethernet Driver           │
                    └──────────────────────────────────┘

        Your PC
        or Macintosh
        computer
                         To the Netopia D-Series
```
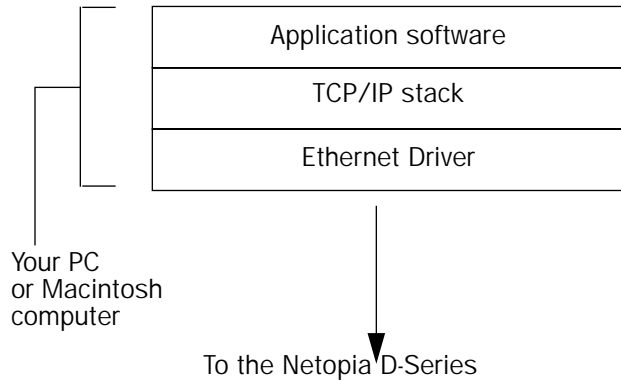
Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora e-mail client and the Web browsers Microsoft Internet Explorer and Netscape Navigator.

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 D-Series. There are a number of TCP/IP stacks available for PC computers. Windows 95 includes a built-in TCP/IP stack. See "Configuring TCP/IP on Windows 95 or 98 computers" on page 4-28. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on Macintosh computers" on page 4-30.

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 D-Series 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 an Ethernet network

The Netopia D-Series supports Ethernet connections through its eight Ethernet ports. The Netopia D-Series automatically detects which Ethernet port is in use.

10Base-T

You can connect a standard 10Base-T Ethernet network to the Netopia D-Series using any of its available Ethernet ports.

Netopia D-Series back panel
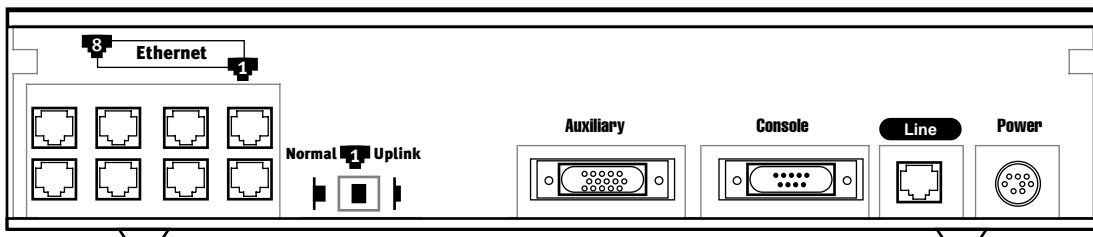
The Netopia D-Series in a 10Base-T network

To connect your 10Base-T network to the Netopia D-Series through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than eight devices to connect, you can attach additional devices using another 10Base-T hub.
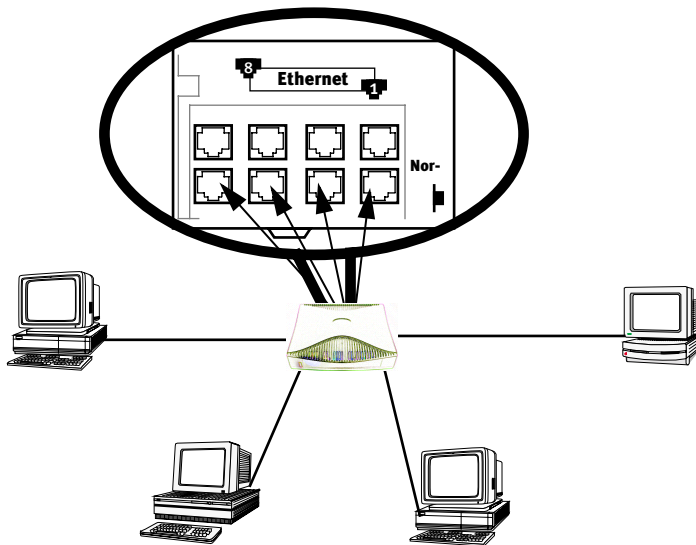
If you add devices connected through a hub, connect the hub to Ethernet port number 1 on the Netopia D-Series and set the Normal/Uplink switch to Uplink.
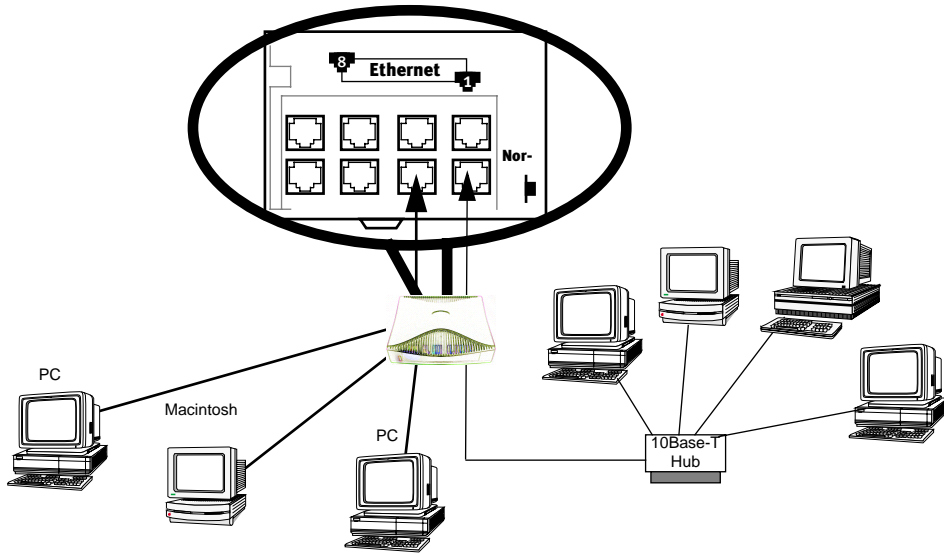
Chapter 4

Configuring TCP/IP

Computers on your network must have TCP/IP installed and configured. This chapter tells you how to configure TCP/IP on the desktop computers on your network.

This chapter covers the following topics:

■   "Configuring TCP/IP on Windows 95 or 98 computers" on page 28

■   "Configuring TCP/IP on Macintosh computers" on page 30

Note: For information on configuring TCP/IP on Windows 2000 or NT computers, please see the Microsoft documentation.

Configuring TCP/IP on Windows 95 or 98 computers

Configuring TCP/IP on a Windows computer requires the following:

■   An Ethernet card (also known as a network adapter)

■   The TCP/IP protocol must be "bound" to the adapter or card

If you are manually configuring for a fixed or static IP address, perform the following:

1.   Go to Start Menu/Settings/Control Panels and double click the **Network** icon. From the Network components list, select the **Configuration** tab.

2.   Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the **IP Address** tab. Click "Specify an IP Address."
     Enter the following:
     IP Address: 192.168.1.2
     Subnet Mask: 255.255.255.0, or for 12-user models 255.255.255.240
     This address is an example of one that can be used to configure the Netopia D-Series with the Easy option in the SmartStart Wizard. Your ISP or network administrator may ask you to use a different IP address and subnet mask.
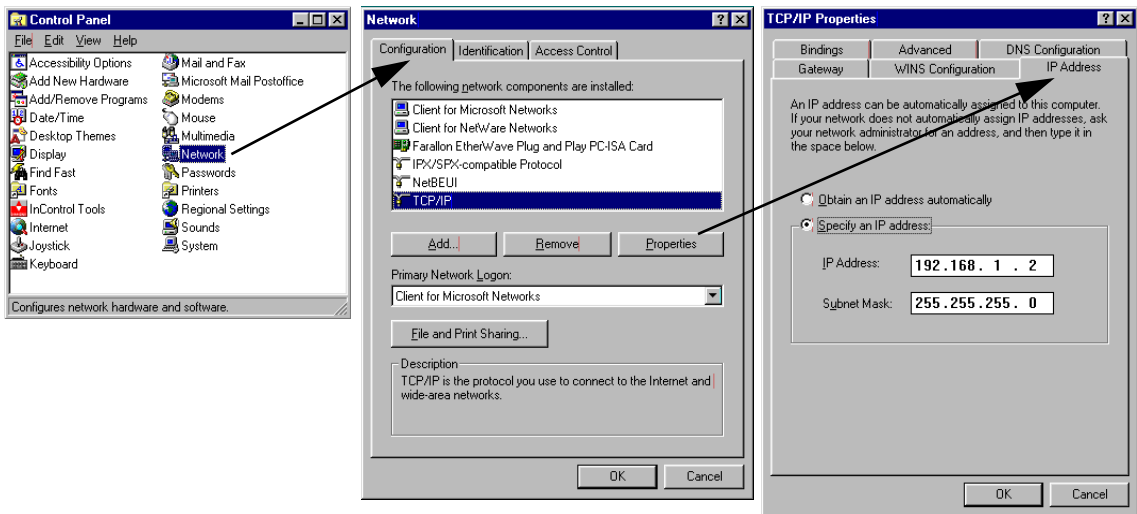
3. Click on the **Gateway** tab (shown below). Under "New gateway," enter **192.168.1.1**. Click **Add**. This is the Netopia D-Series's pre-assigned IP address.
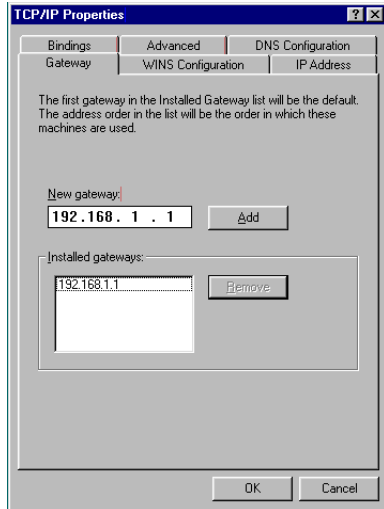
Click on the **DNS Configuration** tab. Click **Enable DNS**. Enter the following information:

Host: Type the name you want to give to this computer.

Domain: Type your domain name. If you don't have a domain name, type your ISP's domain name; for example, netopia.com.

DNS Server Search Order: Type the primary DNS IP address given to you by your ISP. Click **Add**. Repeat this process for the secondary DNS.

Domain Suffix Search Order: Enter the same domain name you entered above.
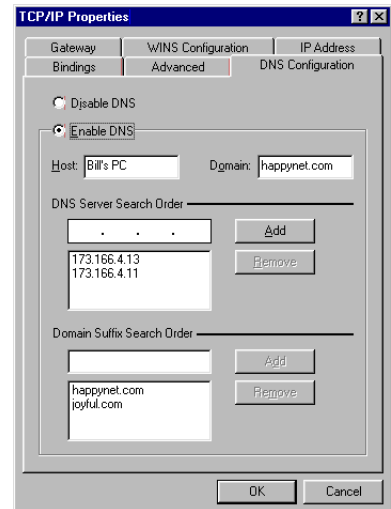
4. Click **OK** in this window, and the next window. When prompted, reboot the computer.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Configuring TCP/IP on Macintosh computers

The following is a quick guide to configuring TCP/IP for MacOS computers. Configuring TCP/IP in a Macintosh computer requires the following:

■ You must have either Open Transport or Classic Networking (MacTCP) installed.

■ You must have built-in Ethernet or a third-party Ethernet card and its associated drivers installed in your Macintosh.

If you are manually configuring for a fixed or static IP address, perform the following:

1. Go to the Apple menu. Select **Control Panels** and then **TCP/IP** or **MacTCP**.

2. With the TCP/IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.

   Or, in the MacTCP window, select **Ethernet** and click the **More** button.
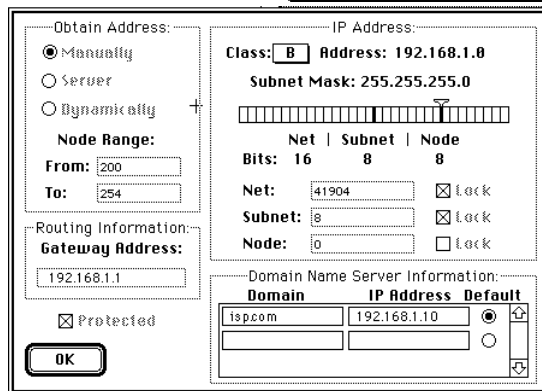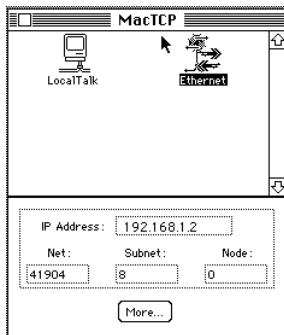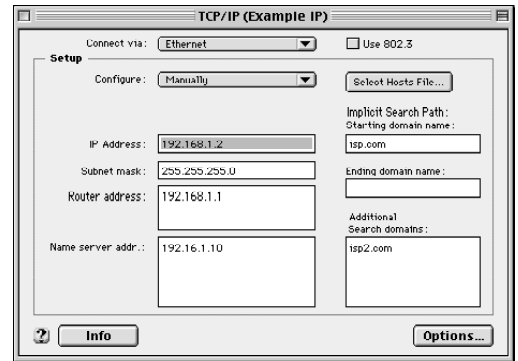
3. In the TCP/IP window or in the MacTCP/More window, select or type information into the fields as shown in the following table.

Option:	Select/Type:
Connect via:	Ethernet
Configure:	Manually
IP Address:	192.168.1.2
Subnet mask:	255.255.255.0, or for 12-user models 255.255.255.240
Router or Gateway address:	192.168.1.1
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP

Option:	Select/Type:
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

4. Close the TCP/IP or MacTCP control panel and save the settings.

5. If you are using MacTCP, you must restart the computer. If you are using Open Transport, you do not need to restart. These are the only fields you need to modify in this screen.

Note: You can also use these instructions to configure other computers on your network with manual or static IP addresses. Be sure each computer on your network has its own IP address.

Part II: Advanced Configuration

Chapter 5

Console-Based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia D-Series. Console-based management provides access to a wide variety of features that the Netopia D-Series supports. You can customize these features for your individual setup. This chapter describes how to access the console-based management screens.

This section covers the following topics:

■   "Connecting a console cable to your Netopia D-Series" on page 5-36

■   "Connecting through a Telnet session" on page 5-37

■   "Navigating through the console screens" on page 5-38

Console-based management screens contain five entry points to the Netopia D-Series configuration and monitoring features. The entry points are displayed in the Main Menu shown below:

```
                        Netopia D3232 v4.6




                WAN Configuration...

                System Configuration...

                Utilities & Diagnostics...

                Statistics & Logs...


                Quick View...




 Return/Enter for WAN Line configuration.
 You always start from this main screen.
```

Note: Although it references the Netopia D3232, this screen applies to all Netopia D-Series DSL DSUs.

■   The **WAN Configuration** menu displays and permit changing the following options:

■   Clock Source: Network or Internal

■   Bridge Mode Filter Set: Basic Firewall or NetBIOS Filter

■   Remove Filter Set

■   The **System Configuration** menus display and permit changing:

■   Management IP Setup. See "Management IP setup" on page 6-42.

- ■ Filter Sets (Firewalls). See *"Security"* on page 8-61.

- ■ Date and time. See *"Date and time"* on page 6-43.

- ■ Console configuration. See *"Connecting a console cable to your Netopia D-Series"* on page 5-36.

- ■ SNMP (Simple Network Management Protocol). See *"SNMP"* on page 7-57.

- ■ Security. See *"Security"* on page 8-61.

- ■ Upgrade feature set. See *"Upgrade feature set"* on page 6-44.

- ■ Logging. See *"Event histories"* on page 7-54.

■ The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the Netopia D-Series's behavior, as well as for updating the firmware and rebooting the system. See *"Utilities and Diagnostics"* on page 9-91 for detailed information.

■ The **Statistics & Logs** menus display nine sets of tables and device logs that show information about your Netopia D-Series, your network and their history. See *"Statistics & Logs"* on page 7-53 for detailed information.

■ The **Quick View** menu displays at a glance current real-time operating information about your Netopia D-Series. See *"Quick View status overview"* on page 7-51 for detailed information.

Connecting a console cable to your Netopia D-Series

If you will be assigning an IP address to the Netopia D-Series other than the default 192.168.1.1, it is best to access the unit through the serial console.

You can perform all of the system configuration activities for your Netopia D-Series through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows95 on the PC, or ZTerm, included on the CustomerCare CD, for Macintosh computers.

The Netopia D-Series back panel has a connector labeled "Console" for attaching the Netopia D-Series to either a PC or Macintosh computer via the serial port on the computer. (On a Macintosh computer, the serial port is called the Modem port or Printer port.) This connection lets you use the computer to configure and monitor the Netopia D-Series via the console screens.
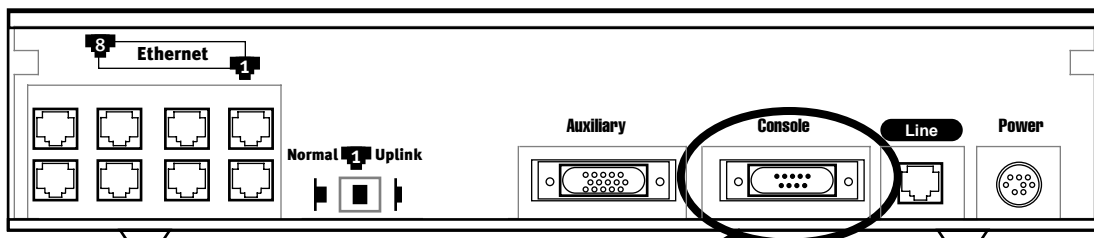
Console connection port
DB-9 (male)

To connect the Netopia D-Series to your computer for serial console communication, use the supplied dual console cable connector end appropriate to your platform:

■ One DB-9 connector end attaches to a PC.

■ The mini-DIN8 connector end attaches to a Macintosh computer.

■ The DB-9 end of the Console cable attaches to the Netopia D-Series's Console port.

■ If you connect a PC with Microsoft Windows 95 or NT, you can use the HyperTerminal application bundled with the operating system.

■ If you connect a Macintosh computer, you can use the ZTerm terminal emulation program on the supplied CustomerCare CD.

Launch your terminal emulation software and configure the communications software for the values shown in the table below. These are the default communication parameters that the Netopia D-Series uses.

Parameter	Suggested Value
Terminal type	**PC**: ANSI-BBS **Mac**: ANSI, VT-100, or VT-200
Data bits	8
Parity	None
Stop bits	1
Speed	57600 bits per second
Flow Control	None
Note: The Netopia D-Series firmware contains an autobaud detection feature. If you are at any screen on the serial console, you can change your baud rate and press Return (HyperTerminal for the PC requires a disconnect). The new baud rate is displayed at the bottom of the screen.	

Connecting through a Telnet session

Features of the Netopia D-Series can be configured through the console screens via Telnet.

Before you can access the console screens through Telnet, you must have:

■ A network connection locally to the Netopia D-Series or IP access to the Netopia D-Series.

The default IP address of the Netopia D-Series is 192.168.1.1, subnet mask 255.255.255.0. In order to perform the initial configuration via Telnet your computer must have an IP address between 192.168.1.2 and 192.168.1.254, subnet mask 255.255.255.0.

Caution: If you change the Netopia D-Series's IP address to some value outside of this range, you may lose contact with the unit via Telnet.

Alternatively, you can have a direct serial console cable connection using the provided console cable for your platform (PC or Macintosh) and the Console port on the back of the Netopia D-Series. For more information on attaching the console cable, see *"Connecting a console cable to your Netopia D-Series" on page 5-36.*

■   Telnet software installed on the computer you will use to configure the Netopia D-Series

Configuring Telnet software

If you are configuring your Netopia D-Series using a Telnet session, your computer must be running a Telnet software program.

■   If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or simply run Telnet from the Start menu.

■   If you connect a Macintosh computer, you can use the NCSA Telnet program supplied on the CustomerCare CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Navigating through the console screens

Use your keyboard to navigate the Netopia D-Series's configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the console screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
To set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	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	Up arrow or Control + k
Move one item down	Down arrow or Control + O
Display a dump of the device event log	Control + e
Display a dump of the WAN event log	Control + f
Refresh the screen	Control + L
Go to topmost selectable item	<
Go to bottom right selectable item	>

Chapter 6

WAN and System Configuration

This chapter describes how to use the console-based management screens to access and configure advanced features of your Netopia D-Series DSL DSU. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their Netopia D-Series's connection and system configuration.

This chapter also describes DSL Bonding, or iMux, and how to configure your Netopia D-Series equipment to use it.

This section covers the following topics:

System Configuration screens

You can connect to the Netopia D-Series's system configuration screens in either of two ways:

■ By using Telnet with the Netopia D-Series's Ethernet port IP address. The default is 192.168.1.1, subnet mask 255.255.255.0.

■ Through the console port, using a local terminal (see "Connecting a console cable to your Netopia D-Series" on page 5-36)

You can also retrieve the Netopia D-Series's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 7-57).

Open a Telnet connection to the Netopia D-Series's IP address; for example, the default "192.168.1.1."

The console screen will open to the **Main Menu**, similar to the screen shown below:

```
                    Netopia D3232 v4.6




            WAN Configuration...

            System Configuration...

            Utilities & Diagnostics...

            Statistics & Logs...


            Quick View...



Return/Enter displays options for the system.
You always start from this main screen.
```

Note: Although it references the Netopia D3232, this screen applies to all Netopia D-Series DSL DSUs.

Navigating through the system 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:

Main Menu → System Configuration → Management IP Setup → IP Setup
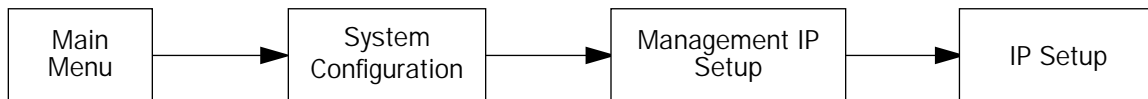
This particular path guide shows how to get to the Management IP Setup screens. The path guide represents these steps:

1.   Beginning in the Main Menu, select **System Configuration** and press Return. The System Configuration screen appears.

2.   Select **Management IP Setup** and press Return. The IP Setup screen appears.

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

System configuration features

The Netopia D-Series DSL DSU's default settings may be all you need to configure your Netopia D-Series. Some users, however, require advanced settings or prefer manual control over the default selections. For these users, the Netopia D-Series provides system configuration options.

To access the system configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration menu screen appears:

```
                        System Configuration

            Management IP Setup...
            Filter Sets...

            Date and Time...

            Console Configuration...

            SNMP (Simple Network Management Protocol)...

            Security...

            Upgrade Feature Set...


            Logging...
     Return/Enter to configure Networking Protocols (such as TCP/IP).
     Use this screen if you want options beyond Easy Setup.
```
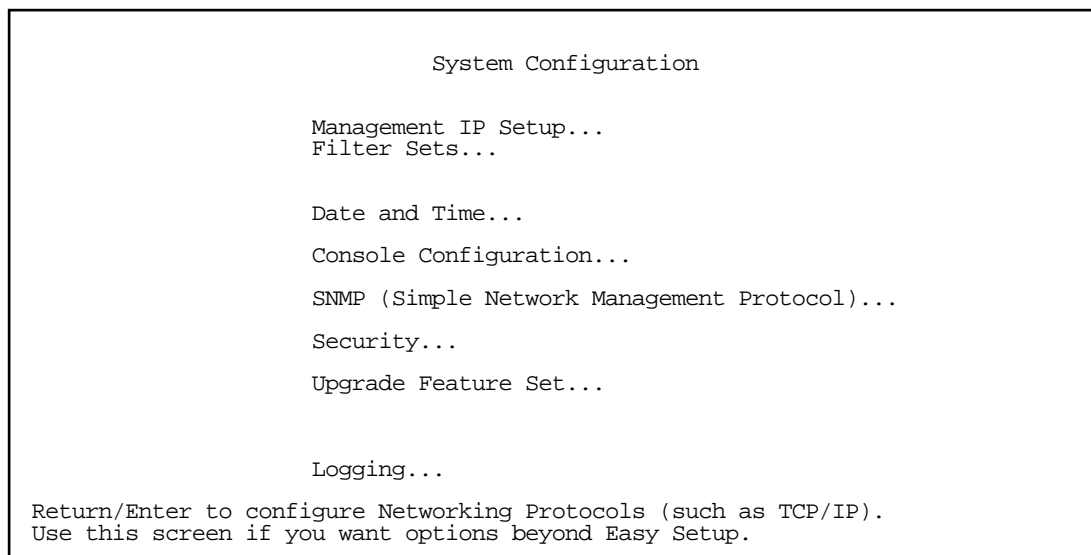
Options available under the System Configuration menu are described in the following sections.

Management IP setup

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. You will need this information before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia D-Series is reset.

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

```
┌─────────┐      ┌───────────────┐      ┌────────────┐      ┌───────────┐
│  Main   │ ───▶ │    System     │ ───▶ │ Management │ ───▶ │  IP Setup │
│  Menu   │      │ Configuration │      │     IP     │      │           │
│         │      │               │      │   Setup    │      │           │
└─────────┘      └───────────────┘      └────────────┘      └───────────┘
```
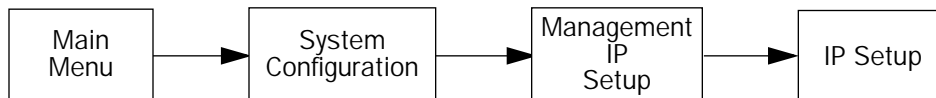
The IP Setup screen appears.

This screen allows you to change the Netopia D-Series's Ethernet IP Address, Subnet Mask, and Default IP Gateway.

```
                          IP Setup

        Ethernet IP Address:              192.168.1.1
        Ethernet Subnet Mask:             255.255.255.0


        Default IP Gateway:               0.0.0.0










     Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
     Set up the basic IP attributes of your Netopia in this screen.
```

Follow these steps to configure IP Setup for your Netopia D-Series:

■   Select **Ethernet IP Address** and enter the IP address for the Netopia D-Series'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 D-Series.

     A default gateway should be able to successfully route packets when the Netopia D-Series cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router, in bridge mode, or the locally attached router, in DSU mode.

Filter sets

When using the Netopia D-Series in bridge mode only, these screens allow you to configure security on your network by means of filter sets. Details are given in "About filters and filter sets" on page 8-64.

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 System Configuration screen and press Return. The Set Date and Time screen appears.

```
                          Set Date and Time


         System Date Format:                  MM/DD/YY
         Current Date (MM/DD/YY):             3/16/1999

         System Time Format:                  AM/PM
         Current Time:                        10:29
         AM or PM:                            AM
```

Follow these steps to set the system's date and time:

1. Select **System Date Format**. A popup allows you to choose the format used in your country or locality. Options are: MM/DD/YY, DD/MM/YY, and YY/MM/DD.

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**. A popup allows you to choose either AM/PM or 24hr formats.

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. If you chose AM/PM format, select **AM or PM** and choose **AM** or **PM**. If you chose 24hr format, this menu item is hidden.

Console configuration

You can change the default terminal communications parameters to suit your requirements.

To go to the Console Configuration screen, select **Console Configuration** in the System Configuration screen.

```
                        Console Configuration

        Baud Rate...                       57600

        Hardware Flow Control:             No








        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.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent. Details are given in "SNMP" on page 7-57.

Security

These screens allow you to add users and define passwords on your network. Details are given in "Security" on page 8-61.

Upgrade feature set

You can upgrade your Netopia D-Series by adding new feature sets through the Upgrade Feature Set utility.

See the release notes that came with your Netopia D-Series or feature set upgrade, or visit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia D-Series.

Logging

You can configure a UNIX-style syslog client for the PC to report a number of subsets of the events entered in the Netopia D-Series's WAN Event History. See "WAN Event History" on page 7-55. The Syslog client daemon program (for the PC only) is supplied as a .ZIP file on the CustomerCare CD.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.

```
                         Logging Configuration


         WAN Event Log Options
         Log Boot and Errors:              Yes
         Log Line Specific:                Yes



         Syslog Parameters
         Syslog Enabled:                   No
         Hostname or IP Address:
         Facility...                       Local 0




   Return/Enter accepts * Tab toggles * ESC cancels.

```

By default, all events are logged in the event history.

■   By toggling each event descriptor either **Yes** or **No**, you can determine which ones are logged and which are ignored.

■   You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.

■   You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.

■   You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.

Installing the Syslog client

The Goodies folder on the CustomerCare CD contains a Syslog client daemon program that can be configured to report the WAN events you specified in the Logging Configuration screen.

To install the Syslog client daemon, exit from the graphical CustomerCare CD program and locate the CD directory structure through your Windows desktop, or through Windows Explorer. Go to the Goodies directory on the CD and locate the Sds15000.exe program. This is the Syslog daemon installer. Run the Sds15000.exe program and follow the on screen instructions for enabling the Windows Syslog daemon.

The following screen shows a sample syslog dump of WAN events:

```
6, 152, 173.166.107.100, 3/10/99, 9:55:03 AM,  RFC1483: IP up, channel 2, gateway: 163.176.107.1
6, 152, 173.166.107.100, 3/10/99, 9:55:08 AM,   RFC1483-2 rate set to 576 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:09 AM,   DML-4 up
6, 152, 173.166.107.100, 3/10/99, 9:55:10 AM,   RFC1483-2 rate set to 432 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:10 AM,   RFC1483-2 rate set to 432 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:13 AM,   DML-3 up
6, 152, 173.166.107.100, 3/10/99, 9:55:13 AM,   DML-1 up
6, 152, 173.166.107.100, 3/10/99, 9:55:13 AM,   DML-2 up
6, 152, 173.166.107.100, 3/10/99, 9:55:14 AM, >>WAN: Data link activated at 144 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:14 AM, >>WAN: Data link activated at 144 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:14 AM, >>WAN: Data link activated at 144 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:15 AM,   RFC1483-2 rate set to 144 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:17 AM,   RFC1483: Channel 2 up
6, 152, 173.166.107.100, 3/10/99, 9:55:20 AM, >>WAN: Data link activated at 144 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:23 AM, BRIDGE: Line is up in ATM-Funi mode
6, 152, 173.166.107.100, 3/10/99, 9:55:24 AM, --Device restarted--------------------------
6, 152, 173.166.107.100, 3/10/99, 9:55:36 AM, >>WAN: IDSL 1 activated at 1568 Kbps
6, 152, 173.166.107.100, 3/10/99, 9:55:37 AM, BRIDGE: Line is up in ATM-Funi mode
```

DSL Bonding (iMux)

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

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

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

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

What DSL Bonding does

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

■   The concept of multiplexing applies when a number of relatively small data streams are combined into a single line with greater bandwidth, in order to increase the efficiency and maximize utilization of a higher speed WAN connection. An example of multiplexing would be the combination of multiple DS0 links in a single T1 or E1 circuit.

■   DSL Bonding takes a single high-speed data stream and spreads it across several lower speed physical links, which logically form a single aggregated channel or group. Multiple SDSL or IDSL lines are combined to create a single logical data channel that is the aggregate of the individual lines' bandwidths, minus a small amount used for overhead. A packet of information from a LAN, video conferencing session, or other data application is broken down into individual bits or cells which are transmitted in a round robin fashion across two SDSL or IDSL circuits. At the other end of the link, the bits or cells are reassembled in the

same order in which they were transmitted, and the reconstructed packet is sent on to the recipient's networking equipment.

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

Netopia DSL Bonding

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

Currently, the D-Series equipment does not support the potential use of more than one ISDN U-BRI channel for switched ISDN applications – the additional BRIs available on a single or dual WAN module configuration can only be bonded to the first BRI in IDSL DML mode.

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

WAN configuration

To configure your Wide Area Network (WAN) connection and DSL link, navigate to the WAN Configuration screen from the Main Menu and select **WAN Configuration**, then **Choose Interface to Configure**.

Note: On the Netopia D7100, select **WAN Configuration**, then **SDSL Line Configuration**. Skip to page 6-49.

| Main Menu | → | WAN Configuration | → | WAN Setup | → | Choose Interface to Configure |
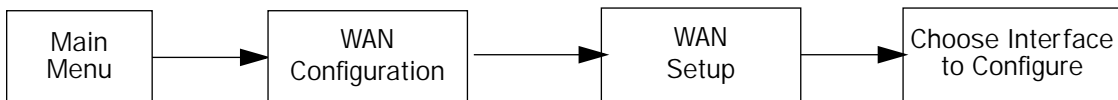
The **Choose Interface to Configure** screen appears.

The screen below shows the ISDN/IDSL option for the WAN to be configured on the D3100-I or D3232.

```
                    Choose Interface to Configure

        ISDN/IDSL (Wan Module 1 and 2) Setup...

        Auxiliary Serial Port Setup...
```

The screen below shows the D7171's SDSL option.

```
                    Choose Interface to Configure

        CMN SDSL (Wan Module 1 and 2) Setup...

        Auxiliary Serial Port Setup...
```

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

The Line Configuration screen appears, **IDSL Line Configuration** for the D3100-I or D3232,

```
                       IDSL Line Configuration
                                       +----------+
                                       +----------+
            Clock Source...            │ Network  │
                                       │ Internal │
                                       +----------+
            Bridge Mode Filter Set...      Filter Set  1
            Remove Filter Set




      Return/Enter goes to new screen.
```

or **SDSL Line Configuration** for the D7100.

```
                       SDSL Line Configuration
                                       +----------+
                                       +----------+
            Clock Source...            │ Network  │
                                       │ Internal │
                                       +----------+
            Bridge Mode Filter Set...      Filter Set  1
            Remove Filter Set




      Return/Enter goes to new screen.
```

or **SDSL Line Configuration** for the D7171.

```
                       SDSL Line Configuration


            Clock Source...                Network

            Data Link Encapsulation...     RFC1483

            Prioritize Delay-Sensitive Data:   No




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

■ The **Clock Source** may be either Network or Internal. If you select Network (the default), the Netopia D-Series IDSL interface functions in customer premise equipment (CPE) mode. This mode is the normal mode for communicating with an ISP. If you select Internal, the Netopia D-Series functions in central office equipment (COE) mode, simulating a DSLAM. This allows for back-to-back short haul applications with another Netopia IDSL device operating in CPE mode.

■ A **Data Rate** pop-up item is available only if the clock source is Internal. This item allows you to set the data rate for the DSL link (and the attached CPE device).

■ A **Bridge Mode Filter Set** pop-up item allows you to select a filter set to make active on the IDSL or SDSL link. See "About filters and filter sets" on page 8-64 for more information.

■ You can deactivate any previously selected filter set by selecting **Remove Filter Set** and pressing Return.

■ A **Data Link Encapsulation** pop-up item allows you to select an ecapsulation type for the link.

■ **Prioritize Delay-Sensitive Data** may be either Yes or No. The default is No.

Chapter 7

Monitoring Tools

This chapter discusses the Netopia D-Series'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.

This section covers the following topics:

- "Quick View status overview" on page 7-51
- "Statistics & Logs" on page 7-53
- "Event histories" on page 7-54
- "System Information" on page 7-57
- "SNMP" on page 7-57

Quick View status overview

You can get a useful, overall status report from the Netopia D-Series in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.

```
┌──────────┐         ┌──────────┐
│  Main    │  ───▶   │          │
│  Menu    │         │Quick View│
└──────────┘         └──────────┘
```
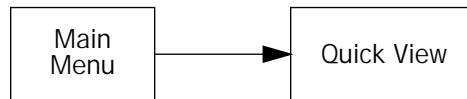
The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

Note: The status sections vary according to the interface of your Netopia D-Series.

General status

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

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

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


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


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

```

Current Date: The current date; this can be set with the Date and Time utility (see).

Default IP Gateway: The Netopia D-Series's default gateway, which must be manually configured. If you are using the Netopia D-Series's defaults this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

CPU Load: Percentage of the system's resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

IP Address: The Netopia D-Series's IP address, entered in the IP Setup screen.

MAC Address: The Netopia D-Series's hardware address, for each MAC layer interface.

Status lights

This section shows the current real-time status of the Netopia D-Series's status lights (LEDs). It is useful for remotely monitoring the Netopia D-Series's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the Netopia D-Series.

```
  -PWR-+-----WAN1------+--CON--AUX--+-----WAN2------+--EN--+--------LEDS---------
        LNK RDY CH1 Ch2    LNK  LNK    LNK RDY CH1 CH2  DATA │ '-'= Off 'G'= Green
     G   -   G   -   -     Y    -      -   -   -   -    -    │ 'R'= Red 'Y'= Yellow

```

Each LED representation can report one of four states:

–: A dash means the LED is off.

R: The letter "R" means the LED is red.

G: The letter "G" means the LED is green.

Y: The letter "Y" means the LED is yellow.

The section describes the meanings of the colors for each LED.

Statistics & Logs

```
┌──────────┐         ┌──────────────────┐         ┌────────────────────┐
│   Main   │────────▶│ Statistics & Logs│────────▶│ General Statistics │
│   Menu   │         │                  │         │                    │
└──────────┘         └──────────────────┘         └────────────────────┘
```

When you are troubleshooting your Netopia D-Series, the Statistics & Logs screens provide insight into the recent event activities of the Netopia D-Series.

From the Main Menu go to **Statistics & Logs** and select one of the options described in the sections below.

General Statistics

To go to the General Statistics screen, select **General Statistics** and press Return. The General Statistics screen appears.

```
                        General Statistics

  Physical I/F----Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
  Ethernet Hub    123456789  123456789  12345678  12345678  12345678  12345678
  Aux Sync        123456789  123456789  12345678  12345678  12345678  12345678
  IDSL 1          123456789  123456789  12345678  12345678  12345678  12345678




  Network---------Rx Bytes---Tx Bytes---Rx Pkts---Tx Pkts----Rx Err----Tx Err
  IP              123456789  123456789  12345678  12345678  12345678  12345678
```

The General Statistics screen displays information about data traffic on the Netopia D-Series's data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

■   Ethernet Hub

■   Aux Sync

■   IDSL 1 or SDSL 1

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted for the following protocols:

■   IP (IP packets on the Ethernet)

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

Rx Bytes. The number of bytes received

Tx Bytes. The number of bytes transmitted

Rx Packets: The number of packets received

Tx Pkts. The number of packets transmitted

Rx Err: The number of bad Ethernet packets received

Tx Err: An error occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

Event histories

The Netopia D-Series 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 Netopia D-Series's system and one for the WAN. The Netopia D-Series's built-in battery backup prevents loss of event history from a shutdown or reset.

The Netopia D-Series's event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History**. The WAN Event History screen appears.

Main Menu	→	Statistics & Logs	→	• WAN Event History • Device Event History

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

```
                              WAN Event History
                                 Current Date --  11/5/99
 11:48:19 AM
  -Date-----Time-----Event-------------------------------------------------------

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


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

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.

Ch.: The channel involved in the event.

Dir. Number: The directory number (number dialed) involved in the event (switched circuit models only).

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 **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.

To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

Device Event History

The Device Event History screen lists a total of 128 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.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.

```
                          Device Event History
                                    Current Date --  3/10/99 10:41:49 AM
    -Date-----Time-----Event------------------------------------------------
    ----------------------------------SCROLL UP----------------------------------
    03/10/99 10:22:48   Telnet connection up, address 192.168.1.2
    03/10/99 10:15:56 --BOOT: Cold start v4.6      -----------------------------
    03/09/99 16:43:07 --BOOT: Warm start v4.6      -----------------------------
    03/09/99 16:34:20 --BOOT: Cold start v4.6      -----------------------------
    03/09/99 11:10:12 --BOOT: Cold start v4.6      -----------------------------
    03/08/99 18:06:19   BOOT: Reverted to default configuration
    03/08/99 18:06:19 --BOOT: Warm start v4.6      -----------------------------




    ----------------------------------SCROLL DOWN---------------------------------
    Clear History...


    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 SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** 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 appears. Press Return or Escape to dismiss the dialog box.

To clear the Device Event History, select **Clear History** and press Return.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia D-Series DSL DSU.

From the Statistics & Logs menu select **System Information**. The System Information screen appears.

```
                         System Information

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

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

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

        AppleTalk Feature Set          Not Installed

        Analog Dial-In Kit             Installed


        IMUX Support                   Installed
```

Note: The information display varies by model, firmware version, feature set, and so on.

You can tell at a glance your particular system configuration.

SNMP

The Netopia D-Series includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

The Netopia D-Series supports the following management information base (MIB) documents:

■   MIB II (RFC 1213)

■   Interface MIB (RFC 1229)

■   Ethernet MIB (RFC 1643)

■   Netopia MIB

These MIBs are on the CustomerCare CD included with the Netopia D-Series. 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.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.

```
┌──────────┐        ┌──────────────┐        ┌──────────┐
│   Main   │───────▶│    System    │───────▶│          │
│   Menu   │        │ Configuration│        │   SNMP   │
└──────────┘        └──────────────┘        └──────────┘
```
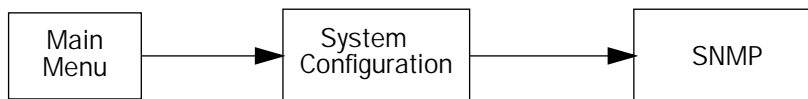
```
                           SNMP Setup


        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 D-Series's SNMP agent.

2. Select **System Location** and enter the Netopia D-Series's physical location (room, floor, building, etc.).

3. Select **System Contact** and enter the name of the person responsible for maintaining the Netopia D-Series.

System Name, System Location, and System Contact set the values returned by the Netopia D-Series 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 D-Series. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the Netopia D-Series, but cannot modify the Netopia D-Series'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.

Setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the Netopia D-Series. (The Netopia D-Series may still send SNMP Traps if those are properly enabled.)

This allows the administrator to block SNMP access to the Netopia D-Series, and to provide more granular control over the allowed SNMP operations to the Netopia D-Series.

■ Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the Netopia D-Series, but Get Requests and Get-Next Requests will still be honored using the Read-Only community string (assuming that is not the empty string).

■ Setting only the Read-Only community string to the empty string will *not* block Get Requests or Get-Next Requests since those operations (and Set Requests) are still allowed using the (non-empty) Read-Write community string.

Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia D-Series through SNMP. For more information on security issues, see "Security" on page 8-61.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia D-Series) 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 D-Series include the following:

■ An authentication failure trap is generated when the Netopia D-Series detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.

■ A cold start trap is generated after the Netopia D-Series is reset.

■ An interface down trap (ifDown) is generated when one of the Netopia D-Series's interfaces, such as a port, stops functioning or is disabled.

■ An interface up trap (ifUp) is generated when one of the Netopia D-Series's interfaces, such as a port, begins functioning.

The Netopia D-Series sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia D-Series. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.

```
                          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 **Continue** and press Return.

Chapter 8

Security

The Netopia D-Series 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 section covers the following topics:

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 D-Series and your network more secure:

■   Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.

■   Configure the Netopia D-Series through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia D-Series, no passwords are required to access the configuration screens. Anyone could tamper with the Netopia D-Series'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.

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 a screen requesting a name/password combination to access the Main Menu.

To set up user accounts, in the System Configuration screen select **Security** and press Return.

```
┌──────────────┐     ┌──────────────┐     ┌──────────────┐
│    Main      │ ──▶ │   System     │ ──▶ │   Security   │
│    Menu      │     │ Configuration│     │              │
└──────────────┘     └──────────────┘     └──────────────┘
```
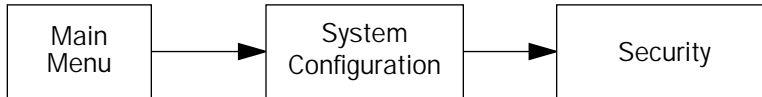
The Security Options screen appears.

```
                         Security Options




        Enable Telnet Console Access:                    Yes
        Enable Telnet Access to SNMP Screens:            Yes


        Show Users...
        Add User...
        Delete User...


        Password for This Screen (11 chars max):



  Return/Enter accepts * Tab toggles * ESC cancels.
  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 for 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. 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. The Add Name With Write Access screen appears.

```
                        Add Name With Write Access

        Enter Name:

        Enter Password (11 characters max):




        ADD NAME/PASSWORD NOW              CANCEL
```

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**. You are returned to the Security Options screen.

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 Escape.

Telnet access

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

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia D-Series if you suspect there is a chance of tampering.

To restrict Telnet access, select **Security** in the Advanced Configuration menu. The Security Options screen will appear. There are two levels of Telnet restriction available:

To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See "SNMP traps" on page 7-59.)

To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About filters and filter sets

Important Note: The Netopia D-Series's filter sets only work when the unit is in bridge mode. They have no effect when the unit is in DSU mode.

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 D-Series's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the Netopia D-Series'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 be either 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.

```
                              packet
                               ◯

        first
        filter
                                              no
                            match?          ─────────▶
                                              send
                                              to next
                                              filter
                            yes


                            pass or
                           discard?        ─────────▶
                                             discard
                                             (delete)

                            pass


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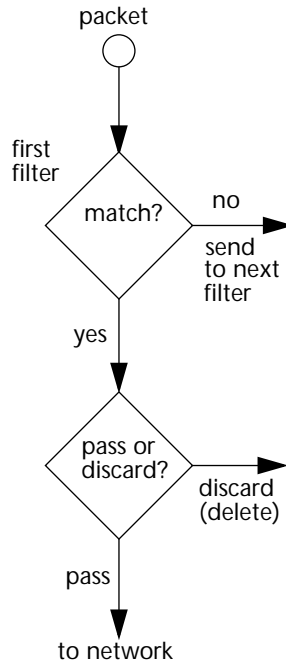
If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

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, 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.

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.

A filtering rule

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:

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 D-Series:

```
+-#--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 an IP filter.

Parts of an IP filter

There are two types if filters and filter sets: IP filters and Generic filters. The following discussion applies only to IP filters and filter sets.

An IP filter consists of criteria based on packet attributes. A typical IP 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

An IP filter can also match a packet's port number attributes. 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, an IP filter can be applied to selected 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

An IP 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 |
| 2   0.0.0.0           0.0.0.0          TCP   NC         =6000   Yes No |
| 3   0.0.0.0           0.0.0.0          ICMP  --         --      Yes Yes|
| 4   0.0.0.0           0.0.0.0          TCP   NC         >1023   Yes Yes|
| 5   0.0.0.0           0.0.0.0          UDP   NC         >1023   Yes Yes|
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
| +-------------------------------------------------------------------+ |
```

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 those protocols are used.

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), look at how a rule is translated into an IP 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.

   The Source IP Address Mask and Destination IP Address Mask fields indicate how many bits in the corresponding address the filter rule applies to.

   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

3. Using the tables on , find the destination port and protocol numbers (the 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   192.211.211.17   0.0.0.0          ANY   --        --      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           ANY   --        --      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 must 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 permitted is prohibited."

■   "That which is not expressly prohibited is permitted."

The first rule is far more secure, and is the best approach to filter design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and in the future.

Filtering tutorial

General filtering terms

Filter rule: A filter set is comprised of individual filter rules.

Filter set: A grouping of individual filter rules.

Firewall: A component or set of components that restrict access between a protected network and the Internet, or between two networks.

Host: A workstation on the network.

Packet: Unit of communication on the Internet.

Packet filter: Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.

Port: A number that defines a particular type of service.

Basic IP packet components

All IP packets contain the same basic header information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that an IP packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions. Generic filters can look into the data.

Basic protocol types

TCP: Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.

UDP: User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not retransmit the data. RFC 768 is the specification for UDP.

There are many more ports defined in the Assigned Addresses RFC. The tables on show some of these port assignments.

Filter Logic

Filter design is a test of logic, and filter rule ordering is critical. If a packet is passed through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not pass through the remainder of the filter rules.

For example, if you had the following filter set...

Allow WWW access;

Allow FTP access;

Allow SMTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first rule (WWW), go through the second rule (FTP), and match this rule; the packet is allowed through.

If you had this filter set for example....

Allow WWW access;

Allow FTP access;

Deny FTP access;

Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would pass through the first filter rule (WWW), match the second rule (FTP), and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine whether a packet matches a filter rule.

Logical AND function

When a packet is compared (in most cases) a logical AND function is performed. First the IP addresses and subnet masks are converted to binary and then combined with AND. The rules for the logical use of AND are as follows:

O AND O = O

O AND 1 = O

1 AND O = O

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255BINARY:11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15BINARY: 10100011.10110000.00000001.00001111

If you put the incoming packet and subnet mask together with AND, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied rules

With a given set of filter rules, there is an Implied rule that may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied rule is NO.
N+N+N=Y	If all filter rules are NO, the implied rule is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied rule is NO.

Established connections

The TCP header contains one bit called the ACK bit (or TCP Ack bit). This ACK bit appears only with TCP, not UDP. The ACK bit is part of the TCP mechanism that guaranteed the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set; once the TCP connection is in place, the remainder of the TCP packets with have the ACK bit set.

The ACK bit is helpful for filter design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, since these packets had to be originated from the local network.

Example IP Filter set screen

This is an example of the Netopia Filter set screen:

```
                    Change Input Filter 1
        Enabled:                    Yes
        Forward:                    No
        Type...                     IP

        Source IP Address:          0.0.0.0
        Source IP Address Mask:     0.0.0.0

        Dest. IP Address:           0.0.0.0
        Dest. IP Address Mask:      0.0.0.0

        Protocol Type:              TCP
        Source Port Compare...      No Compare
        Source Port ID:             0
        Dest. Port Compare...       Equal
        Dest. Port ID:              2000
        Established TCP Conns. Only:  No


 Return/Enter accepts * Tab toggles * ESC cancels.
 Enter the packet specific information for this filter.
```

Filter basics

In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

Example network
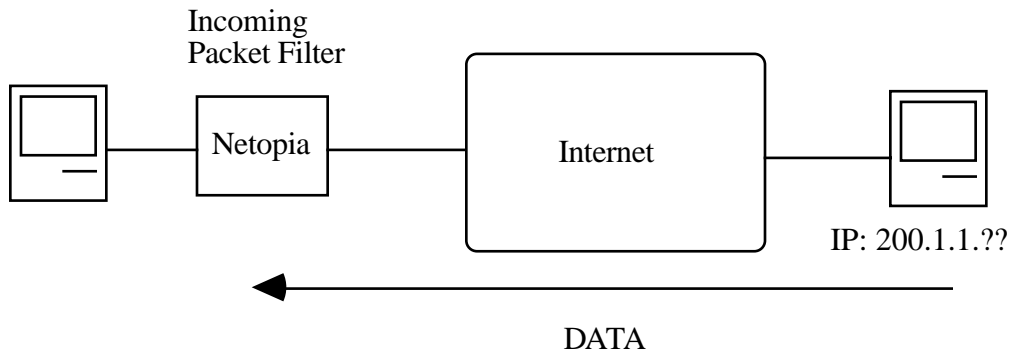
Example IP filters

Example 1

Write a filter rule that blocks the class C subnet represented by 200.1.1.0/25 from accessing the net.

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

To determine if the packet will match on the filter, perform a Boolean AND on the source IP address and the filter's source IP mask:

IP Address	Binary Representation of the last byte of the IP address	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	00000000	(Logical AND result)

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (whose last byte is binary 00000000) in the Netopia D-Series. This will *not* forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		

255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia D-Series. This rule *will* forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation of last byte	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	10110000	(Logical AND result)

Since the Source IP Network Address in the Netopia D-Series's filter rule is 01100000 (=96 decimal), and the source IP address after the logical AND is 1011000, this rule does *not* match and this packet will be passed.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104.

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		

255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia D-Series's filter rule is 01100000 (=96 decimal), and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be passed.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96.

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Netopia D-Series is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will NOT be passed. This rule masks off a *single* IP address.

Working with Filters and filter sets

This section covers Filters and filter sets.

```
┌──────────┐        ┌───────────────┐        ┌──────────┐
│   Main   │  ───►  │    System     │  ───►  │  Filter  │
│   Menu   │        │ Configuration │        │   Sets   │
└──────────┘        └───────────────┘        └──────────┘
```
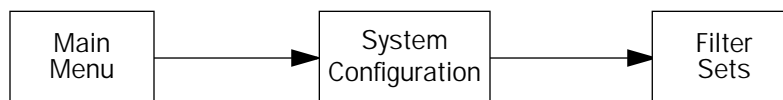
To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section "About filters and filter sets," beginning on page 8-64.

```
                            Filter Sets


                    Add Filter Set...
                    Display/Change Filter Set...
                    Delete Filter Set...












        Return/Enter to modify an existing Filter Set.
        Set Up IP Filter Sets (Firewalls) from this and the following Menus.
```
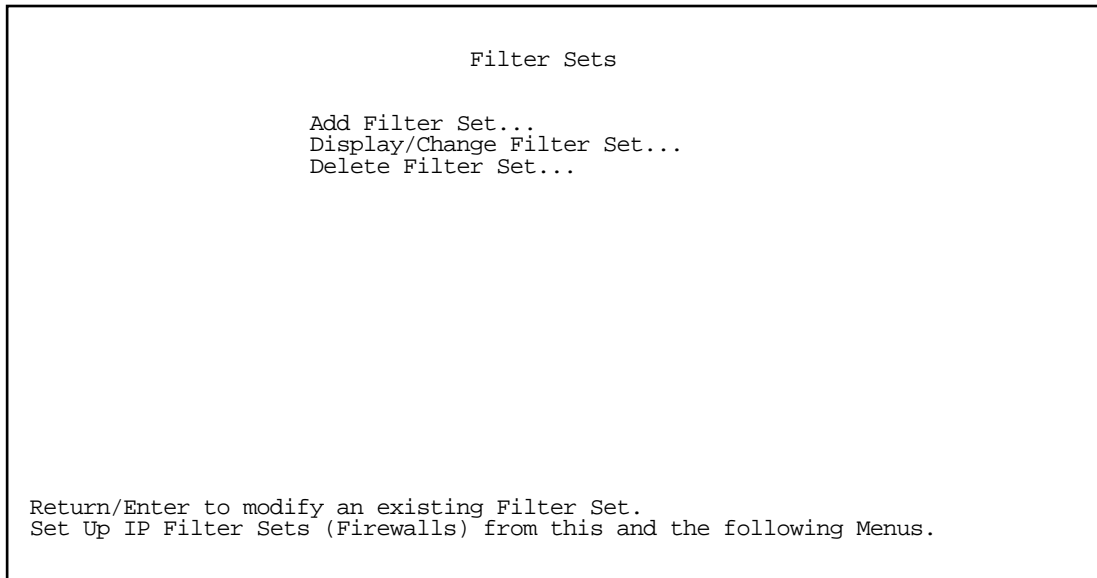
The procedure for creating and maintaining filter sets is as follows:

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 following sections explain how to execute these steps.

Adding a filter set

You can create up to 255 filter rules. You can use them in any combination of input or output in up to eight filter sets.

To add a new filter set, select **Add Filter Set** in the Filter Sets screen and press Return. The Add Filter Set screen appears.

```
                        Add Filter Set...

        Filter Set Name:                Filter Set  1




        ADD FILTER SET                  CANCEL

   Configure the Filter Set name and its associated Filters.
```

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 8-85). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 8-80).

To leave the Add Filter Set screen without saving the new filter set Select **CANCEL**. You are returned 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.
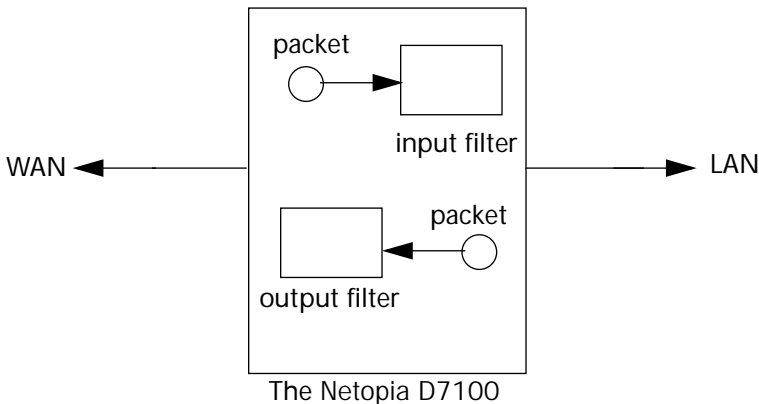
The Netopia D7100

Packets in the Netopia D-Series 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, navigate to the Display/Change Filter Set screen and select **Display/Change Filter Set**.
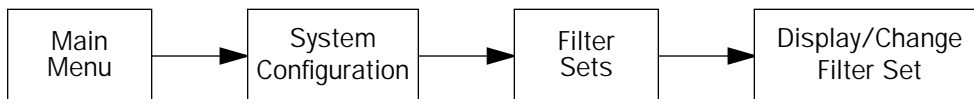
A popup menu displays a list of the filter sets you have created.

Select the one you want to edit.

The Display/Change Filter Set screen appears.

```
                        Display/Change Filter Set...


       Filter Set Name:                  Filter Set  1


                 Add Input Filter to Filter Set...
                 Display/Change Input Filter...
                 Delete Input Filter...
                 Move Input Filter...

                 Add Output Filter to Filter Set...
                 Display/Change Output Filter...
                 Delete Output Filter...
                 Move Output Filter...
```
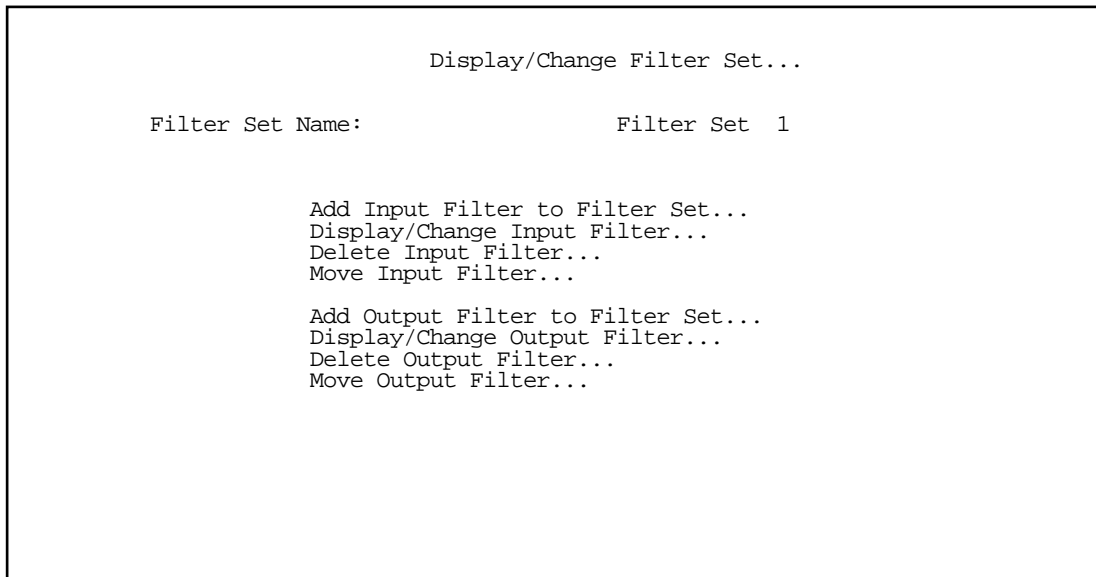
To add an input filter, select **Add Input Filter to Filter Set**.

The Add Filter screen appears. (To add an output filter, select **Add Output Filter**.)

```
                        Add Filter
           Enabled:                      Yes
           Forward:                      No
           Type...                       IP

           Source IP Address:            0.0.0.0
           Source IP Address Mask:       0.0.0.0

           Dest. IP Address:             0.0.0.0
           Dest. IP Address Mask:        0.0.0.0

           Protocol Type:                UDP
           Source Port Compare...        No Compare
           Source Port ID:               0
           Dest. Port Compare...         No Compare
           Dest. Port ID:                0


           ADD THIS FILTER NOW           CANCEL

  Return/Enter to set comparison of packet Port ID and Filter Port ID.
  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 **Type**. A popup menu offers the option of either IP or Generic. If you choose IP, continue with the next step. If you choose Generic filtering, skip to the section "Generic filters" on page 8-86.

    Warning: Changing the filter Type clears the filter values if any were previously entered.

4. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.

5. 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.

6. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.

7. 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.

8. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 8-68).

    Note: If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 9. and 10. will appear. These settings only take effect if the Protocol Type is TCP or UDP.

9. 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 8-67).

10. 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 8-67).

11. 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 and return to the Add Filter Set screen.

Moving filters

The Move Input/Output Filter permits reordering of rules in a filter set.

```
+#----Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+---------------------------------------------------------------------+
| 1    1.1.1.1          0.0.0.0          ANY   --       --      Yes No |
| 2    000000000000     000000000000     0     =        No      Yes No |
| 3    4.4.4.4          0.0.0.0          ANY   --       --      Yes No |
| 4    3.3.3.3          0.0.0.0          ANY   --       --      Yes No |
| 5    5.5.5.5          0.0.0.0          ANY   --       --      Yes No |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
|                                                                     |
+---------------------------------------------------------------------+

  Arrows move filter. RETURN/ENTER to accept new filter location. ESC aborts.
```

All operations are done from a single popup.

■   In the Display/Change Filter Set screen, select **Move Input Filter** (or **Move Output Filter**). A selection mode popup appears. In this mode you scroll to the rule you want to move and press Return on a rule to select it for moving.

The help text tells you what is expected.

■   After pressing Return you are in Move mode. Arrow keys move the selected rule up or down. When you press Return again the rule is put in the new location permanently and the popup is dismissed. You can press Escape at any time in the popup to abort the move and restore the filter set to its original ordering.

Viewing filters

To display a view-only table of input (output) filters, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Display/Change Filter Set screen.

Modifying filters

To modify a filter, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Display/Change Filter Set screen to display a table of filters.

Select a filter from the table and press Return. The Change Filter screen appears. The parameters in this screen are set in the same way as the ones in the Add Filter screen (see "Adding filters to a filter set" on page 8-80).

```
                          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** or **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 Escape to exit the table without deleting the filter.

Viewing filter sets

To display a view-only list of filter sets, select **Display/Change Filter Set** in the 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. The Change Filter Set screen appears. 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 8-80).

```
                    Display/Change Filter Set...


   Filter Set Name:                 Filter Set  1


                  Add Input Filter to Filter Set...
                  Display/Change Input Filter...
                  Delete Input Filter...
                  Move Input Filter...

                  Add Output Filter to Filter Set...
                  Display/Change Output Filter...
                  Delete Output Filter...
                  Move 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, before deleting the current filter set you'll have to note their configuration and then recreate them.

To delete a filter set, select **Delete 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 delete it. Press Escape to exit the list without deleting the filter set.

Generic filters

If you chose Generic filtering in step 3. on page 8-82, the Add Filter screen changes as shown:

```
                          Add Filter
          Enabled:                     Yes
          Forward:                     No
          Type...                      Generic

          Value:                       000000000000
          Mask:                        000000000000
          Offset:                      0

          Compare:                     Equal

          Chain to Next Filter:        No




          ADD THIS FILTER NOW          CANCEL

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

Note: Generic filters are more complicated to use than IP filters. If you plan to filter only IP traffic, we recommend that you use IP filters instead.

Generic filters are performed on packets as a whole, after layer 2 encapsulation is removed (ATM-FUNI or Frame Relay). You configure them in much the same way as the IP version.

■   The **Value** and **Mask** fields can be 8 bytes in length, two characters per byte, so for example a MAC address is 6 bytes: 00-00-C5-60-34-74.

   The Value, Mask, and Offset are used together to determine if the packet matches the filter. The Value is logically ANDed with the Mask; the Offset specifies the number of bytes into the packet where the Value ANDed with the Mask must be present. If these match, the filter matches the packet.

■   Several Generic Filters can be ANDed together by toggling **Chain to Next Filter** to Yes. In this case all the filters chained must match the packet, and the last filter in the chain determines the Forwarding decision. The Compare field works as it does in the Filter version

About generic filters

One of the more difficult aspects of writing Generic filter sets is determining how many bytes into the packet (the Offset) the value you want to test is. In order to find the Offset value a good understanding of packet formats is helpful. The following figure depicts a typical packet format structure for purposes of this example.

Destination Address	Source Address	Frame Type	Frame Data	CRC
6 octets	6 octets	2 octets	64 - 1500 octets	4 octets

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Source Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Destination Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                       IP Header Format
        Note that one tick mark represents one bit position.


 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Acknowledgment Number                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                                |
| Offset| Reserved  |R|C|S|S|Y|I|            Window              |
|       |           |G|K|H|T|N|N|                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                       TCP Header Format
        Note that one tick mark represents one bit position.
```
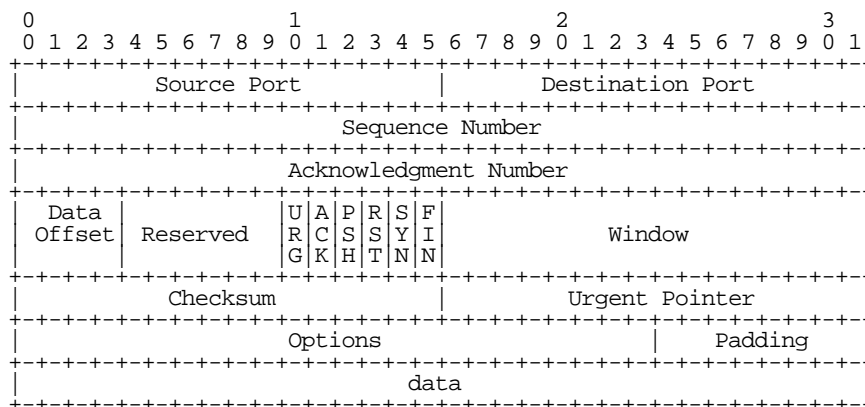
Observe that the first six bytes of the packet (frame) are used to indicate the destination MAC address and the next six are used define the source MAC address. So, for example, to write a Generic filter set that would block all incoming traffic to Mac address 00-00-c8-e3-95 you could create a filter rule like this:

```
                          Add Input Filter
              Enabled:                        Yes
              Forward:                        No
              Type...                         Generic

              Value:                          0000C8E395000000
              Mask:                           FFFFFFFFFF000000
              Offset:                         6

              Compare:                        Equal

              Chain to Next Filter:           No




              ADD THIS FILTER NOW             CANCEL

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

Note the Offset is set to look at a value six bytes into the packet, the Value is 0000C8E395000000 and the Mask is set to match only the hexidecimal digits we're interested in -- the ones that represent the MAC address.

■ The next item that's commonly evaluated in a Generic filter is the frame type. The frame type is located at an offset of twelve bytes. For IP packets it has a value of 0800 (hex) and for ARP the value is 0806 (hex). So a filter set summary to block all incoming IP and ARP packets looks like this:

```
    +-#----Value------------Mask-------------Offst-Compare--Chain---On?-Fwd-+
    +----------------------------------------------------------------------+
    | 1    0800000000000000  FFFF000000000000  12      =        No     Yes No |
    | 2    0806000000000000  FFFF000000000000  12      =        No     Yes No |
    |                                                                      |
    |                                                                      |
```

A filter set blocking all incoming IPX requires two filter rules. One to verify the byte with offset of 12 bytes is less than 600 (hex) ANDed (chained with) a filter that verifies the byte offset by 14 is not equal to FFFF.

■ The filter set should look like this (with the first filter rule's chain field set to "Yes" because the packet has to match both rules to be qualified as an IPX packet.)

```
    +-#----Value------------Mask-------------Offst-Compare--Chain---On?-Fwd-+
    +----------------------------------------------------------------------+
    | 1    0600000000000000  FFFF000000000000  12      <        Yes    Yes    |
    | 2    FFFF000000000000  FFFF000000000000  14      =        No     Yes No |
    |                                                                      |
    |                                                                      |
```

The following example further illustrates filter rule chaining, different sized masks and the full 8 bytes of the Value field.

Create a filter set designed to block telnet access from a given external node (the example below uses 176.163.52.18) to a given internal node (176.163.107.254).

The filter rule summary (input) should look like this:

```
+-#----Value------------Mask-------------Offst-Compare--Chain---On?-Fwd-+
+----------------------------------------------------------------------+
|  1   0500000000000000  0F00000000000000  14    =         No      Yes No |
|  2   0800000000000000  FFFF000000000000  12    =         Yes     Yes    |
|  3   0600000000000000  FF00000000000000  23    =         Yes     Yes    |
|  4   B0A33412B0A3B0FE  FFFFFFFFFFFFFFFF  26    =         Yes     Yes    |
|  5   0017000000000000  FFFF000000000000  36    =         No      Yes No |
```

- Filter #1 checks that the IHL has a size of 5. This is a useful security check to verify a potential hacker has not padded the packet with options that would then throw off following filter rule checks on bytes further into the packet.

- Filter #2 checks the incoming packet is IP.

- Filter #3 checks that the packet is using TCP.

- Filter #4 simultaneously checks the source IP address is 176.163.52.18 (= B0A33412 in hex) and the destination IP address is 176.163.107.254 (= B0A3B0FE in hex).

- Filter #5 checks the TCP port address is telnet (= 23 decimal = 17 hex).

Note: This filter set is presented only to illustrate how Generic filtering works. You are strongly advised to actually use IP filters to block IP only traffic.

Chapter 9

Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes.

This section covers the following topics:

Note: These utilities and tests are accessible only through the console-based management screens. See Chapter 5, "Console-Based Management," for information on accessing the console-based management screens.

You access the **Utilities & Diagnostics** screens from the **Main Menu**.

```
            Utilities & Diagnostics


        Ping...
        Trace Route...
        Telnet...


        Disconnect Telnet Console Session...

        Trivial File Transfer Protocol (TFTP)...
        X-Modem File Transfer...


        Revert to Factory Defaults...

        Restart System...
```

Ping

The Netopia D-Series 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 D-Series. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

In the Utilities & Diagnostic screen, select **Ping** and press Return. The ICMP Ping screen appears.

```
                              ICMP Ping

          Name of Host to Ping:
          Packets to Send:                  5
          Data Size:                        56
          Delay (seconds):                  1

                              START PING


          Status:

          Packets Out:                      0
          Packets In:                       0
          Packets Lost:                     0 (0%)
          Round Trip Time
            (Min/Max/Avg):                  0.000 / 0.000 / 0.000 secs



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

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 can 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 can 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 can 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 Escape.

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 status messages shown in the table below:

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 that follows, a Netopia D-Series 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 D-Series before the third Ping packet is sent. The first and third return Ping packets are on time.
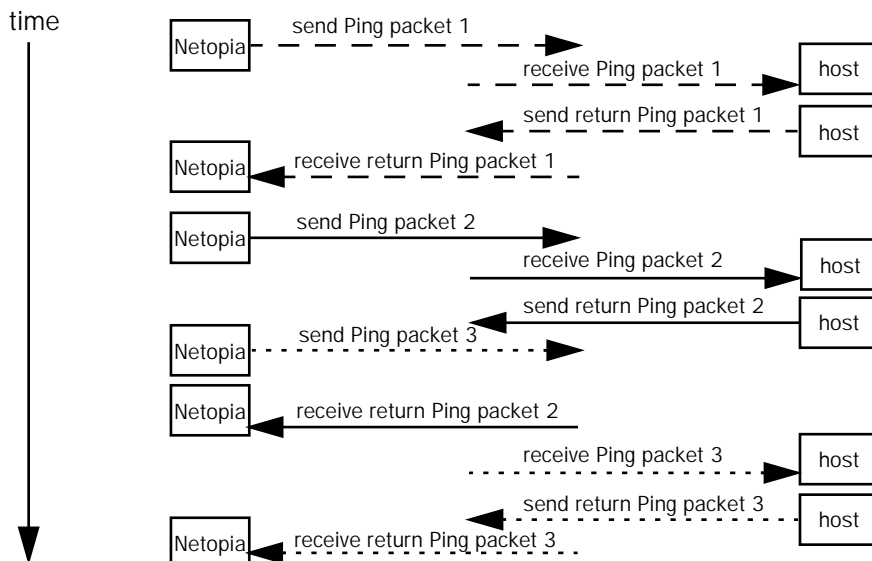
Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** 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 D-Series 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 on the previous page). 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.

Trace Route

You can count the number of routers between your Netopia D-Series and a given destination with the Trace Route utility.

In the Statistics & Diagnostics screen, select **Trace Route** and press Return. The Trace Route screen appears.

```
                        Trace Route

        Host Name or IP Address:

        Maximum Hops:                    30
        Timeout (seconds):               5

        Use Reverse DNS:                 Yes


                     START TRACE ROUTE







    Enter the IP Address/Domain Name of a host.
    Trace route to a network host.
```

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** to set the maximum number of routers to count between the Netopia D-Series and the destination router, up to the maximum of 64. The default is 30 hops.

3. Select **Timeout (seconds)** 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 D-Series and the destination router. The default is Yes.

5. Select **START TRACE ROUTE** and press Return. A scrolling screen will appear that lists the destination, number of hops, IP addresses of each hop, and DNS names, if selected.

6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Telnet client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.

```
                            Telnet
            Host Name or IP Address:

            Control Character to Suspend:      Q


                        START A TELNET SESSION









     Enter the IP Address/Domain Name of a host.


```

■ Enter the host name or the IP address in dotted decimal format of the machine you want to telnet into and press Return.

■ Either accept the default control character "Q" used to suspend the Telnet session, or type a different one.

■ **START A TELNET SESSION** becomes highlighted.

■ Press Return and the Telnet session will be initiated.

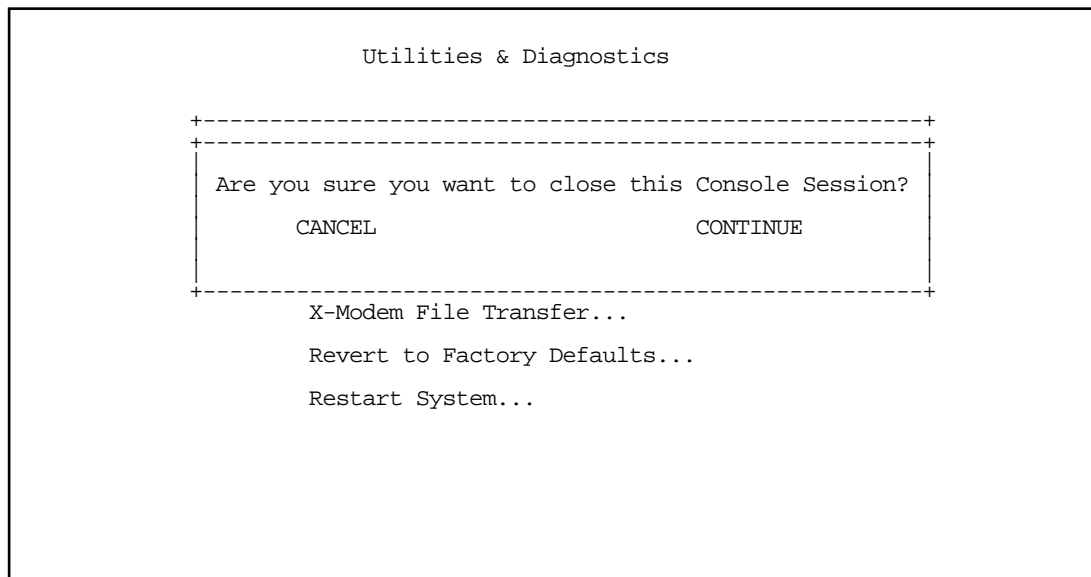■ To suspend the session, press Control-Q, or whatever other control character you specified.

   Two new options will appear in the Telnet screen (not shown):

   Resume Suspended Session – select this one if you want to go back to your Telnet session

   Terminate Suspended Session – select this one if you want to end the session

Disconnect Telnet console session

If you want to close your Telnet Console session, select **Disconnect Telnet Console Session** and press Return. A dialog box appears asking you to cancel or continue your selection.

```
                        Utilities & Diagnostics


          +------------------------------------------------------+
          +------------------------------------------------------+
          |                                                      |
          |  Are you sure you want to close this Console Session? |
          |          CANCEL                         CONTINUE     |
          |                                                      |
          |                                                      |
          +------------------------------------------------------+
                      X-Modem File Transfer...

                      Revert to Factory Defaults...

                      Restart System...
```

If you select **Continue**, you will immediately terminate your session.

Factory defaults

You can reset the Netopia D-Series to its factory default settings. In the Utilities & Diagnostics screen, select **Revert to Factory Defaults** and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia D-Series will reboot and its settings will return to the factory defaults, deleting your configurations.

If you lose your password and are unable to access the console screens, you can manually reset the Netopia D-Series in an emergency. See "How to reset the Netopia D-Series to factory defaults," in Appendix A, "Trouble-shooting."

Note: Reset to factory defaults with caution. You will need to reconfigure all of your settings in the Netopia D-Series.

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 Netopia D-Series as the client. To use the Netopia D-Series as a TFTP client, a TFTP server must be available. Netopia, Inc. has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return. The Trivial File Transfer Protocol (TFTP) screen appears.

```
                    Trivial File Transfer Protocol (TFTP)


        TFTP Server Name:


        Firmware File Name:

        GET ROUTER FIRMWARE FROM SERVER...
        GET WAN MODULE FIRMWARE FROM SERVER...


        Config File Name:

        GET CONFIG FROM SERVER...
        SEND CONFIG TO SERVER...


        TFTP Transfer State -- Idle

        TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Netopia D-Series's firmware and how to download and upload configuration files.

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

There are two types of firmware in the Netopia D-Series DSL DSU: router firmware and WAN module firmware. The router firmware governs how the Netopia D-Series communicates with your network and the WAN module; the WAN module firmware governs how the WAN module communicates with the remote site. WAN module firmware is included on your CustomerCare CD for XMODEM transfer and later updates will be available on the Netopia website. Router firmware updates are also periodically posted on the Netopia website.

To update either the Netopia D-Series's or the internal WAN module's firmware, follow these steps:

■   Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

■   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).

■   Select **GET ROUTER FIRMWARE FROM SERVER** or **GET WAN MODULE FIRMWARE FROM SERVER** and

press Return. You will see the following dialog box:
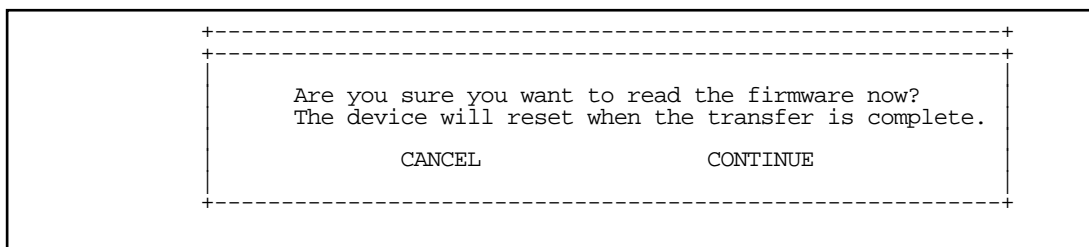
```
        +-----------------------------------------------------------+
        +-----------------------------------------------------------+
        |                                                           |
        |        Are you sure you want to read the firmware now?     |
        |        The device will reset when the transfer is complete.|
        |                                                           |
        |           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 firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

■   Be sure the firmware update you load onto your Netopia D-Series is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.

■   Do not manually power down or reset the Netopia D-Series while it is automatically resetting or it could be damaged.

■   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 Netopia D-Series can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the Netopia D-Series's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

■   Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

■   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).

■ Select **GET CONFIG FROM SERVER** and press Return. You will see the following dialog box:
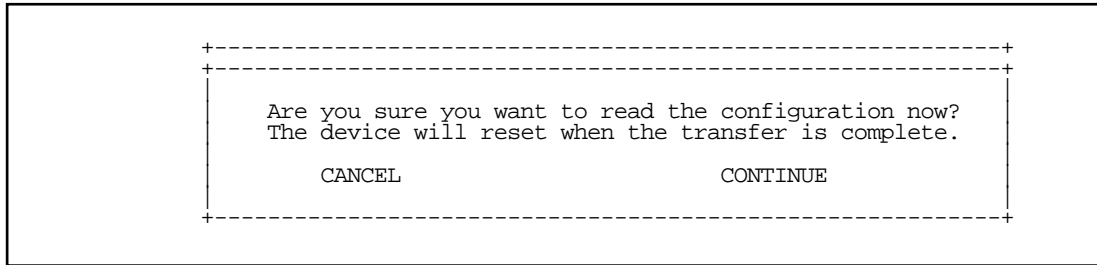
```
+------------------------------------------------------------+
+------------------------------------------------------------+
|                                                            |
|      Are you sure you want to read the configuration now?  |
|      The device will reset when the transfer is complete.  |
|                                                            |
|          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.

■ 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 Netopia D-Series's current configuration to a TFTP server. The file can then be downloaded by a different Netopia D-Series unit to configure its parameters (see "Downloading configuration files" on page 9-98). 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 D-Series unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server 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. Netopia will begin to transfer the file.

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.

Transferring configuration and firmware files with XMODEM

You can transfer configuration and firmware files with XMODEM through the Netopia D-Series's console port. Be sure your terminal emulation program supports XMODEM file transfers.

To go to the **X-Modem File Transfer** screen, select it in the Utilities & Diagnostics menu.

Note: The X-Modem File Transfer screen is only available if you are connected via the Console port.

```
                        X-Modem File Transfer

      Send Firmware to Netopia...

      Send Config to Netopia...

      Receive Config from Netopia...


      Send Firmware to Netopia WAN module...

      WAN module Firmware Status:              IDLE
```

Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administration. The procedure below applies whether you are using the console or the WAN interface module.

Follow these steps to update the Netopia D-Series'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** (or **Send Firmware to Netopia WAN module**) and press Return. The following dialog box appears:

```
   +-------------------------------------------------------------------+
   +-------------------------------------------------------------------+
   |                                                                   |
   |   Are you sure you want to send a firmware file to your Netopia?  |
   |   If so, when you hit Return/Enter on the CONTINUE button, you will|
   |   have 10 seconds to begin the transfer from your terminal program.|
   |                                                                   |
   |          CANCEL                              CONTINUE             |
   |                                                                   |
   +-------------------------------------------------------------------+
```

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 power down or reset the Netopia D-Series while it is automatically resetting or it could be damaged.

Downloading configuration files

The Netopia D-Series can be configured by downloading a configuration file. The downloaded file reconfigures all of the Netopia D-Series'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).

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:
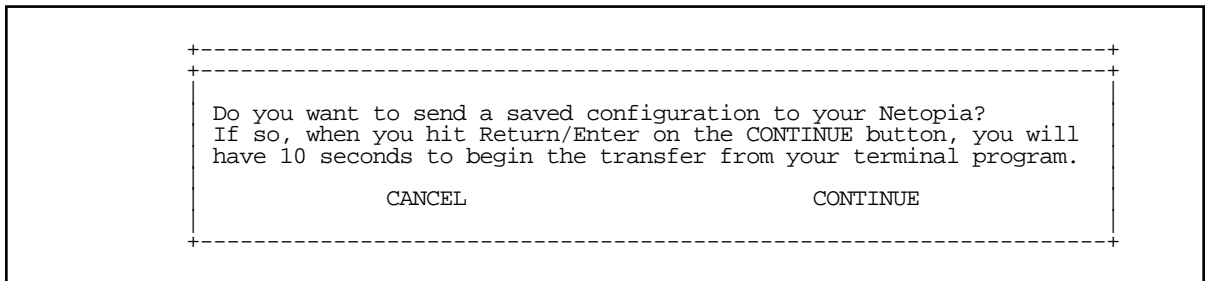
```
+---------------------------------------------------------------------+
+---------------------------------------------------------------------+
|                                                                     |
|  Do you want to send a saved configuration to your Netopia?         |
|  If so, when you hit Return/Enter on the CONTINUE button, you will   |
|  have 10 seconds to begin the transfer from your terminal program.  |
|                                                                     |
|          CANCEL                              CONTINUE               |
|                                                                     |
+---------------------------------------------------------------------+
```

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 D-Series's current configuration can be uploaded from the Netopia D-Series to disk. The file can then be downloaded by a different Netopia D-Series to configure its parameters (see "Downloading configuration files," above). 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 D-Series by Netopia or your network administrator.

The procedure below applies whether you are using the console or the WAN interface. 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:

```
+--------------------------------------------------------------------+
|                                                                    |
|     Are you sure you want to save your current Netopia configuration? |
|     If so, when you hit Return/Enter on the CONTINUE button, you will |
|     have 10 seconds to begin the transfer from your terminal program. |
|                                                                    |
|           CANCEL                              CONTINUE             |
|                                                                    |
+--------------------------------------------------------------------+
```
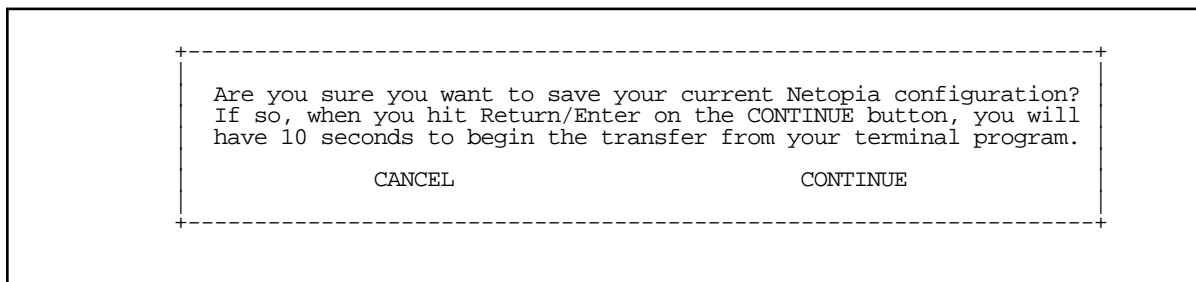
3. Select **CANCEL** to exit without uploading the file, or select **CONTINUE** to upload the file.

    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.

Restarting the system

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Netopia D-Series and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

Part III: Appendixes

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using the Netopia D-Series. It also includes information on how to contact Netopia Technical Support.

Important information on these problems can be found in the event histories kept by the Netopia D-Series. These event histories can be accessed in the Statistics & Logs screen.

This section covers the following topics:

■   "Configuration problems" on page A-105

■   "How to reset the Netopia D-Series to factory defaults" on page A-107

■   "Power outages" on page A-107

■   "Technical support" on page A-108

Configuration problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1.   The computer's connection to the Netopia D-Series

2.   The Netopia D-Series's connection to the telecommunication line(s)

3.   The telecommunication line's connection to your ISP

4.   The ISP's connection to the Internet

If the connection from the computer to the Netopia D-Series was not successful, verify that the following conditions are in effect:

■   The Netopia D-Series is turned on.

■   An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia D-Series.

■   Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as "c:\windows\telnet.exe".)

■   Your PC or Macintosh is properly configured for TCP/IP.

■   Your PC or Macintosh has an IP address.

■   Your PC or Macintosh has a subnet mask that matches or is compatible with the Netopia D-Series's subnet mask.

Note: If you are attempting to modify the IP address or subnet mask from a previous, successful configuration attempt, you will need to clear the IP address or reset your Netopia D-Series to the factory default before reinitiating the configuration process. For further information on resetting your Netopia D-Series to factory default, see "Factory defaults" on page 9-96.

Console connection problems

Can't see the configuration screens (nothing appears)

■ Make sure the cable connection from the Netopia D-Series's console port to the computer being used as a console is securely connected.

■ Make sure 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 or the ▲ up or down▼ key several times to refresh the terminal screen.

■ Make sure 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. The default values are 9600, N, 8, and 1.

Characters are missing from some of the configuration screens

■ Try changing the Netopia D-Series's default speed of 9600 bps and setting your terminal emulation software to match the new speed.

Network problems

This section contains tips for troubleshooting 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 D-Series's Ping utility, in the Utilities & Diagnostics screen, and try to ping local and remote hosts. See *"Ping" on page 9-92* 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.netopia.com, for example), verify that the DNS server's IP address is correct and that it is reachable from the Netopia D-Series (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. See *"Statistics & Logs" on page 7-53* for more information.

How to reset the Netopia D-Series to factory defaults

Lose your password? This section shows how to reset the Netopia D-Series so that you can access the console screens once again. Keep in mind that all of your connection profiles and settings will need to be reconfigured.

If you don't have a password, the only way to get back into the Netopia D-Series is the following:

1. Turn the Netopia D-Series upside down.

2. Referring to the diagram below, find the paper clip size Reset Switch slot.
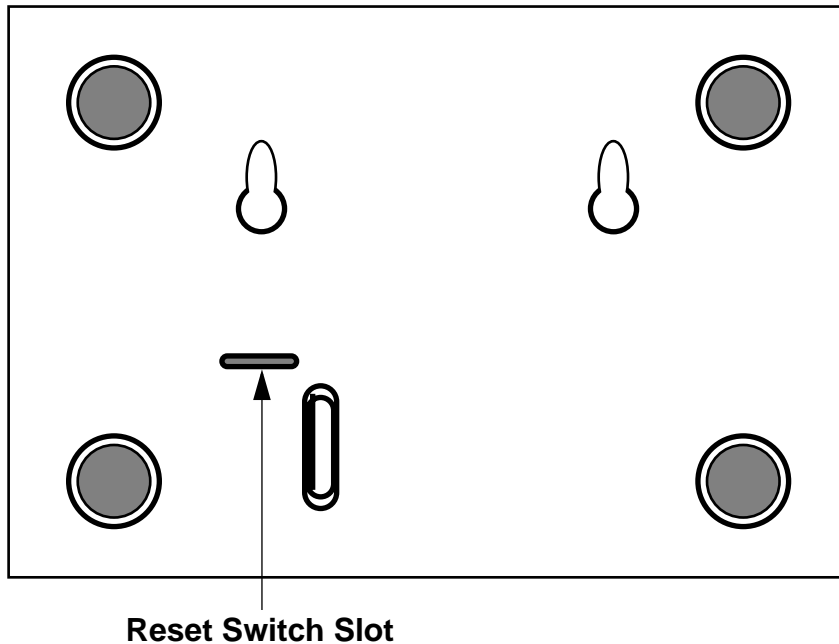
Reset Switch Slot

3. Carefully insert the larger end of a standard size paper clip until you contact the internal Reset Switch. (No need to unwind the paper clip.)

4. Press this switch.

5. This will reset the unit to factory defaults and you will now be able to reprogram the Netopia D-Series.

Power outages

If you suspect that power was restored after a power outage and the Netopia D-Series is connected to a remote site, you may need to switch the Netopia D-Series off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the Netopia D-Series should reestablish the connection.

Technical support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Netopia

Look in this 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 Netopia technical support.

Environment profile

■ Locate the Netopia D-Series's model number, product serial number, and firmware version. The serial number is on the bottom of the Netopia D-Series, along with the model number. The firmware version appears in the Netopia D-Series'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 Netopia Technical Support with the information you used to configure the Netopia D-Series. 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 Netopia Customer Service by e-mail, telephone, fax, or post:

Internet: techsports@netopia.com (for technical support)
info@netopia.com (for general information)

Phone: 1 800-782-6449
Fax: 1 510-814-5023

Netopia, Inc.
Customer Service
2470 Mariner Square Loop
Alameda, California 94501
USA

Netopia Bulletin Board Service: 1 510-865-1321

Online product information

Product information can be found in the following:

Netopia World Wide Web server via http://www.netopia.com
Internet via anonymous FTP to ftp.netopia.com/pub

FAX-Back

This service provides technical notes that answer the most commonly asked questions, and offers solutions for many common problems encountered with Netopia products.

FAX-Back: +1 510-814-5040

Appendix B

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Table 1:

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110

Table 1:

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Table 2:

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001

Table 2:

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110
159	10011111	191	10111111	223	11011111	255	11111111

Appendix C

Further Reading

Alexander, S. & R. Droms, *DHCP Options and BOOTP Vendor Extensions*, RFC 2131, Silicon Graphics, Inc., Bucknell University, March 1997.

Angell, David. *ISDN for Dummies* Foster City, CA: IDG Books Worldwide, 1995. Thorough introduction to ISDN for beginners.

Apple Computer, Inc. *AppleTalk Network System Overview*. Reading, MA: Addison-Wesley Publishing Company, Inc., 1989.

Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, MA: Addison-Wesley Publishing Company, Inc., 1991.

Asymmetric Digital Subscriber Line (ADSL) Forum, *Framing and Encapsulation Standards for ADSL: Packet Mode*, TR-003, June 1997.

Black, U. *Data Networks: Concepts, Theory and Practice*. Englewood Cliffs, NJ: Prentice Hall, 1989.

Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, CA: IEEE Computer Society Press, 1988.

Black, Uyless. *Emerging Communications Technologies* Englewood Cliffs, NJ: PTR Prentice Hall, 1994. Describes how emerging communications technologies, including ISDN and Frame Relay, operate and where they fit in a computer/communications network.

Bradley, T., C. Brown & A. Malis, *Multiprotocol Interconnect over Frame Relay*, Network Working Group, Internet Engineering Task Force, RFC 1490, July 1993.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Introduction to the Simple Gateway Monitoring Protocol." *IEEE Network*: March 1988.

Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Network Management and the Design of SNMP." *ConneXions: The Interoperability Report*, Vol. 3: March 1989.

Chapman, D. Brent. "Network (In)Security Through IP Packet Filtering" Paper available from Great Circle Associates, 1057 West Dana Street, Mountain View, CA 94041.

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.

Chappell, L. *Novell's Guide to NetWare LAN Analysis*. San Jose, CA: Novell Press, 1993.

Clark, W. "SNA Internetworking." *ConneXions: The Interoperability Report*, Vol. 6, No. 3: March 1992.

Comer, D.E. *Internetworking with TCP/IP: Principles, Protocols, and Architecture* Vol. I, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1991.

Copper Mountain Networks, Internal Control Protocol (ICP) Interface Control Document (ICD), January 5, 1998.

Davidson, J. *An Introduction to TCP/IP*. New York, NY: Springer-Verlag, 1992.

Droms, R., *Dynamic Host Configuration Protocol*, RFC 2131, Bucknell University, March 1997.

Ferrari, D. *Computer Systems Performance Evaluation*. Englewood Cliffs, NJ: Prentice Hall, 1978.

Garcia-Luna-Aceves, J.J. "Loop-Free Routing Using Diffusing Computations." Publication pending in IEEE/ACM Transactions on Networking, Vol. 1, No. 1, 1993.

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.

Green, J.K. *Telecommunications*, 2nd ed. Homewood, IL: Business One Irwin, 1992.

Heinanen, J., *Multiprotocol Encpasulation over ATM Adaptation Layer 5*, RFC 1483, July 1993.

Jones, N.E.H., and D. Kosiur. *MacWorld Networking Handbook*. San Mateo, CA: IDG Books Worldwide, Inc., 1992.

Kousky, K. "Bridging the Network Gap." *LAN Technology*, Vol. 6, No. 1: January 1990.

LaQuey, Tracy. *The Internet Companion: A Beginner's Guide to Global Networking* Reading, MA: Addison-Wesley Publishing Company, 1994.

Leinwand, A., and K. Fang. *Network Management: A Practical Perspective*. Reading, MA: Addison-Wesley Publishing Company, 1993.

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.

Lippis, N. "The Internetwork Decade." *Data Communications*, Vol. 20, No. 14: October 1991.

McNamara, J.E. *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, 12 Crosby Drive, Bedford, MA 01730.

Malamud, C. *Analyzing Novell Networks*. New York, NY: Van Nostrand Reinhold, 1991.

Malamud, C. *Analyzing Sun Networks*. New York, NY: Van Nostrand Reinhold, 1991.

Martin, J. *SNA: IBM's Networking Solution*. Englewood Cliffs, NJ: Prentice Hall, 1987.

Martin, J., with K.K. Chapman and the ARBEN Group, Inc. *Local Area Networks: Architectures and Implementations*. Englewood Cliffs, NJ: Prentice Hall, 1989.

Miller, A. Mark. *Analyzing Broadband Networks (Frame Relay, SMDS, & ATM)* M&T Books, San Mateo, CA, 1994. An intermediate/advanced reference on Frame Relay technologies.

Miller, M.A. *Internetworking: A Guide to Network Communications LAN to LAN; LAN to WAN*, 2nd. ed. San Mateo, CA: M&T Books, 1992.

Miller, M.A. *LAN Protocol Handbook*. San Mateo, CA: M&T Books, 1990.

Miller, M.A. *LAN Troubleshooting Handbook*. San Mateo, CA: M&T Books, 1989.

Perlman, R. *Interconnections: Bridges and Routers*. Reading, MA: Addison-Wesley Publishing Company, 1992.

Rose, M.T. *The Open Book: A Practical Perspective on OSI*. Englewood Cliffs, NJ: Prentice Hall, 1990.

Rose, M.T. *The Simple Book: An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, NJ: Prentice Hall, 1991.

Schwartz, M. *Telecommunications Networks: Protocols, Modeling, and Analysis*. Reading, MA: Addison-Wesley Publishing Company, 1987.

Sherman, K. *Data Communications: A User's Guide*. Englewood Cliffs, NJ: Prentice Hall, 1990.

Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer. *Inside AppleTalk,* 2nd ed. Reading, MA: Addison-Wesley Publishing Company, 1990.

Siyan, Karanjit. *Internet Firewall and Network Security* Indianapolis, IN: New Riders Publishing, 1995. Similar to the Chapman and Zwicky book.

Smith, Philip. *Frame Relay Principles and Applications* Reading, MA: 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.

Spragins, J.D., et al. *Telecommunications Protocols and Design.* Reading, MA: Addison-Wesley Publishing Company, 1991.

Stallings, W. *Data and Computer Communications.* New York, NY: Macmillan Publishing Company, 1991.

Stallings, W. *Handbook of Computer-Communications Standards,* Vols. 1–3. Carmel, IN: Howard W. Sams, 1990.

Stallings, W. *Local Networks*, 3rd ed. New York, NY: Macmillan Publishing Company, 1990.

Stevens, W.R. *TCP/IP Illustrated*, Vol 1. Reading, MA: Addison-Wesley Publishing Company, 1994.

Sunshine, C.A. (ed.). *Computer Network Architectures and Protocols*, 2nd ed. New York, NY: Plenum Press, 1989.

Tannenbaum, A.S. *Computer Networks*, 2nd ed. Englewood Cliffs, NJ: Prentice Hall, 1988.

Terplan, K. *Communication Networks Management.* Englewood Cliffs, NJ: Prentice Hall, 1992.

Tsuchiya, P. "Components of OSI: IS-IS Intra-Domain Routing." *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.

Tsuchiya, P. "Components of OSI: Routing (An Overview)." *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.

Zimmerman, H. "OSI Reference Model–The ISO Model of Architecture for Open Systems Interconnection." *IEEE Transactions on Communications COM-28*, No. 4: April 1980.

Appendix D

Technical Specifications and Safety Information

Pinouts for V.35 DCE cable
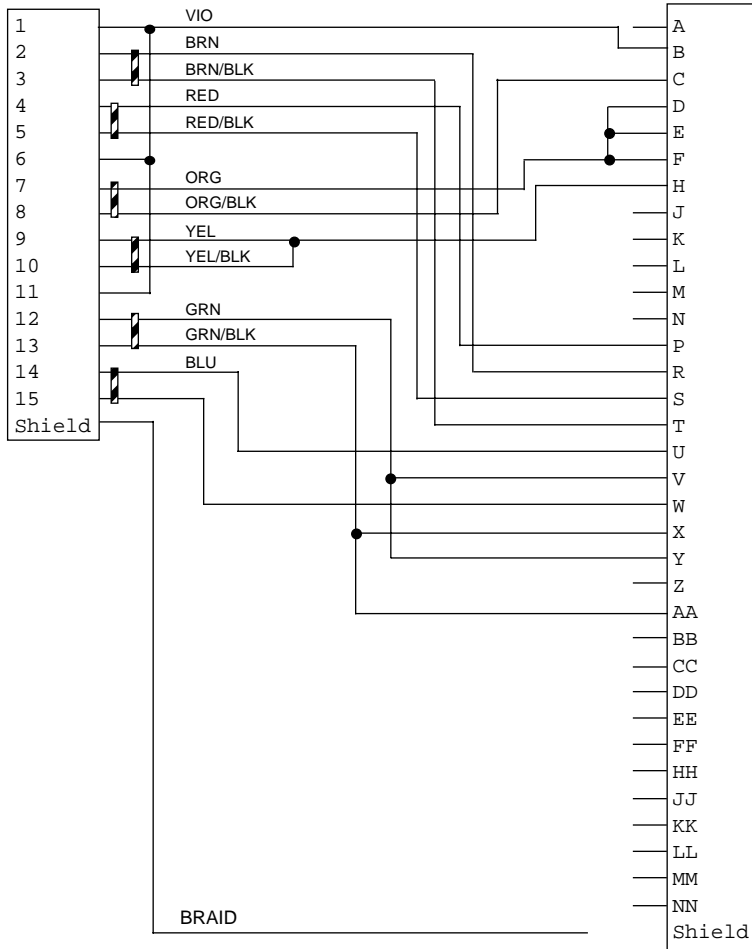
HD-15		V.35	
Pin 1		Pin A	(not used)
Pin 2		Pin B	Signal Ground
Pin 3		Pin C	Request to Send
Pin 4		Pin D	Clear to Send
Pin 5		Pin E	Data Set Ready
Pin 6		Pin F	Data Carrier Detect
Pin 7		Pin H	Data Terminal Ready
Pin 8		Pin J	(not used)
Pin 9		Pin K	(not used)
Pin 10		Pin L	(not used)
Pin 11		Pin M	(not used)
Pin 12		Pin N	(not used)
Pin 13		Pin P	Transmit Data (P)
Pin 14		Pin R	Receive Data (P)
Pin 15		Pin S	Transmit Data (N)
		Pin T	Receive Data (N)
		Pin U	Ext. Transmit Clock (P)
		Pin V	Receive Clock (P)
		Pin W	Ext. Transmit Clock (N)
		Pin X	Receive Clock (N)
		Pin Y	Transmit Clock (P)
		Pin Z	(not used)
		Pin AA	Transmit Clock (N)
		Pin BB	(not used)
		Pin CC	(not used)
		Pin DD	(not used)
		Pin EE	(not used)
		Pin FF	(not used)
		Pin HH	(not used)
		Pin JJ	(not used)
		Pin KK	(not used)
		Pin LL	(not used)
		Pin MM	(not used)
		Pin NN	(not used)

Pinouts for D3232 Splitter

Pin	Signal
1	TCP2
2	TCN2
3	TCP1
4	RCP1 (TIP1)
5	RCN1 (RING1)
6	TCN1
7	RCP2 (TIP2)
8	RCN2 (RING2)

B8
B7
B6
B5
B4
B3
B2
B1

A8
A7
A6
A5
A4
A3
A2
A1
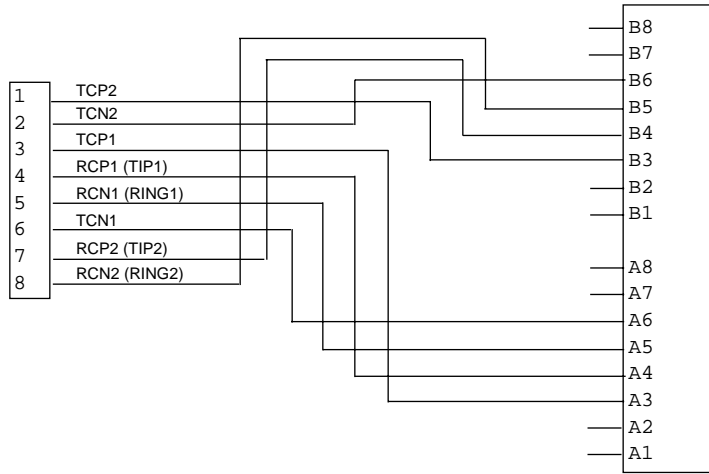
Description

Dimensions: 124.0 cm (w) x 20.0 cm (d) x 5.3 cm (h)
9.4″ (w) x 7.9″ (d) x 2.1″ (h)

Communications interfaces: The Netopia D-Series DSL DSU has an RJ-45 jack for IDSL or SDSL connections; an 8–port 10Base-T Ethernet hub for your LAN connection; a DB-9 Console port; and an HD-15 Auxiliary port that can be used as either a serial or LocalTalk port.

Power requirements

■   12 VDC input

■   1.5 amps

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via XMODEM or TFTP

Routing: TCP/IP Internet Protocol Suite, RIP, AppleTalk*, LocalTalk-to-Ethernet routing*, AURP tunneling*, MacIP*, IPX

* Optional add-on feature

WAN support: IDSL or SDSL

Security: IP/IPX firewalls, UI password security

SNMP network management: SNMPv1, MIB-II (RFC 1213), Interface MIB (RFC 1229), Ethernet MIB (RFC 1643), AppleTalk MIB-I (1243), Netopia D-Series MIB

Management/configuration methods: HTTP (Web server), serial console, remote modem console, Telnet, SNMP

Diagnostics: Ping, event logging, routing table displays, traceroute, statistics counters, web-based management

Agency approvals

The Netopia D-Series DSL DSU has met the safety standards (per CSA-950) of the Canadian Standards Association for Canada.

The Netopia D-Series DSL DSU has met the safety standards (per UL-1950) of the Underwriters Laboratories for the United States.

Regulatory notices

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

United States. This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Service requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. Under FCC rules, no customer is authorized to repair this equipment. This restriction applies regardless of whether the equipment is in or our of warranty. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 2470 Mariner Square Loop, Alameda, California, 94501.

Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

Declaration for Canadian users

The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The load number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop that is used by the device to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the load numbers of all the devices does not exceed 100.

Important safety instructions

Caution

- The direct plug-in power supply serves as the main power disconnect; locate the direct plug-in power supply near the product for easy access.

- For use only with CSA Certified Class 2 power supply, rated 12VDC, 1.5A.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.

- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

- Use caution when installing or modifying telephone lines.

- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.

- Do not use the telephone to report a gas leak in the vicinity of the leak.

Battery

The Netopia D-Series's lithium battery is designed to last for the life of the product. The battery is not user-serviceable.

Caution!

Danger of explosion if battery is incorrectly replaced.

Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Glossary

access line: A telephone line reaching from the telephone company central office to a point usually on your premises. Beyond this point the wire is considered inside wiring.

analog: In telecommunications, telephone transmission and/or switching that is not digital. An analog phone transmission is one that was originally intended to carry speech or voice, but may with appropriate modifications be used to carry data of other types.

ANSI (American National Standards Institute): Devises and proposes recommendations for international communications standards. See also *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.

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 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.

BAP (Bandwidth Allocation Protocol): Protocol that manages the dynamic bandwidth allocation of implementations supporting the PPP Multilink protocol. This is done by defining the Bandwidth Allocation Protocol (BAP), as well as its associated control protocol, the Bandwidth Allocation Control Protocol (BACP). BAP can be used to manage the number of links in a multilink bundle.

baud rate: The rate of the signaling speed of a transmission medium.

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.

broadcast: A network transaction that sends data to all hosts connected to the network.

burstiness: 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 intermittently, 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).*

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.

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.

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 integrity of a block of data. The mathematical function is computed, before the data is transmitted at the originating device. Its numerical value is computed based on the content of the data. This value is compared with a recomputed value of the function at the destination device.

DCE (Data Communications Equipment): Term defined by standards committees that applies to communications equipment, typically modems or printers, as distinct from other devices that attach to the network, typically personal computers or data terminals (DTE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Also see *DTE.*

DDP (Datagram Delivery Protocol): Defines socket-to-socket delivery of datagrams over an AppleTalk internet.

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.

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.

DSU: Digital Service Unit. A device for connecting a communications line to an external digital circuit.

DTE (Data Terminal Equipment): Term defined by standards committees, that applies to communications equipment, typically personal computers or data terminals, as distinct from other devices that attach to the network, typically modems or printers (DCE). The distinction generally refers to which pins in an RS-232-C connection transmit or receive data. Pins 2 and 3 are reversed. Also see *DCE*.

EIA (Electronic Industry Association): A North American standards association.

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.

firmware: System software stored in a device's memory that controls the device. The Netopia ISDN Router's firmware can be updated.

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 traverse from one node to another on a LAN.

hop count: The number of nodes (routers or other devices) 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.

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 Packet 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.

ITU (International Telecommunication Union): United Nations specialized agency for telecommunications. Successor to CCITT.

LAN (local area network): A privately owned network that offers high-speed communications channels to connect information processing equipment in a limited geographic area.

LocalTalk: The cabling specification for AppleTalk running at a speed of 230.4 kbps (kilobits per second).

MAC Address: Media Access Control address. The physical address of a device connected to a network, expressed as a 48-bit hexadecimal number. Sometimes this is called the hardware address, and is a unique number assigned to each device by the manufacturer.

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.*

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.

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.

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.

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): Ordinary analog telephone service such as that used for voice transmission, as distinct from digital service.

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.

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 network 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 TCP/IP, must be used over both networks. Routers may be equipped to provide WAN line support to the LAN devices they serve. They may also provide various management and monitoring functions as well as a variety of configuration capabilities.

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.

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).

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.*

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.

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):   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 10Base5 coaxial cable, the original Ethernet cabling.

thinnet: Industry jargon for 10Base2 coaxial cable, which is thinner (smaller in diameter) than the original Ethernet cabling.

UDP (User Datagram Protocol):   A TCP/IP protocol describing how packets reach applications in destination nodes.

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

Netopia warrants to you, the end user, that the Netopia D-Series DSL DSU (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. Netopia's entire liability and your sole remedy under this warranty during the warranty period is that Netopia shall, at its sole option, either repair or replace the Product.

In order to make a claim under this warranty you must comply with the following procedure:

1. Contact Netopia 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 Netopia 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 NETOPIA ALONE, AND THEY ARE THE ONLY WARRANTIES MADE BY ANYONE REGARDING THE ENCLOSED PRODUCT. NETOPIA AND ITS LICENSOR(S) MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MER-CHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE ENCLOSED PRODUCT. EXCEPT AS OTHERWISE EXPRESSLY PROVIDED ABOVE, NETOPIA 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 NETOPIA, 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 NETOPIA 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. NETOPIA 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.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com