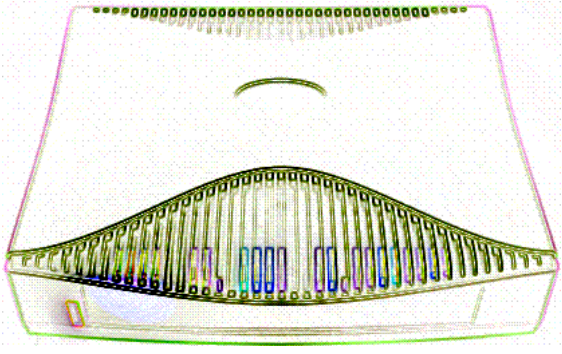
NETOPIA™ R9100 ETHERNET ROUTER FOR DSL AND CABLE MODEMS

User's Reference Guide



netopia®

Copyright

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

Patents

PhoneNET technology contained in Netopia is covered by U.S. Patent Numbers 4,901,342 and 5,003,579.
Other U.S. and foreign patents are pending.

Part Number

For additional copies of this electronic manual, order Netopia part number 6120339-PF-03

Printed Copies

For printed copies of this manual, order Netopia part number TER9100/Doc
(P/N 6120339-00-02)

Contents

Welcome to the Netopia R9100 Ethernet Router *User's Reference Guide*. This guide is designed to be your single source for information about your Netopia R9100 Ethernet Router. 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.

This Table of Contents page you are viewing consists of hypertext links to the chapters and headings listed. If you are viewing this on-line, just click any link below to go to that heading.

Part I: Getting Started

Part II: Advanced Configuration

Part I: Getting Started

Chapter 1

Introduction

Overview

The Netopia R9100 Ethernet Router is a full-featured, stand-alone, multiprotocol broadband router for connecting diverse local area networks (LANs) to the Internet and other remote networks. Combining the Netopia R9100 with a cable or DSL modem provides businesses with a low-cost connection to the Internet while retaining the power of a router. Once your Netopia R9100 Ethernet Router is connected to your computer and an Internet connection device such as a cable or a DSL modem, and your account is activated by your network service provider, you will have a high-speed connection between your PC or LAN and the telephone company's network of high-speed digital facilities.

This section covers the following topics:

Features and capabilities

The Netopia R9100 Ethernet Router provides the following features:

- Continuous-availability networking eliminates dialing and provides lower, more predictable transmission costs.
- Interconnects with most cable modems or DSL modems or bridges that have an Ethernet port.
- 8 port Ethernet hub
- Connectivity to support Ethernet LANs via built-in 8 port 10Base-T hub with uplink port.
- Status lights (LEDs) for easy monitoring and troubleshooting.
- Support for IP routing for Internet and intranet connectivity.
- IP address serving over Ethernet (or a WAN link via dynamic WAN client serving via the Auxiliary port with optional dial-in kit) that allows local or remote network nodes to acquire an IP address automatically and dynamically from a designated pool of available addresses.
- Support for console-based management over Telnet or serial cable connection.
- Support for remote configuration by your reseller, your network administrator, or technicians at Netopia, Inc. via external modem or via IP network.
- Wall-mountable, bookshelf (side-stackable), or desktop-stackable design for efficient space usage.
- SmartIP™, combining NAT and DHCP makes it simple and economical to connect a workgroup of users to the Internet or a remote IP network by using Network Address Translation and a single IP address.

- Analog dial-in using an external modem connected to the Auxiliary port. (Available as a separate add-on kit; order TER/AD1.)
- AppleTalk support (available as a separate add-on AppleTalk kit (order TER/AT1), including a firmware feature set enhancement and custom HD-15 dual RJ-11 PhoneNET® connector) allows for LocalTalk to Ethernet routing, assigning IP addresses to Macintosh users, IP functionality for LocalTalk users, and AURP tunneling for connectivity between remote AppleTalk networks.
- SmartView tool allows for real-time monitoring of router status lights (LEDs), through one or more information forms on a Web-based Java applet. Internet browsers such as Netscape Navigator and Microsoft's Internet Explorer can be used for SmartView.

How to use this guide

This guide is designed to be your single source for information about your Netopia R9100 Ethernet Router. 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 TER9100/Doc.

This guide is organized into chapters describing the Netopia R9100'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

Setting Up Internet Services

This chapter describes how to obtain and set up Internet services.

This section covers the following topics:

Finding an Internet service provider

Internet access is available from Internet Service Providers (ISPs). Typically, there are several ISPs in each area. To locate ISPs in your area, consult your telephone book, local computer magazines, the business section of a local newspaper, or the following URL on the Internet: ‘http://thelist.internet.com’. Also see Netopia’s home page at ‘http://www.netopia.com’ for a list of ISPs with special programs and promotions for Netopia customers.

You could select a cable television company that offers cable modem service as an ISP. Another alternative could be a traditional ISP that partners with a Competitive Local Exchange Carrier (CLEC) telephone service provider to provide a Digital Subscriber Line (DSL).

ISPs typically support Internet connection devices compatible with their service. So-called “cable modems” are an example of such devices. You should choose the connection device that your chosen ISP supports, or you could choose an ISP based on the type of device and connection you prefer.

Most most cable and DSL modems have a 10Base-T Ethernet connection port for connecting a PC. The Netopia R9100 Ethernet Router uses this connection port to connect all the computers on your LAN to the Internet.

If your area has more than one ISP, the following considerations will help you decide which ISP is best suited for your requirements.

Unique requirements

Make sure the ISP can meet any unique requirements you may have, such as:

- Dynamic or static IP addressing
- Custom domain name
- Multiple e-mail addresses
- Web site hosting

Pricing and support

Compare pricing, service, and technical support service among various ISPs.

Endorsements

Consider recommendations from colleagues and reviews in publications.

Deciding on an ISP account

Your ISP may offer various Internet access account plans. Typically, these plans vary by usage charges and the number of host IP addresses supplied. Evaluate your networking needs and discuss them with your ISP before deciding on a plan for your network.

The following checklist is a guide to ensure that you obtain the Internet service you require.

Setting up an account using a Netopia R9100

Check whether your ISP has the Netopia R9100 on its list of supported products that have been tested with a particular configuration. If the ISP does not have the Netopia R9100 on such a list, describe the Netopia R9100 in as much detail as needed, so your ISP account can be optimized. As appropriate, refer your ISP to Netopia's Web site www.netopia.com for more information or call us at 1-800-NETOPIA. Our representative can call your ISP and introduce them to the product. As necessary, we can provide them with the technical background they need to support the product.

Obtaining an IP address

Typically, each network computer that requires Internet access requires its own unique IP address.

Consider expected growth in your network when deciding on the number of addresses to obtain. Alternatively, you can use the Network Address Translation and DHCP features of SmartIP.

If some or all of your networked computers require simultaneous Internet access, and you don't want to use DHCP, obtain a block of IP host addresses large enough for each computer to have its own address, plus one for the Netopia R9100.

SmartIP

The Netopia R9100 Ethernet Router supports the SmartIP™ feature, which includes Network Address Translation.

Network Address Translation provides Internet access to the network connected to the Netopia R9100 using only a single IP address. These routers translate between the internal or local area network (LAN) addresses and a single external IP address, and route accordingly.

For more information on Network Address Translation, see Chapter 9, "IP Setup and Network Address Translation."

Obtaining information from the ISP

After your account is set up, the ISP should send you the IP parameter information that will help you configure the Netopia R9100.

Local LAN IP address information to obtain

Your ISP will need to provide you with the following information:

- The default gateway IP address
- Remote IP address
- Local WAN IP address and subnet mask
- Primary and secondary domain name server (DNS) IP addresses
- Domain name (usually the same as the ISP's domain name unless you have registered for your own individual domain name)

Refer to the section "Quick Easy Setup connection path" on page 7-3 for a handy worksheet.

Note: The default gateway, WAN address and mask, DNS, and domain name are all obtainable via WAN DHCP, if your ISP supports it.

With Network Address Translation

If you are using SmartIP (NAT), you should obtain the following:

- If you are connecting to a remote site using Network Address Translation on your router, your provider will not define the IP address information on your local LAN. You can define this information based on an IP configuration that may already be in place for the existing network. Alternatively, you can use the default IP address range used by the router, where 192.168.1.1 is the default IP address of the router.

Without Network Address Translation

If you are *not* using Network Address Translation, you will need to obtain all of the local LAN IP address information from your ISP and you will need to pay for an IP address for each device on the network.

If you are not using SmartIP (NAT), you should obtain:

- The Ethernet IP address for your Netopia R9100
- The Ethernet IP subnet mask for your Netopia R9100
- An IP address for each device on your network, in the same network range as the Netopia R9100.

Chapter 3

Making the Physical Connections

This section tells you how to make the physical connections to your Netopia R9100 Ethernet Router. This section covers the following topics:

Find a location

When choosing a location for the Netopia Router, 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 Router to the LAN
- 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

For small networks, install the Netopia R9100 near one of the LANs. For large networks, you can install the Netopia R9100 in a wiring closet or a central network administration site. In most cases the router will be near the cable or DSL modem which is near the cable or DSL wall outlet. You could route a line from the wall outlet to a wiring closet if you store the modem and router there.

What you need

Locate all items that you need for the installation.

Included in your router package are:

- The Netopia R9100 Ethernet Router
- A power adapter and cord with a mini-DIN8 connector
- Two RJ-45 cables (one for the Ethernet port on your PC; one for the Line port on the router)
- A dual DB-9 and mini-DIN8 to DB-9 console cable (for a PC or a Macintosh)
- The Netopia 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:

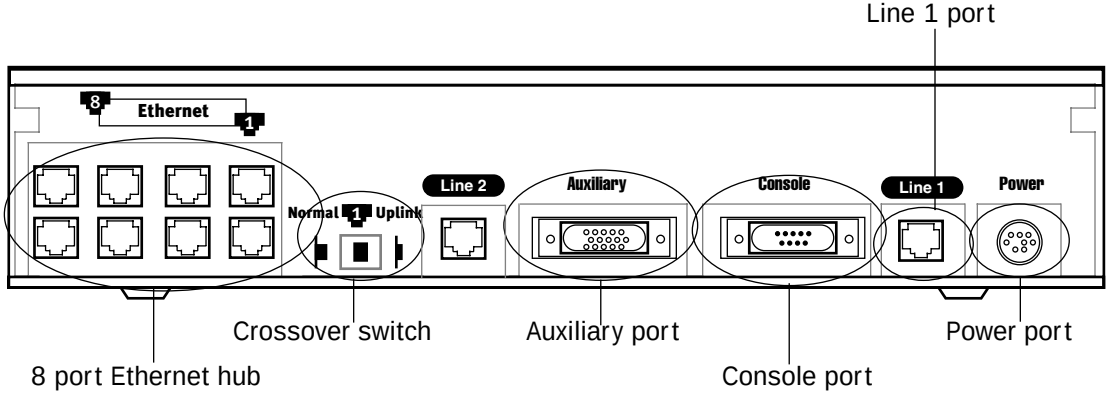
- A Windows 95, 98, or NT–based PC or a Macintosh computer with Ethernet connectivity for configuring the Netopia R9100. This may be built-in Ethernet or an add-on card, with TCP/IP installed and configured. See "Hardware and operating system requirements" on page 3-1.
- An Internet modem such as a cable modem or DSL bridge connected to the appropriate wall outlet for your Internet service source. Your Internet connection device must have a 10 Base-T Ethernet port for connecting it to the router's Line port.

Identify the connectors and attach the cables

Identify the connectors and switches on the back panel and attach the necessary Netopia Router cables.

The figure below displays the back of the Netopia R9100 Ethernet Router.

Netopia R9100 Ethernet Router back panel



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 of one of the RJ-45 cables to the Line 1 port (not the Line 2 port), and the other end to your Internet modem's Ethernet port. DO NOT CONNECT IT DIRECTLY TO A TELCO LINE OUTLET.

3. Connect one end of one of the RJ-45 cables to any of the Ethernet hub ports on the router, and the other end to the Ethernet port of your PC.

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

   You should now have: the power adapter plugged in; the Ethernet cable connected between the router and your computer; and the Line cable connected between the router and your Internet modem.

Netopia R9100 Ethernet Router back panel ports

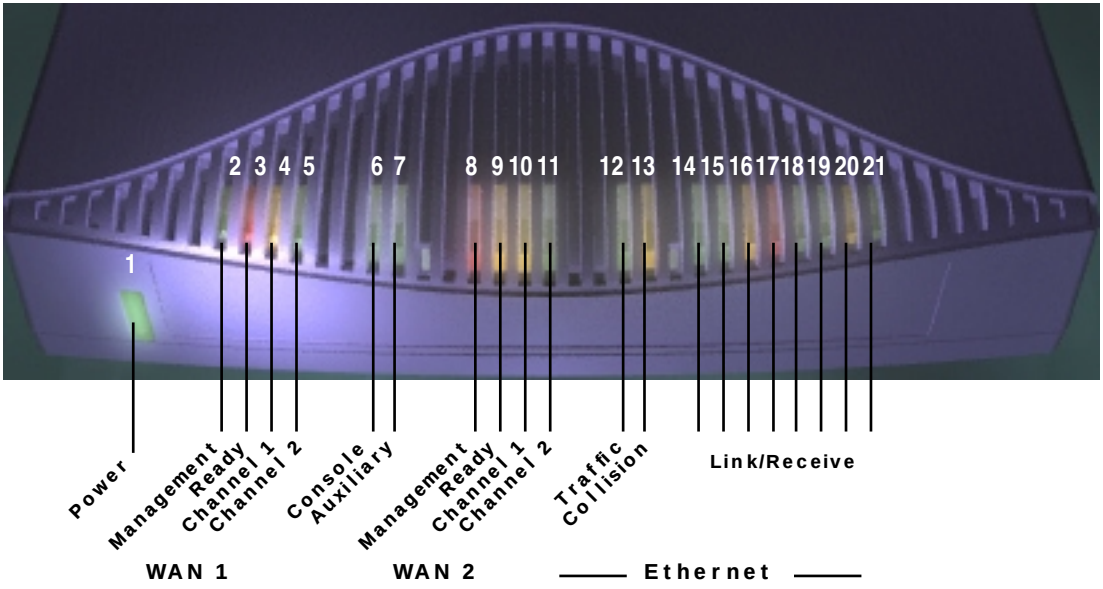
The following table describes all the Netopia R9100 Ethernet Router back panel ports.

Port	Description
Power port	A mini-DIN8 power adapter cable connection.
Line port	The dedicated Ethernet port for your connection to your Internet connection device's Ethernet port. Use Line 1, not Line 2.
Console port	A DB-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 router" on page 6-3.
Auxiliary port	An HD-15 auxiliary port for attaching an external modem or the optional AppleTalk kit.
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 router, set the switch to the **Normal** position. If you are connecting the router to an Ethernet hub, use Ethernet port #1 on the router and set the switch to the **Uplink** position.
8-port Ethernet hub	Eight Ethernet jacks. You will use one of these to configure the Netopia R9100. 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 router, or connect both your computer and the router to an existing Ethernet hub on your LAN.

Netopia R9100 Ethernet Router status lights

The figure below represents the Netopia R9100 status light (LED) panel.

Netopia R9100 LED front panel



The following table summarizes the meaning of the various LED states and colors:

When this happens...	the LEDs...
The Ethernet WAN interface is operational	3 is **green**.
The Ethernet WAN interface detects a collision	3 flashes **orange**.
In normal operation	4 is **off**.
When data is transmitted or received over the Ethernet link	4 flashes **yellow**.
Note: 2, 5, 8 – 11 are unused. Also, Console carrier (6) is ignored if the console is not configured for a remote modem.	

Chapter 4

Connecting to Your Local Area Network

This chapter describes how to physically connect the Netopia R9100 to your local area network (LAN). Before you proceed, make sure the Netopia R9100 is properly configured. You can customize the router's configuration for your particular LAN requirements using console-based Management (see "Console-Based Management" on page 6-1).

This section covers the following topics:

Overview

You can connect the Netopia R9100 to an IP or IPX network that uses Ethernet.

If you have purchased the AppleTalk feature expansion kit, you can also connect the router to a LocalTalk network that uses PhoneNET cabling.

Additionally, you can connect an external modem. See "Adding an external modem" on page 4-7.

Caution!

Before connecting the Netopia R9100 to any AppleTalk LANs that contain other AppleTalk routers, you should read "Routers and seeding" on page 11-3.

See the later sections in this chapter for details on how to connect the Netopia R9100 to different types of networks.

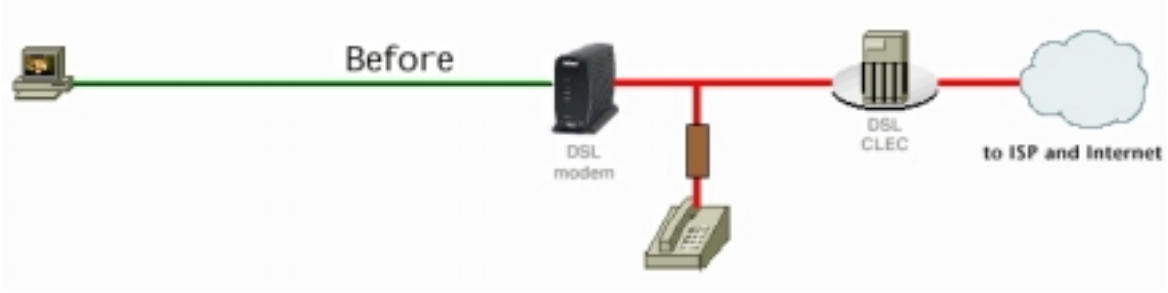
Network Model

The following diagrams illustrate network models for typical deployments of the Netopia R9100 Ethernet Router as an Internet access device.

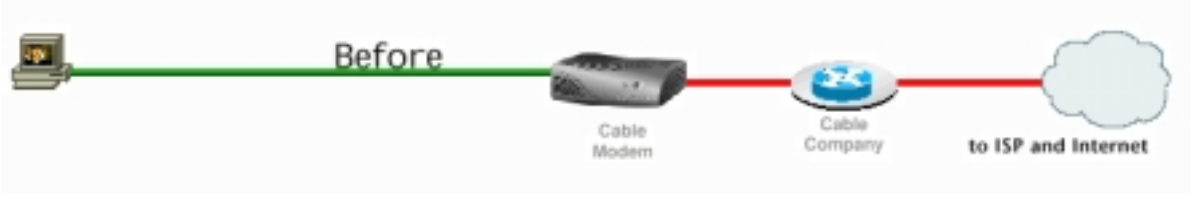
Before

With a DSL or cable modem, you can connect a single computer to the Internet.

using a DSL modem



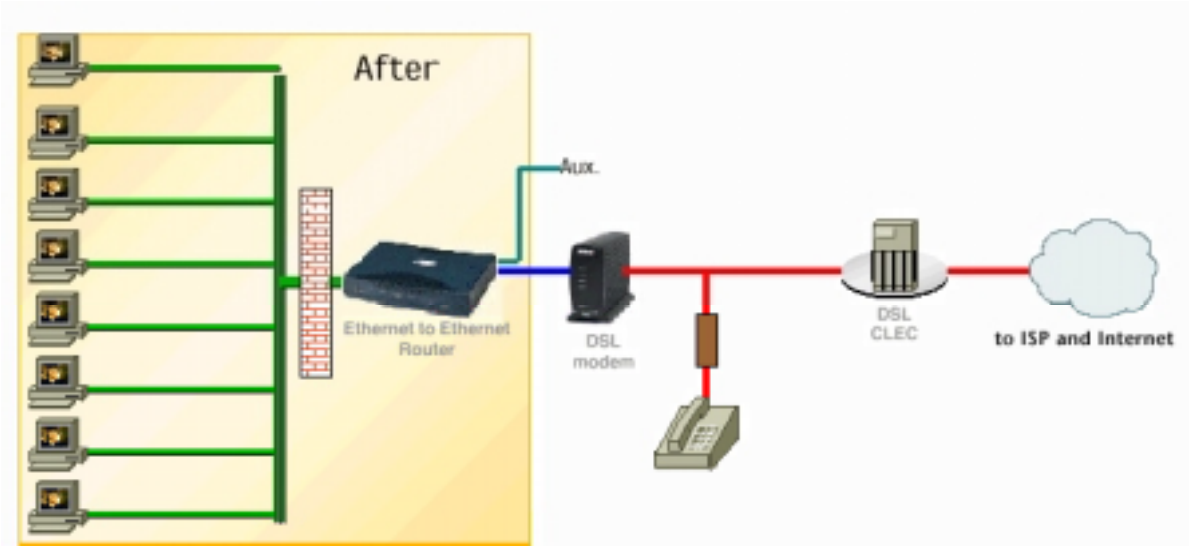
using a cable modem



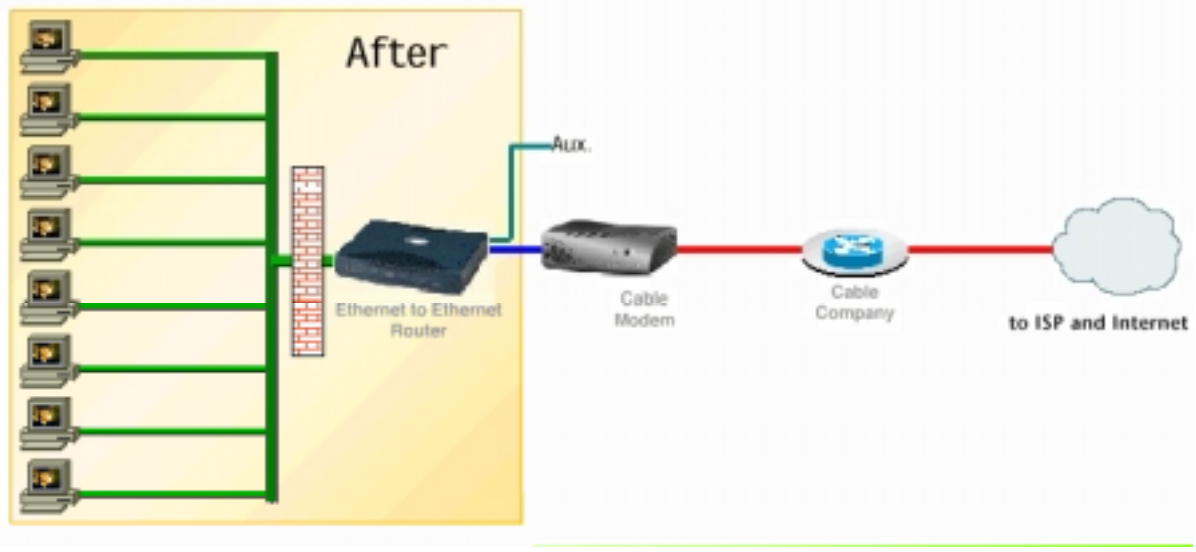
After

Using the Netopia R9100 Ethernet Router, you can connect multiple computers to the Internet with a single user account.

using a DSL modem with a Netopia R9100



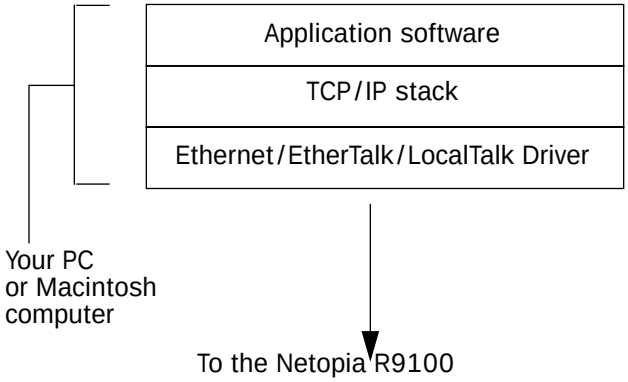
using a cable modem with a Netopia R9100



While this network model is typical, other network models are possible. For example, you may choose to attach the Ethernet WAN port to an external Ethernet hub connected to a number of workstations.

Readying computers on your local network

PC and Macintosh computers must have certain components installed before they can communicate through the Netopia R9100. The following illustration shows the minimal requirements for a typical PC or Macintosh computer.



Application software: This is the software you use to send e-mail, browse the World Wide Web, read newsgroups, etc. These applications may require some configuration. Examples include the Eudora 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 R9100. 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, 98, or NT" on page 3-2. Macintosh computers use either MacTCP or Open Transport. See "Configuring TCP/IP on a Macintosh Computer" on page 3-4.

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 R9100 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 R9100 supports Ethernet connections through its eight Ethernet ports. The router automatically detects which Ethernet port is in use.

You can connect either 10Base-T or EtherWave Ethernet networks to the Netopia R9100.

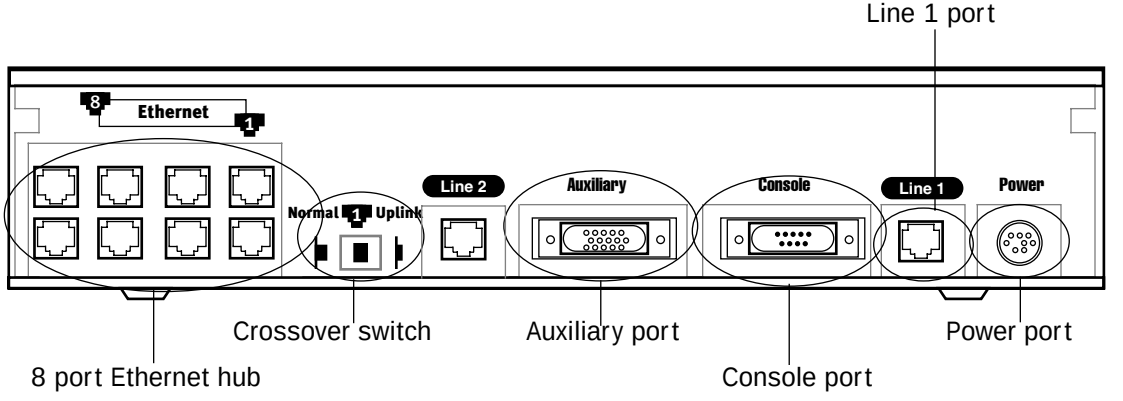
The following table displays some important attributes of these types of Ethernet.

Attribute	EtherWave	10Base-T
Max. length of backbone, branch, or end to end (cable length)	330 feet (100 meters)	330 feet (100 meters)
Cable type	Twisted pair (10Base-T)	Twisted pair (10Base-T)
Netopia R9100 port used	Ethernet	Ethernet
Other restrictions	Maximum 8 devices (daisy chained)	No daisy chain

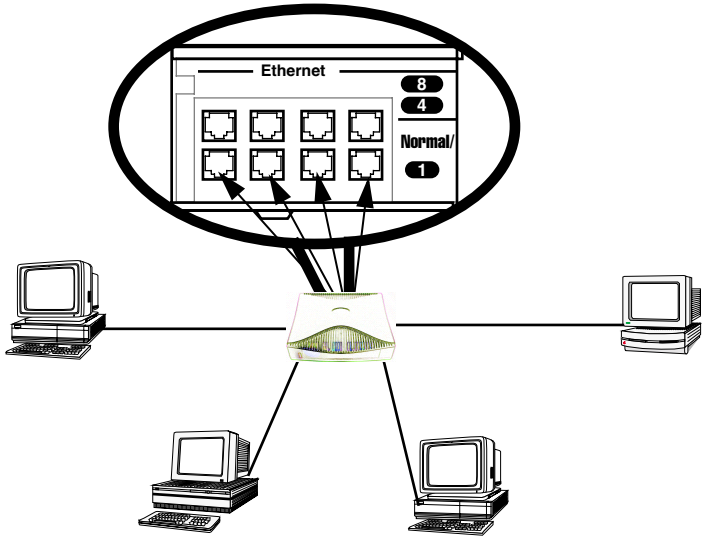
10Base-T

You can connect a standard 10Base-T Ethernet network to the Netopia R9100 using any of its available Ethernet ports.

Netopia R9100 Ethernet Router back panel



The Netopia R9100 in a 10Base-T network

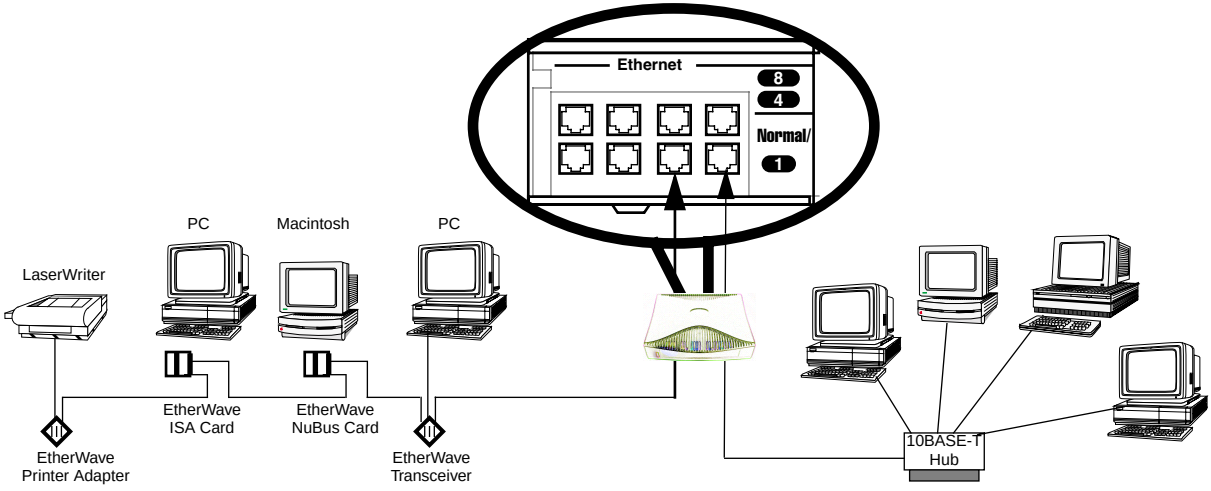


To connect your 10Base-T network to the Netopia R9100 through an Ethernet port, use a 10Base-T cable with RJ-45 connectors.

If you have more than eight devices to connect, you can attach additional devices using either a 10Base-T hub or an EtherWave daisy chain, or some combination of both.

If you add devices connected through a hub, connect the hub to Ethernet port number 1 on the Netopia R9100 and set the Normal/Uplink switch to Uplink.

When there are no more free ports on the 10Base-T hub, the network can be extended using EtherWave, a daisy-chainable solution from Farallon.

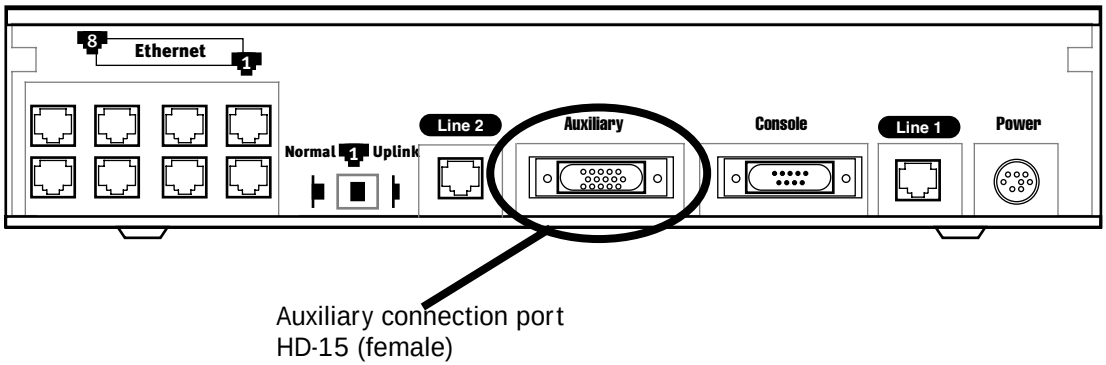


Adding an external modem

You may want to add an external modem to your Auxiliary port. Remote modem terminal emulator setups can dial in to the modem line and establish a remote console session. This allows Netopia Inc.'s "Up and Running, Guaranteed!" department or other administrator with the appropriate security to remotely configure your router for you.

Obtain the special external DB-25 modem cable (Netopia P/N TE6/DB25) either from your reseller or directly from Netopia.

Netopia R9100 Auxiliary port for connecting an external modem



By default, the **Auxiliary** port on your Netopia R9100 is enabled for remote console configuration via an external asynchronous modem. This means that all you have to do is connect your modem to the Auxiliary port and configure its settings in the **Line Configuration** screens under the **WAN Configuration** menu.

Full Auxiliary Port PPP capabilities can be enabled on a Netopia R9100 as an upgrade option.

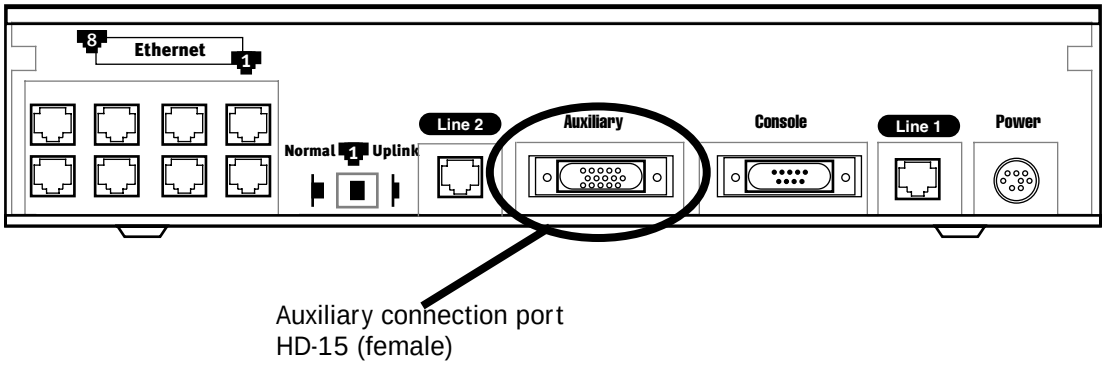
For pinout information on the HD-15 to DB-25 modem cable, see "Pinouts for Auxiliary port modem cable," in Appendix F, "Technical Specifications and Safety Information."

Connecting to a LocalTalk network

If you have purchased the AppleTalk feature expansion kit, you can also connect the router to an AppleTalk network that uses either Ethernet or LocalTalk. Refer to the sheet of optional feature set add-ons in your Netopia R9100 documentation folio.

The AppleTalk feature expansion kit includes a dual RJ-11 PhoneNET connector that attaches to the **Auxiliary** port on the Netopia R9100.

Netopia R9100 Auxiliary port for connecting to LocalTalk



Connect the male HD-15 end of the LocalTalk cable to the **Auxiliary** port on your Netopia R9100. Connect the other end of the cable to your LocalTalk network. You can use only one connection on the Auxiliary port. You cannot use both the PhoneNET connector and an external modem.

If your LocalTalk network is not based on standard PhoneNET cabling, use a PhoneNET-to-LocalTalk adaptor cable available from Farallon Communications, Inc. Connect the adaptor cable's RJ-11 connector to the AppleTalk cable's PhoneNET connector. Connect the cable's mini-DIN-3 connector to your LocalTalk network.

Be sure to observe the standard rules governing maximum cable lengths and limits on the number of nodes on a PhoneNET network. The dual RJ-11 PhoneNET connector allows insertion in the LocalTalk daisy chain or at the end. If the device is connected at the end of the daisy chain, you must install the accompanying terminator.

Wiring guidelines for PhoneNET cabling

Topology	22 gauge .642 mm	24 gauge .510 mm	26 gauge .403 mm
Daisy chain	n/a	n/a	1800 ft. 549 m
Backbone	4500 ft. 1372 m	3000 ft. 229 m	1800 ft. 549 m
4-branch passive star*	1125 ft. 343 m	750 ft. 229 m	450 ft. 137 m
LocalTalk StarController 12-branch active star	3000 ft. 914 m	2000 ft. 610 m	1200 ft. 366 m
* Distance is per branch			

For detailed configuration instructions see “AppleTalk Setup” on page 11-1.

Chapter 5

Setting up your Router with the SmartStart Wizard

Once you've connected your router to your computer and your telecommunications line and installed a web browser, you're ready to run the Netopia SmartStart™ Wizard. The SmartStart Wizard will help you set up the router and share the connection. The SmartStart Wizard walks you through a series of questions and based on your responses automatically configures the router for connecting your LAN to the Internet or to your remote corporate network.

The SmartStart Wizard will:

- automatically check your Windows 95, 98, or NT PC's TCP/IP configuration to be sure you can accept a dynamically assigned IP address, and change it for you if it is not set for dynamic addressing
- check the physical connection from your computer to your router without your having to enter an IP address
- assign an IP address to your router

This chapter covers the following topics:

Before running SmartStart

Be sure you have connected the cables and power source as described in Step 1 "Connect the Router" guide contained in your Netopia folio.

Before you launch the SmartStart application, make sure your computer meets the following requirements:

	PC	Macintosh
System software	Windows 95, 98, or NT operating system	MacOS 7.5 or later
Connectivity software	TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Windows 95, 98, or NT computers" on page 5-6	MacTCP or Open Transport TCP/IP must be installed and properly configured. See "Configuring TCP/IP on Macintosh computers" on page 5-10.
Connectivity hardware	Ethernet card (10Base-T)	Either a built-in or third-party Ethernet card (10Base-T)
Browser software	Netscape Communicator™ or Microsoft Internet Explorer, included on the Netopia CD. Required for web-based registration and web-based monitoring.	

Notes:

- The computer running SmartStart must be on the same Ethernet cable segment as the Netopia R9100. Repeaters, such as 10Base-T hubs between your computer and the Netopia R9100, are acceptable, but devices such as switches or other routers are not.
- SmartStart for the PC will set your TCP/IP control panel to "Obtain an IP address automatically" if it is not already set this way. This will cause your computer to reboot. If you have a specified IP address configured in the computer, you should make a note of it before running SmartStart, in case you do not want to use the dynamic addressing features built in to the Netopia Router and need to restore the fixed IP address.

Setting up your Router with the SmartStart Wizard

The SmartStart Wizard is tailored for your platform, but it works the same way on either a PC or a Macintosh. Insert the Netopia CD, and in the desktop navigation screen that appears, launch the SmartStart Wizard application.

SmartStart Wizard configuration screens

The screens described in this section are the default screens shipped on the Netopia CD. They derive from two initialization (.ini) files included in the same directory as the SmartStart application file. Your reseller or your ISP may have supplied you with customized versions of these files.

- If you have received a CD or diskette that has been customized by your reseller or ISP, you can run the SmartStart Wizard directly from the CD or diskette and follow the instructions your reseller or ISP provides. This makes your Netopia R9100 configuration even easier.
- If you have received only the .ini files from your reseller or ISP, perform the following:
  - Copy the entire directory folder containing the SmartStart Wizard application from the Netopia CD to your hard disk.
  - Copy the customized .ini files to the same directory folder that contains the SmartStart Wizard application, allowing the copy process to overwrite the original .ini files.
  - Run the SmartStart Wizard from your hard disk. You can then follow the instructions your reseller or ISP provides.

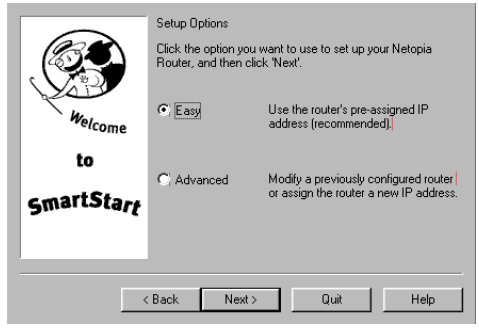
The SmartStart Wizard presents a series of screens to guide you through the preliminary configuration of a Netopia R9100. It will then create a connection profile using the information you supply to it.

Welcome screen. The first screen welcomes you to the SmartStart Wizard configuration utility.

Click the Next button after you have responded to the interactive prompts in each screen.

The Help button will display useful information to assist you in responding to the interactive prompts.

Easy or Advanced options screen. You can choose either Easy or Advanced setup.



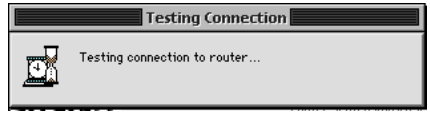
- If you choose Easy, SmartStart automatically uses the preconfigured IP addressing setup built into your router. This is the best choice if you are creating a new network or don't already have an IP addressing scheme on your new network.

  If you choose Easy, you will see a "Connection Test screen," like the one shown below while SmartStart checks the connection to your router.

- If you choose Advanced, skip to page 5-6 now. The SmartStart Wizard displays the "Router IP Address screen" on page 5-5, in which you can choose ways to modify your router's IP address.

Easy option

Connection Test screen. SmartStart tests the connection to the router. While it is testing the connection, a progress indicator screen is displayed and the router's Ethernet LEDs flash.



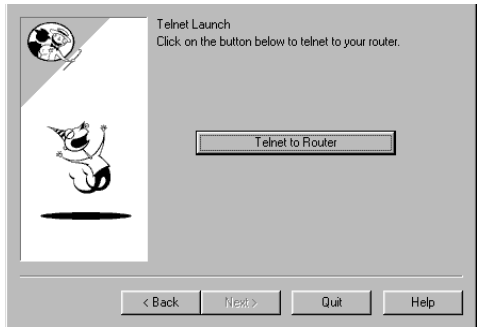
When the test succeeds, SmartStart indicates success.

If the test fails, the wizard displays an error screen. If the test fails, check the following:

- Check your cable connections. Be sure you have connected the router and the computer properly, using the correct cables. Refer to the Step 1 "Connect the Router" sheet in your Netopia R9100 documentation folio.
- Make sure the router is turned on and that there is an Ethernet connection between your computer and the router.
- Check the TCP/IP control panel settings to be sure that automatic IP Addressing (Windows) or DHCP (Macintosh) is selected. If you are using a Windows PC, SmartStart will automatically detect a static IP address and offer to configure the computer for automatic addressing. On a Macintosh computer, you must manually set the TCP/IP Control Panel to DHCP. See "Configuring TCP/IP on Macintosh computers" on page 5-10. If you currently use a static IP address outside the 192.168.1.x network, and want to continue using it, use the Advanced option to assign the router an IP address in your target IP range. See "Advanced option" on page 5-5.
- If all of the above steps fail to resolve the problem, reset the router to its factory default settings and rerun SmartStart. See "Factory defaults" on page 14-6 for instructions.

When the test is successful, SmartStart presents you with the "Additional Configuration screen," shown below.

Additional Configuration screen. If you have a router that has a permanent unswitched connection to your ISP, such as an Ethernet WAN interface router attached to a cable modem, the Additional Configuration screen appears.



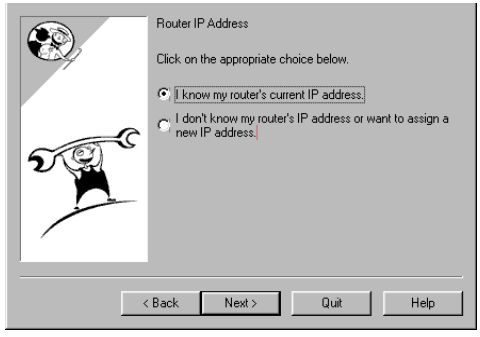
You may want to do additional configuration to customize your network environment. SmartStart lets you launch your Telnet application. Click the Telnet button to launch your Telnet application.

Advanced configuration options available via Telnet are explained in "Console-Based Management" on page 6-1.

However, if you need no further configuration options, click Quit. Congratulations! You're done!

Advanced option

Router IP Address screen. If you selected the Advanced option in the "Easy or Advanced options screen" on page 5-4, SmartStart asks you to choose between entering the router's current IP address and assigning an IP address to the router.

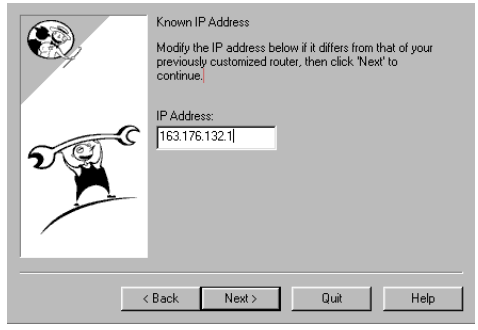


If the router has already been assigned an IP address, select the first radio button. If you do this, the "Known IP Address screen," appears (shown below.)

If you want to reconfigure the router with a new IP address and subnet mask, select the second radio button. If you do this, the "New IP Address screen" on page 5-6 appears.

When you have done this, click Next.

Known IP Address screen. SmartStart displays a recommended address for the router based on the IP address of the computer.



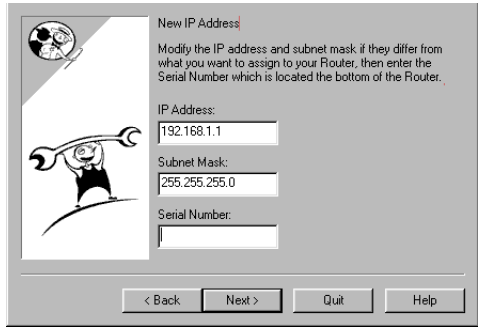
If you know the router has an IP address different from the default value, enter it now. Otherwise, accept the recommended address.

When you have done this, click Next.

SmartStart tests the connection to your router.

SmartStart then returns you to an "Additional Configuration screen" on page 5-5.

New IP Address screen. If you want to change the router's IP address, you enter the new IP address, the subnet mask, and the router's serial number in this screen. Remember, the serial number is on the bottom of the router. It is also found in your documentation folio.



Note: Forcing a new IP address may turn off the Netopia R9100's IP address serving capabilities, if you assign an IP address and subnet mask outside the router's current IP address serving pool. The Netopia R9100 does not allow an invalid address to be served. Use this option with caution.

When you have done this, click Next.

SmartStart forces the new IP address into the router, tests the connection, and then resets the router.

SmartStart then returns you to the "Additional Configuration screen" on page 5-5.

Sharing the Connection

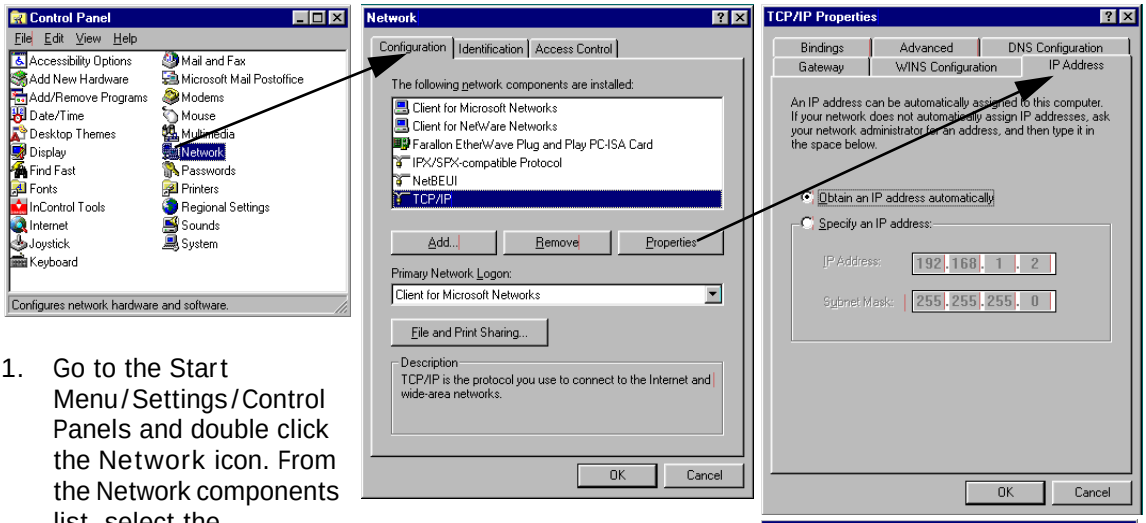
Configuring TCP/IP on Windows 95, 98, or NT computers

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

Dynamic configuration (recommended)

If you configure your Netopia R9100 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP) server, which enables dynamic addressing, is enabled by default in the router. If your PC is not set for dynamic addressing, SmartStart will offer to do this for you when you launch it. In that case, you will have to restart your PC and relaunch SmartStart. If you configure your PC for dynamic addressing in advance, SmartStart need only be launched once. To configure your PC for dynamic addressing do the following:



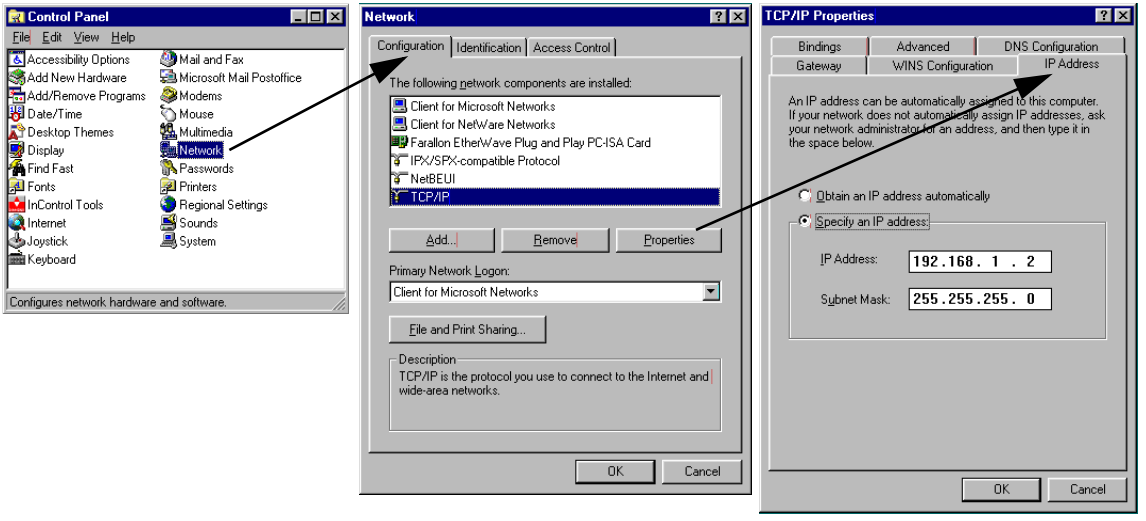
1. Go to the Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click “Obtain an IP Address automatically.”
3. Click on the DNS Configuration tab. Click Disable DNS. DNS will be assigned by the router with DHCP.
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 to accept IP addresses served by the Netopia R9100.

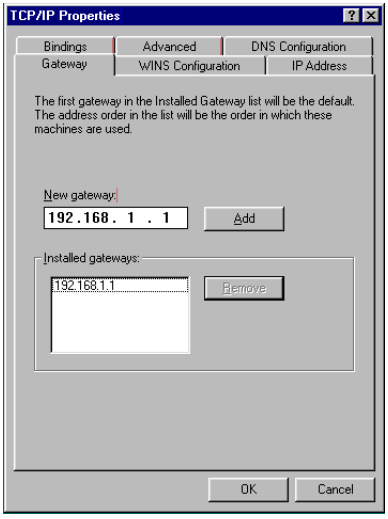
Static configuration (optional)

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

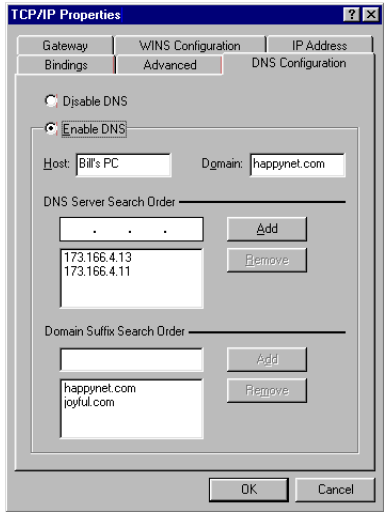
1. Go to Start Menu/Settings/Control Panels and double click the Network icon. From the Network components list, select the Configuration tab.
2. Select TCP/IP-->Your Network Card. Then select Properties. In the TCP/IP Properties screen (shown below), select the IP Address tab. Click "Specify an IP Address."
   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 router 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 R9100’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.

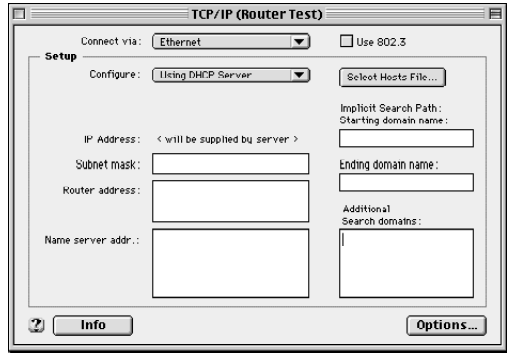
  Note: If you want to use the Dynamic Host Configuration Protocol (DHCP) server built into your Netopia R9100 to assign IP addresses to your Macintoshes, you must be running Open Transport, standard in MacOS 8, and optional in earlier system versions. You can have your Netopia R9100 dynamically assign IP addresses using MacTCP; however, to do so requires that the optional AppleTalk kit be installed which can only be done after the router is configured.

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

Dynamic configuration (recommended)

If you configure your Netopia R9100 using SmartStart, you can accept the dynamic IP address assigned by your router. The Dynamic Host Configuration Protocol (DHCP), which enables dynamic addressing, is enabled by default in the router. To configure your Macintosh computer for dynamic addressing do the following:

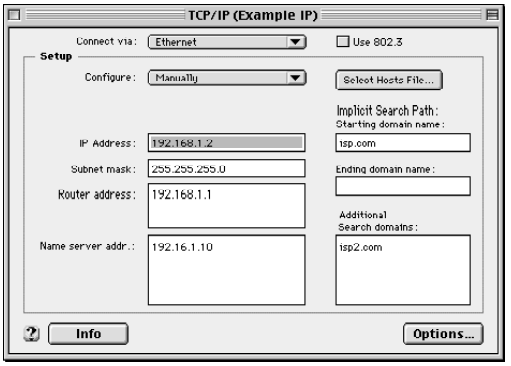
1. Go to the Apple menu. Select Control Panels and then TCP/IP.
2. With the TCP/IP window open, go to the Edit menu and select User Mode. Choose Basic and click OK.
3. In the TCP/IP window, select "Connect via: Ethernet" and "Configure: Using DHCP Server."



Note: You can also use these instructions to configure other computers on your network to accept IP addresses served by the Netopia R9100.

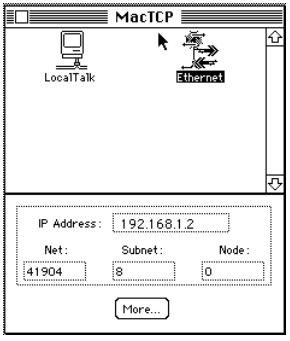
Static configuration (optional)

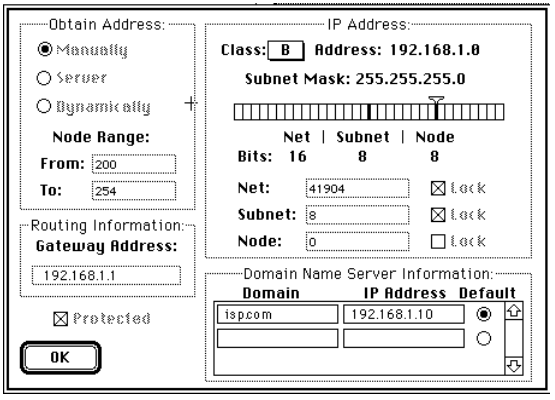
If you are manually configuring for a fixed or static IP address, perform the following:



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
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.

Dynamic configuration using MacIP (optional)

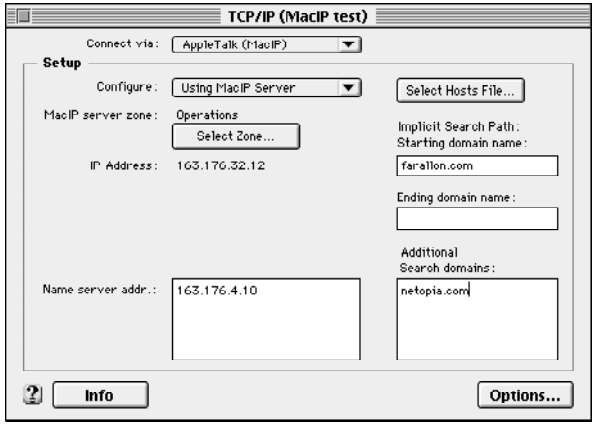
If you want to use MacIP to dynamically assign IP addresses to the Macintosh computers on your network you must install the optional AppleTalk feature set kit.

Note: You cannot use MacIP dynamic configuration to configure your Netopia R9100 Ethernet Router because you must first configure the router in order to enable AppleTalk.

Once the AppleTalk kit is installed, you can configure your Macintoshes for MacIP. To configure dynamically using MacIP, perform the following:

Using Open Transport TCP / IP

1. Go to the Apple menu. Select **Control Panels** and then **TCP / IP**.
2. With the TCP / IP window open, go to the Edit menu and select **User Mode**. Choose **Advanced** and click **OK**.



3. In the TCP / IP window, select or type information into the fields as shown in the following table.

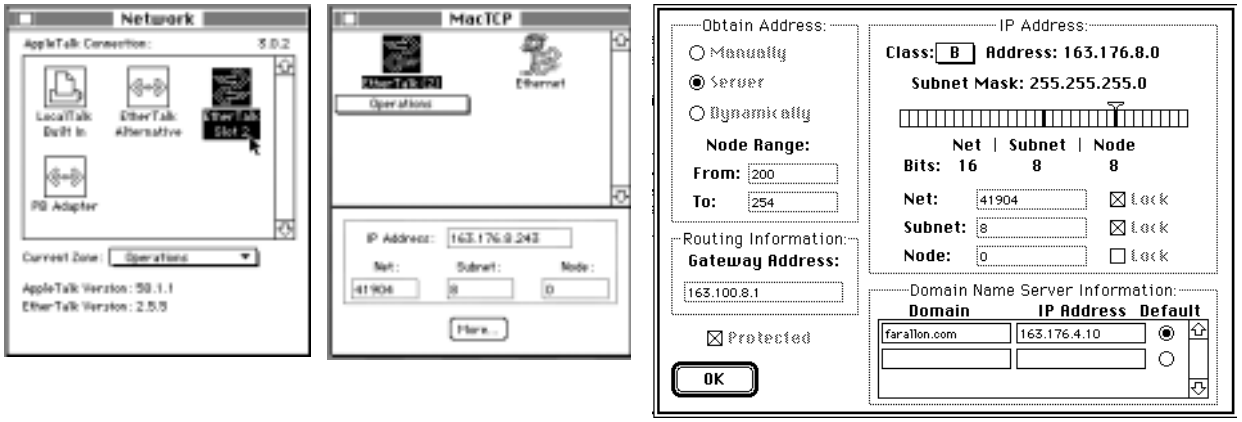
TCP / IP Option:	Select / Type:
Connect via:	AppleTalk (MacIP)
Configure:	Using MacIP server
MacIP Server zone:	(select available zone)
Name server address:	Enter the primary and secondary name server addresses given to you by your ISP
Implicit Search Path: Starting domain name:	Enter your domain name; if you do not have a domain name, enter the domain name of your ISP

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

   These are the only fields you need to modify in these screens.

Using Classic Networking (MacTCP)

1. Go to the Apple Menu. Select **Control Panels** and then **Network**.
2. In the Network window, select **EtherTalk**.



3. Go back to the Apple menu. Select **Control Panels** and then **MacTCP**.
4. Select **EtherTalk**.

   From the pull-down menu under EtherTalk, select an available zone; then click the **More** button.

   In the MacTCP/More window select the **Server** radio button. If necessary, fill in the Domain Name Server Information given to you by your administrator.
5. Restart the computer.

   These are the only fields you need to modify in these screens.

Note: More information about configuring your Macintosh computer for TCP/IP connectivity through a Netopia R9100 can be found in Technote NIR_026, “Open Transport and Netopia Routers,” located on the Netopia Web site.

Chapter 6

Console-Based Management

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R9100. Console-based management provides access to a wide variety of features that the router 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:

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

```
                        Netopia R9100 v4.3

                    Easy Setup...
                    WAN Configuration...
                    System Configuration...
                    Utilities & Diagnostics...
                    Statistics & Logs...
                    Quick Menus...
                    Quick View...



You always start from this main screen.
```

- The **Easy Setup** menus display and permit changing the values contained in the default WAN and IP configuration. Experienced users can use Easy Setup to initially configure the router directly through a console session.

  Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.

- The **WAN Configuration** menu displays and permits changing your WAN and IP configuration(s) and default profile, and configuring or reconfiguring the manner in which you may be using the router to connect to

more than one service provider or remote site.

- The **System Configuration** menus display and permit changing:
  - Network protocols setup. See "IP Setup and Network Address Translation" on page 9-1, "IPX Setup" on page 10-1, and "AppleTalk Setup" on page 11-1.
  - Filter sets (firewalls). See "Security" on page 13-1.
  - IP address serving. See "IP address serving" on page 9-16.
  - Date and time. See "Date and time" on page 8-12.
  - Console configuration. See "Connecting a console cable to your router" on page 6-3.
  - SNMP (Simple Network Management Protocol). See "SNMP" on page 12-12.
  - Security. See "Security" on page 13-1.
  - Upgrade feature set. See "Upgrade feature set" on page 8-13.
- The **Utilities & Diagnostics** menus provide a selection of seven tools for monitoring and diagnosing the router's behavior, as well as for updating the firmware and rebooting the system. See "Utilities and Diagnostics" on page 14-1 for detailed information.
- The **Statistics & Logs** menus display a selection of tables and device logs that show information about your router, your network and their history. See "Statistics & Logs" on page 12-3 for detailed information.
- The **Quick Menus** screen is a shortcut entry point to a wide variety of the most commonly used configuration menus that are accessed through the other menu entry points.
- The **Quick View** menu displays at a glance current real-time operating information about your router. See "Quick View status overview" on page 12-1 for detailed information.

Connecting through a Telnet session

Features of the Netopia R9100 can be configured through the console screens.

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

- A network connection locally to the router or IP access to the router.

  Note: 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 router. For more information on attaching the console cable, see "Connecting a console cable to your router" on page 6-3.
- Telnet software installed on the computer you will use to configure the router

Configuring Telnet software

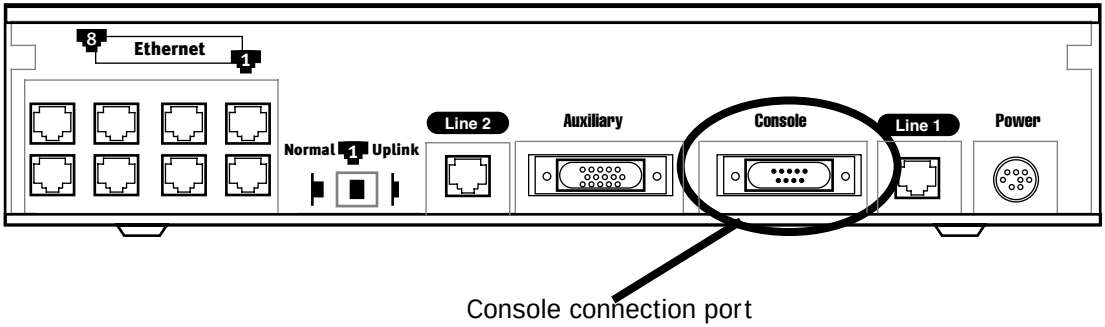
If you are configuring your router using a Telnet session, your computer must be running a Telnet software program.

- 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 Netopia R9100 CD. You install NCSA Telnet by simply dragging the application from the CD to your hard disk.

Connecting a console cable to your router

You can perform all of the system configuration activities for your Netopia R9100 through a local serial console connection using terminal emulation software, such as HyperTerminal provided with Windows95 on the PC, or ZTerm, included on the Netopia CD, for Macintosh computers.

The Netopia R9100 back panel has a connector labeled “Console” for attaching the Router 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 R9100 via the console screens.



Console connection port
DB-9 (male)

To connect the Netopia R9100 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 R9100’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 Netopia R9100 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 R9100 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*	Options are: 9600, 19200, 38400, or 57600 bits per second
Flow Control	None
Note: The router 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.	

Navigating through the console screens

Use your keyboard to navigate the Netopia R9100'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 + j
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 7

Easy Setup

This chapter describes how to use the Easy Setup console screens on your Netopia R9100 Ethernet Router. After completing the Easy Setup console screens, your router will be ready to connect to the Internet or another remote site.

This chapter covers the following topics:

Easy Setup console screens

Using three Easy Setup console screens, you can:

- Define your Wide Area Network (WAN) connection for your router to connect to your ISP or remote location
- Set up IP addresses and IP address serving
- Password–protect configuration access to your Netopia R9100 Ethernet Router

Accessing the Easy Setup console screens

To access the console screens, Telnet to the Netopia Router over your Ethernet network, or physically connect with a serial console cable and access the Netopia Router with a terminal emulation program. See "Connecting through a Telnet session" on page 6-2 or "Connecting a console cable to your router" on page 6-3.

Note: Before continuing, make sure you have the information that your telephone service provider, ISP, or network administrator has given you for configuring the Netopia Router.

The Netopia Router's first console screen, Main Menu, appears in the terminal emulation window of the attached PC or Macintosh computer when

- The Netopia Router is turned on
- The computer is connected to the Netopia Router
- The Telnet or terminal emulation software is running and configured correctly

A screen similar to the following Main Menu appears:

```
                        Netopia R9100 v4.3

                    Easy Setup...
                    WAN Configuration...
                    System Configuration...
                    Utilities & Diagnostics...
                    Statistics & Logs...
                    Quick Menus...
                    Quick View...


Your Baud Rate has been changed to 57600
You always start from this main screen.
```

If you do not see the Main Menu, verify that:

- The computer used to view the console screen has its serial port connected to the Netopia R9100's Console port or an Ethernet connection to one of its Ethernet ports. See "Connecting a console cable to your router" on page 6-3 or "Connecting through a Telnet session" on page 6-2.
- The Telnet or terminal emulation software is configured for the recommended values.
- If you are connecting via the Console port, your computer's serial port is not being used by another device, such as an internal modem, or an application. Turn off all other programs (other than your terminal emulation program) that may be interfering with your access to the port.
- You have entered the correct password, if necessary. Your Netopia R9100's console access may be password protected from a previous configuration. See your system administrator to obtain the password.

  See Appendix A, "Troubleshooting," for more suggestions.

Quick Easy Setup connection path

This section may be all you need to do to configure your Netopia R9100 Ethernet Router to connect to the Internet.

If your ISP supports DHCP

Your Netopia R9100 Ethernet Router comes preconfigured with the ability to accept an IP address dynamically assigned by your ISP. To do this, it acts as a Dynamic Host Configuration Protocol client to your ISP's DHCP server. This means that each time you power the Router on when it is connected to the Internet connection line, it configures itself with IP address settings without any input on your part. If your ISP supports this method, skip these instructions and go to Chapter 4, “Connecting to Your Local Area Network.” You don’t need to do anything else. This is the true Plug-and-Play solution.

If your ISP doesn’t support DHCP

Some ISPs may not be running a DHCP server. In this case, they may simply assign your router a Static IP Address and will supply you with several values for you to enter into the Router. The ISP will provide the values shown below:

Local WAN IP Address	
Local WAN IP Mask	
Default IP Gateway	
Domain Name	
Primary Domain Name Server	
Secondary Domain Name Server	

(You can record these values; print this page and use the spaces above.)

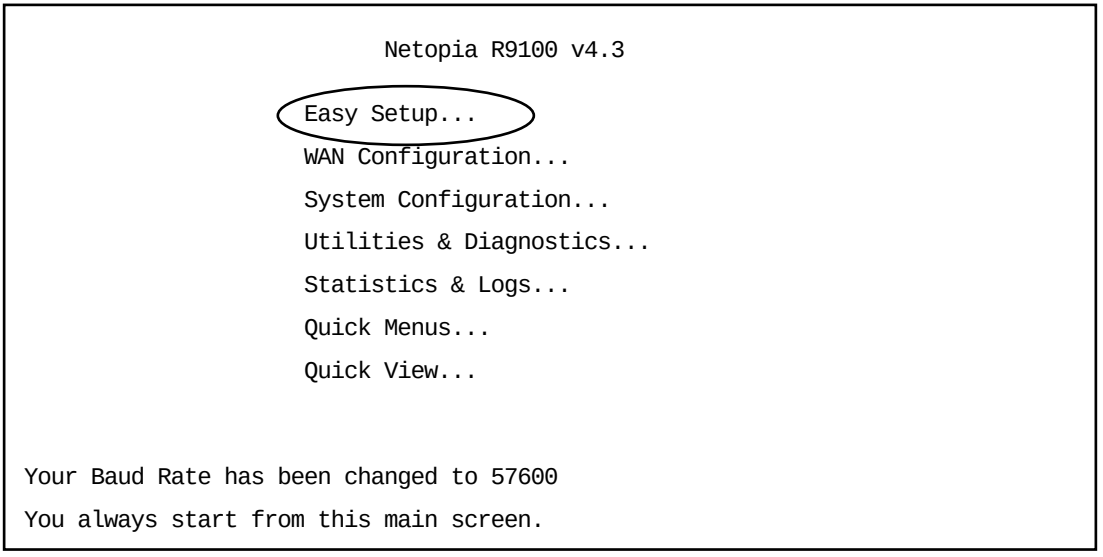
If your ISP assigns your Router a Static IP address, do the following:

1. From the computer connected to your router, as described in the section “Identify the connectors and attach the cables” on page 3-2, open a Telnet session to 192.168.1.1 to bring up the **Main Menu**.

   If you don't know how to do this, see “Connecting through a Telnet session” on page 6-2.

   Alternatively, you can connect the console cable and open a direct serial console connection, using a terminal emulator program. See “Connecting a console cable to your router” on page 6-3.

The Main Menu appears.



2. Select the first item on the Main Menu list, **Easy Setup**. Press Return to bring up the Easy Setup menu screen.
3. Press the Down arrow key until the editable field labelled **Local WAN IP Address** is highlighted.
4. Type the IP Address your ISP gave you. Press Return. The next field **Local WAN IP Mask** will appear.
5. Type the Subnet Mask your ISP gave you. Press Return.
6. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return to bring up the next screen.
7. Press the Down arrow key until the editable field labelled **Domain Name** is highlighted.
8. Type the Domain Name your ISP gave you. Press Return. The next field **Primary Domain Name Server** will be highlighted.
9. Type the Primary Domain Name Server address your ISP gave you. Press Return. A new field **Secondary Domain Name Server** will appear. If your ISP gave you a secondary domain name server address, enter it here. Press Return until the next field **Default IP Gateway** is highlighted.
10. Enter the Default IP Gateway address your ISP gave you. Press Return.
11. Press the Down arrow key until you reach **NEXT SCREEN**. Press Return.
12. Do this again, through the next two screens until you reach **RESTART DEVICE**. When RESTART DEVICE is highlighted, press Return. When prompted, select **CONTINUE**, and press Return.

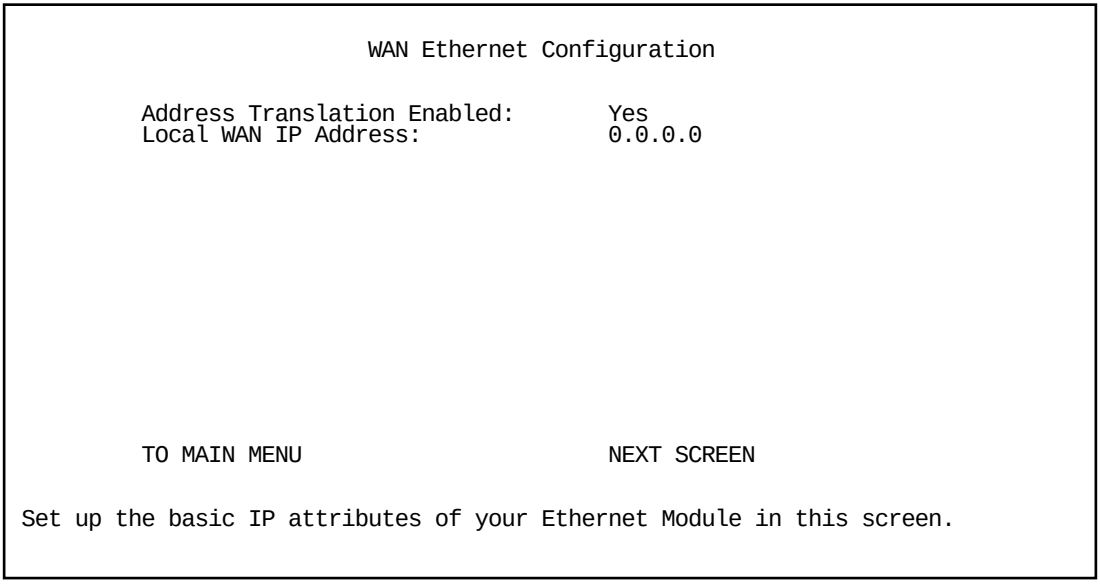
The router will restart and your configuration settings will be activated. You can then Exit or Quit your Telnet application.

For more Easy Setup options see "More Easy Setup options" on page 7-5.

More Easy Setup options

You always begin Easy Setup by selecting **Easy Setup** in the Main Menu, then pressing Return.

The WAN Ethernet Configuration screen appears.



WAN Ethernet Configuration

The WAN Ethernet Configuration screen is where you configure the parameters that control the Netopia R9100's connection to a specific remote destination, usually your ISP or a corporate site.

1. To enable address translation, toggle **Address Translation Enabled** to **Yes** (the default). For more information on Network Address Translation, see Chapter 9, "IP Setup and Network Address Translation," on page 9-1.

   Address Translation Enabled allows you to specify whether or not the router performs Network Address Translation (NAT) on the Ethernet WAN port. NAT is enabled by default.

2. To *manually* configure an IP address for use on the Ethernet WAN port, select **Local WAN IP Address** and enter the IP address you want to use.

   Otherwise, accept the default value 0.0.0.0. If you accept the default, the Netopia R9100 Ethernet Router will act as a DHCP client on the Ethernet WAN port and attempt to acquire an address from a DHCP server. By default, the router acts as a DHCP client on the Ethernet WAN port and obtains its IP address and subnet mask from the DHCP server.

3. A new field **Local WAN IP Mask** (not shown) becomes visible only if you have configured a non-zero Ethernet IP address. If you have configured a non-zero Ethernet IP address, enter an appropriate subnet mask.

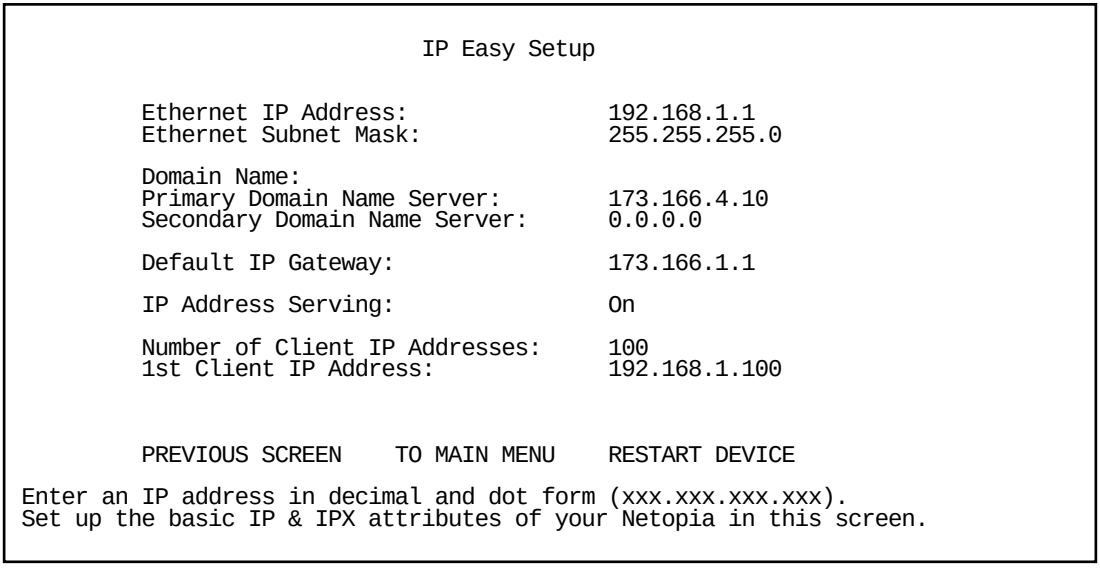
4. Select **NEXT SCREEN** and press Return. The IP Easy Setup screen appears.

IP Easy Setup

The IP Easy Setup screen is where you enter information about your Netopia Router's:

- Ethernet IP address
- Ethernet Subnet mask
- Domain Name
- Domain Name Server IP address
- Default gateway IP address
- Whether to serve IP addresses or not

Consult with your network administrator to obtain the information you will need. For more information about setting up IP, see "IP Setup and Network Address Translation" on page 9-1.



1. Select **Ethernet IP Address** and enter the first IP address from the IP address range your ISP has given you. This will be the Netopia Router's IP address.

   If Network Address Translation is enabled in Easy Setup, the Ethernet IP Address defaults to an address within a range reserved by the Internet address administration authority for use within private networks, 192.168.1.1.

   Because this is a private network address, it should never be directly connected to the Internet. Using NAT for all your WAN and IP configurations will ensure this restriction. See "IP Setup and Network Address Translation" on page 9-1 of this guide for more information.

2. Select **Ethernet Subnet Mask** and enter the subnet mask your ISP has given you. The Ethernet Subnet Mask defaults to a standard class mask derived from the class of the Ethernet IP address you entered in the previous step.

3. Select **Domain Name** and enter the domain name your ISP has given you.

Note: If the Netopia R9100's WAN interface is acting as a DHCP client, do not change the default settings for Steps 3, 4, and 5.

4. Select **Primary Domain Name Server** and enter the IP address your ISP has given you. An alternate or **Secondary Domain Name Server** field will appear, where you can enter a secondary DNS IP address if your ISP has given you one.
5. If you do not enter a **Default IP Gateway** value, the router defaults to the remote IP address you entered in Easy Setup. If the Netopia Router does not recognize the destination of any IP traffic, it forwards that traffic to this gateway.

   Do not confuse the remote IP address and the Default IP Gateway's address with the block of local IP addresses you receive from your ISP. You use the local IP addresses for the Netopia R9100's Ethernet port and for IP clients on your local network. The remote IP address and the default gateway's IP address should point to your ISP's router.
6. Toggle **IP Address Serving** to **On** or **Off**.
7. Select **NEXT SCREEN** and press Return. The Easy Setup Security Configuration screen appears.

Easy Setup Security Configuration

The Easy Setup Security Configuration screen lets you password-protect your Netopia R9100. Input your **Write Access Name** and **Write Access Password** with names or numbers totaling up to eleven digits.

If you password protect the console screens, you will be prompted to enter the name and password you have specified every time you log in to the console screens. Do not forget your name and password. If you do, you will be unable to access any of the configuration screens.

Additional security features are available. See "Security" on page 13-1.

```
                    Easy Setup Security Configuration

It is strongly suggested that you password-protect configuration access to your
Netopia. By entering a Name and Password pair here, access via serial,
Telnet, SNMP and Web Server will be password-protected.

Be sure to remember what you have typed here, because you will be prompted for
it each time you configure this Netopia.

You can remove an existing Name and Password by clearing both fields below.

         Write Access Name:

         Write Access Password:



         PREVIOUS SCREEN       TO MAIN MENU      RESTART DEVICE

Configure a Configuration Access Name and Password here.
```

The final step in configuring the Easy Setup console screens is to restart the Netopia R9100, so that the configuration settings take effect.

1. Select **RESTART DEVICE**. A prompt asks you to confirm your choice.

2. Select **CONTINUE** to restart the Netopia Router and have your selections take effect.

Note: You can also restart the system at any time by using the Restart System utility (see "Restarting the system" on page 14-12) or by turning the Netopia Router off and on with the power switch.

Easy Setup is now complete.

Part II: Advanced Configuration

Chapter 8

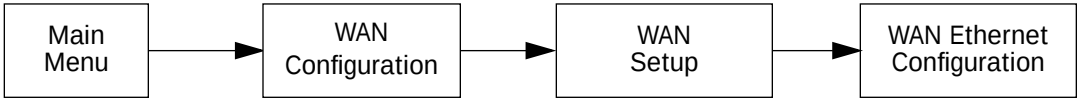
WAN and System Configuration

Console-based management is a menu-driven interface for the capabilities built in to the Netopia R9100. Console-based management provides access to a wide variety of features that the router supports. You can customize these features for your individual setup. This chapter describes how to access the console-based management screens.

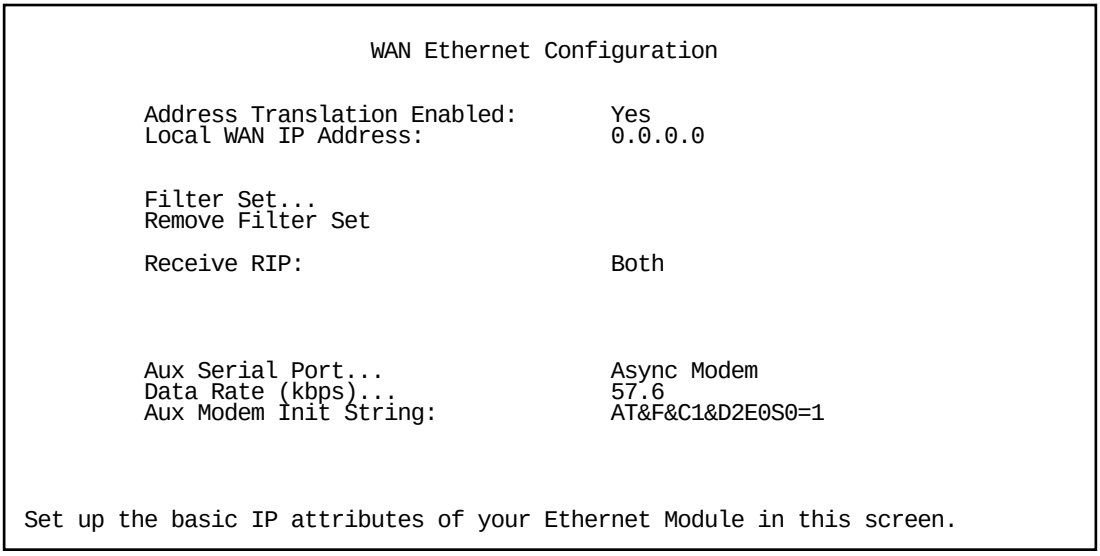
This section covers the following topics:

WAN configuration

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



The WAN Ethernet Configuration screen appears.



- **Address Translation Enabled** allows you to specify whether or not the router performs Network Address Translation (NAT) on the Ethernet WAN port. NAT is enabled by default.
- **Local WAN IP Address** allows you to manually configure an IP address for use on the Ethernet WAN port. The value 0.0.0.0 indicates that the device will act as a DHCP client on the Ethernet WAN port and attempt to acquire an address from a DHCP server. By default, the router acts as a DHCP client on the Ethernet WAN port.
- **Local WAN IP Mask** allows you to manually configure an IP subnet mask for use on the Ethernet WAN port. This item is visible only if you have configured a non-zero Ethernet IP Address; otherwise, the router obtains a subnet mask via DHCP.
- The **Filter Set** pop-up allows you to associate an IP filter set with the Ethernet WAN port. See "About filters and filter sets" on page 13-4.
- **Remove Filter Set** allows you to remove a previously associated filter set.
- The **Receive RIP** pop-up controls the reception and transmission of Routing Information Protocol (RIP) packets on the Ethernet WAN port. The default is Both. The Transmit RIP pop-up is hidden if NAT is enabled.

  Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R9100 needs to recognize. Set to "Both" (the default) the Netopia R9100 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to "v1," the Netopia R9100's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia R9100 will accept routing information provided by RIP packets from other routers that use different subnet masks.

If you want the Netopia R9100 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R9100 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R9100 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R9100 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

- Selecting **Aux Serial Port** displays the serial line configuration pop-up in which you specify the configuration for the router's auxiliary serial port.

  There are three options: Unused, LocalTalk, or Async Modem. The default for the auxiliary port is Async Modem for "Up & Running, Guaranteed" (URG). If you have installed the optional AppleTalk feature set the default is LocalTalk.

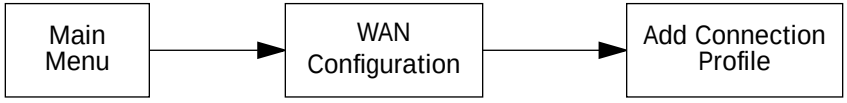
  For the Async Modem option (the default), the screen displays:

  - The **Data Rate** pop-up offers a limited set of clock rates: 19.2, 38.4, 57.6, 115.2, and 230.4. For broadest application, 57.6 is the default.
  - You may specify an **Aux Modem Init String** for your modem type.

Creating a new Connection Profile

For a Netopia R9100, Connection profiles are useful only on an asynchronous modem attached to the Auxiliary port. This requires enabling the Asynch modem feature set available as an add-on option (order TER/AD1). See the accompanying list of available add-on options in your product folio. If you have enabled the Auxiliary port option, you can create Connection Profiles. Otherwise, you can skip this section.

Connection Profiles define the telephone and networking protocols necessary for the router to make a remote connection. A Connection Profile is like an address book entry describing how the router is to get to a remote site, or how to recognize and authenticate a remote user dialing in to the router. For example, to create a new **Connection Profile**, you navigate to the **WAN Configuration** screen from the Main Menu, and select Add Connection Profile.



The **Add Connection Profile** screen appears.

```
                          Add Connection Profile

         Profile Name:                      Profile 02
         Profile Enabled:                   Yes

         IP Enabled:                        Yes
         IP Profile Parameters...

         IPX Enabled:                       No


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


         Telco Options...



         ADD PROFILE NOW                    CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
Configure a new Conn. Profile. Finished?  ADD or CANCEL to exit.
```

On a Netopia R9100 Ethernet Router you can add up to 15 more connection profiles, for a total of 16, but you can only use one at a time.

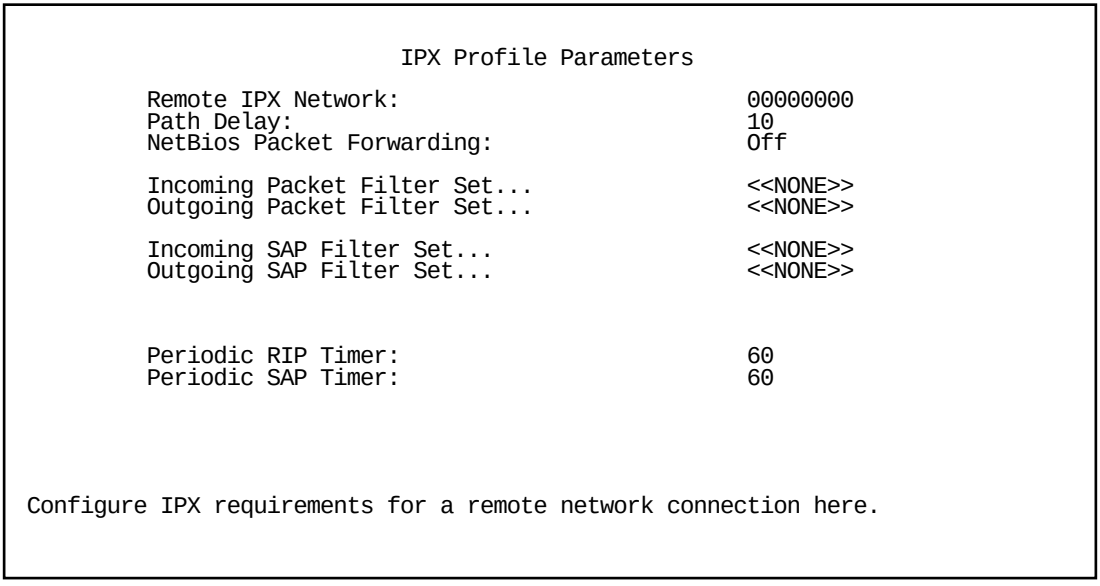
1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle the **Profile Enabled** value to Yes or No. The default is Yes.
3. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

```
                          IP Profile Parameters

         Address Translation Enabled:       Yes


         Local WAN IP Address:              0.0.0.0

         Remote IP Address:                 0.0.0.0
         Remote IP Mask:                    0.0.0.0

         Filter Set...
         Remove Filter Set

         Receive RIP:                       Off




Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.
```

4. Toggle or enter any IP Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see “IP Setup and Network Address Translation” on page 9-1.

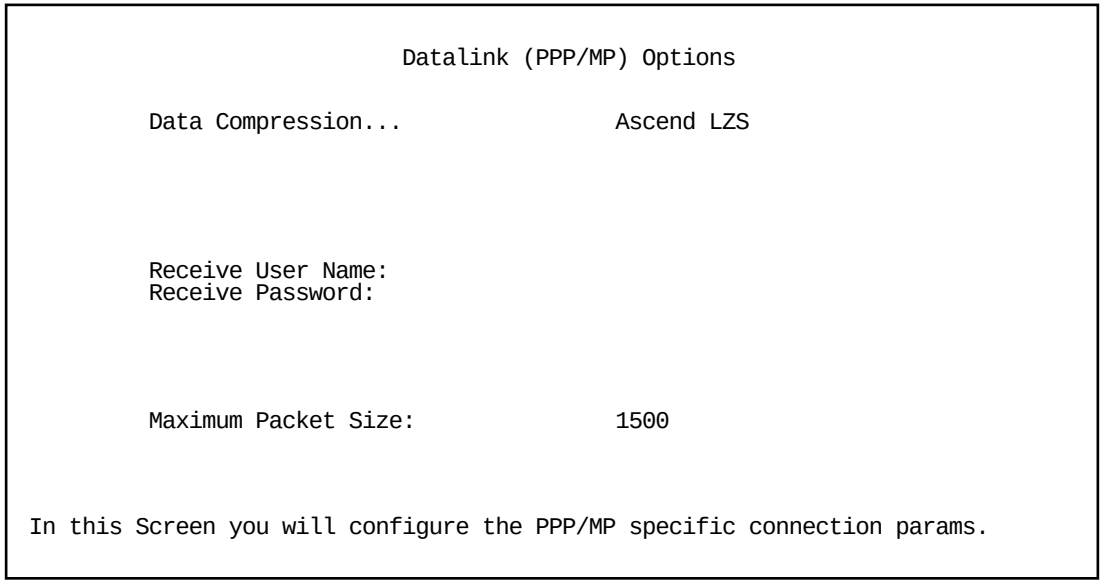
5. If you will be connecting with an IPX remote network, toggle **IPX Enabled** to Yes, and press Return. Otherwise, accept the default No.

   If you enable IPX routing, an **IPX Profile Parameters** menu item becomes available. Select IPX Profile Parameters and press Return. The IPX Profile Parameters screen appears.



6. Toggle or enter any IPX Parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information, see “IPX Setup” on page 10-1.

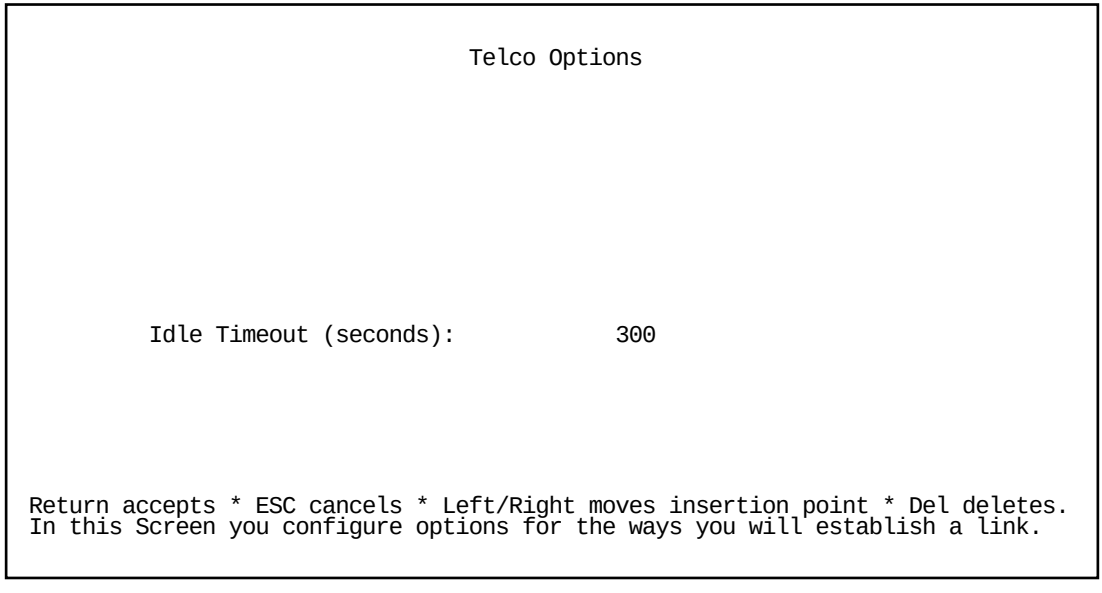
7. Select **Datalink Options** and press Return. The Datalink Options screen appears.



You can accept the defaults, or change them if you wish. You can also specify user name and password for both outgoing and incoming calls. the Send User Name/Password parameters are used to specify your identity when dialing out to a remote location. The Receive User Name/Password parameters are used when receiving dial-in clients such as via RAS configuration.

Return to the Add Connection Profile screen by pressing Escape.

8. Select **Telco Options** and press return. the Telco Options screen appears.

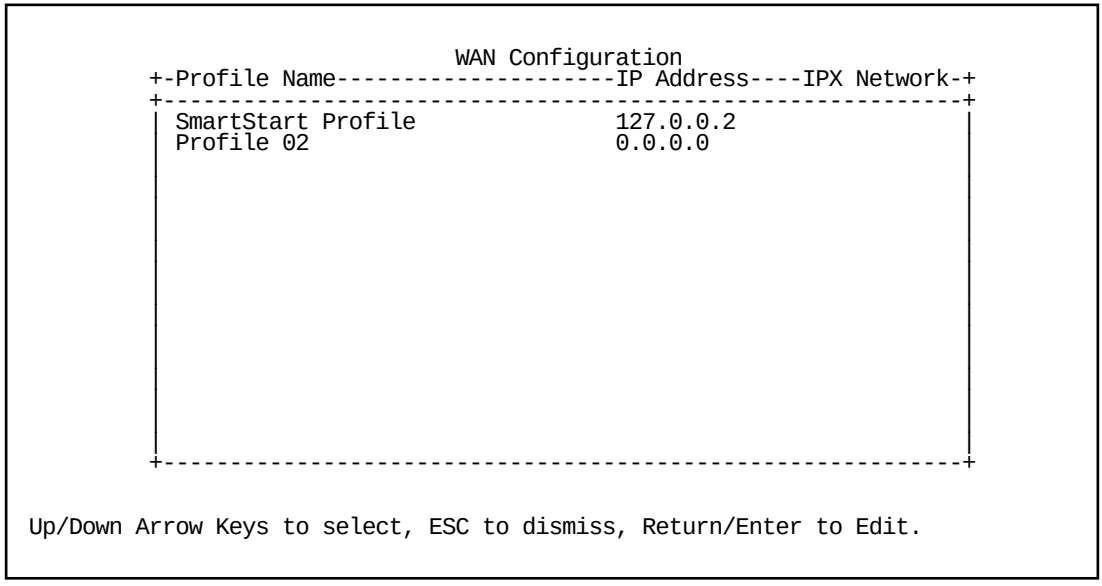


You can set the Idle timeout duration to be greater or less than the default 300 seconds (five minutes).

When you are finished with these entries, press Escape to return to the **Add Connection Profile** screen.

9. Select **ADD PROFILE NOW** and press Return. Your new Connection Profile will be added.

   If you want to view the Connection Profiles in your router, return to the WAN Configuration screen, and select **Display / Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.



Default Answer Profile for Dial-in Connections

The Netopia R9100 Ethernet Router can answer calls on the Auxiliary port. To answer calls, the Netopia R9100 uses a Default Answer Profile. The Default Answer Profile controls how incoming calls are set up, authenticated, filtered, and more.

How the Default Answer Profile works

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

The main criterion used to check calls is whether they match one of the Connection Profiles already defined. The default profile checks that the incoming call's name and password match the receive name and password of a Connection Profile.

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

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

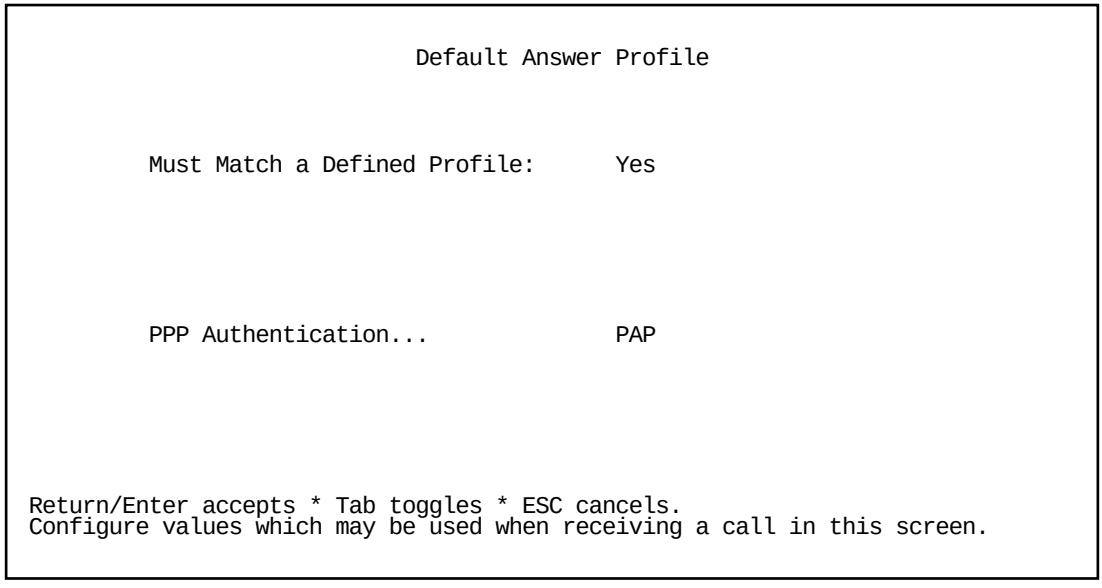
If an incoming call is not required to match a connection profile, and fails to do so, it is accepted as a standard IP connection. Accepted, unmatched calls adopt the call parameter values set in the Default Answer Profile.

To determine the call parameter values that unmatched calls will adopt, customize the Default Answer Profile parameters in the Default Answer Profile screen.

Customizing the default profile

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

1. Select **Default Answer Profile** in the WAN Configuration screen. Press Return. The Default Profile screen appears.



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

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

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

   If authentication in the Default Answer Profile is set to CHAP, the value of the **CHAP Challenge Name** item must be identical to the value of the **Send Host Name** item of the Connection Profile to be matched by the caller.

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

Class A addresses are assumed to have a mask of 255.0.0.0

Class B addresses are assumed to have a mask of 255.255.0.0

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

If a remote network has a non-standard mask (that is, it uses subnetting), the only way for it to successfully connect to the Netopia Router is by matching a connection profile. In other words, you will have to set up a connection profile for that network.If **Must Match a Defined Profile** is set to **No**, you can also set the following parameters for accepted calls that do not match a connection profile:

Call acceptance scenarios

The following are a few common call acceptance scenarios and information on how to configure the Netopia R9100 for those purposes.

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

  Note: The authentication method you choose determines which connection profiles are accessible to callers. For example, if you choose PAP, callers using CHAP or no authentication will be dropped by the answer profile.
- To allow calls that *only* match a connection profile's remote IP and/or IPX address:
  - Toggle **Must Match a Defined Profile** to **Yes**, *and*
  - set **Authentication** to **None**.

System configuration screens

You can connect to the Netopia R9100's system configuration screens in either of two ways:

- By using Telnet with the Router's Ethernet port IP address
- Through the console port, using a local terminal (see "Connecting a console cable to your router" on page 6-3)

You can also retrieve the Netopia R9100's configuration information and remotely set its parameters using the Simple Network Management Protocol (see "SNMP" on page 12-12).

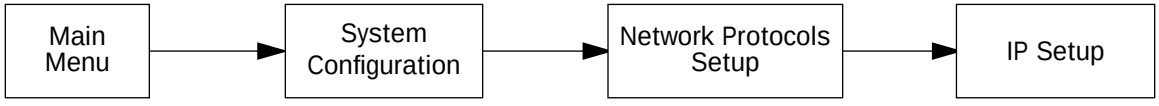
Open a Telnet connection to the router's IP address; for example, "192.168.1.1."

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

```
                        Netopia R9100 v4.3

                    Easy Setup...
                    WAN Configuration...
                    System Configuration...
                    Utilities & Diagnostics...
                    Statistics & Logs...
                    Quick Menus...
                    Quick View...



You always start from this main screen.
```

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:



This particular path guide shows how to get to the Network Protocols 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 **Network Protocols** and press Return. The Network Protocols screen appears.
3. Select **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 R9100 Ethernet Router's default settings may be all you need to configure your Netopia R9100. Some users, however, require advanced settings or prefer manual control over the default selections. For these users, the Netopia R9100 provides system configuration options.

To help you determine whether you need to use the system configuration options, review the following requirements. If you have one or more of these needs, use the system configuration options described in later chapters.

- System configuration of dynamic IP address distribution through DHCP, MacIP, or BootP
- Greater network security through the use of filters
- System configuration of AppleTalk LAN settings
- System configuration of connections to AppleTalk networks through the Internet or any IP network, using AURP (AppleTalk "tunneling")

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

The System Configuration menu screen appears:

```
                          System Configuration

                    Network Protocols Setup...
                    Filter Sets (Firewalls)...
                    IP Address Serving...

                    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.
```

Network protocols setup

These screens allow you to configure your network's use of the standard networking protocols:

- IP: Details are given in "IP Setup and Network Address Translation" on page 9-1.
- IPX: Details are given in "IPX Setup" on page 10-1.
- AppleTalk: Details are given in "AppleTalk Setup" on page 11-1.

  Note: AppleTalk requires the optional AppleTalk feature expansion kit.

Filter sets (firewalls)

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in "Security" on page 13-1.

IP address serving

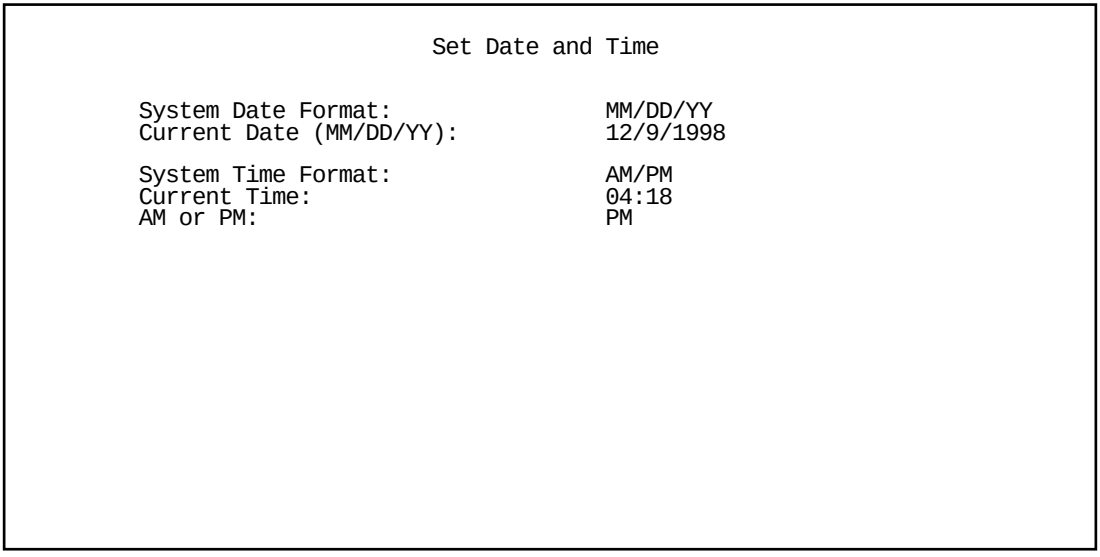
These screens allow you to configure IP address serving on your network by means of DHCP, WANIP, BootP, and with the optional AppleTalk kit, MacIP.

- Details are given in "IP address serving" on page 9-16.

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.



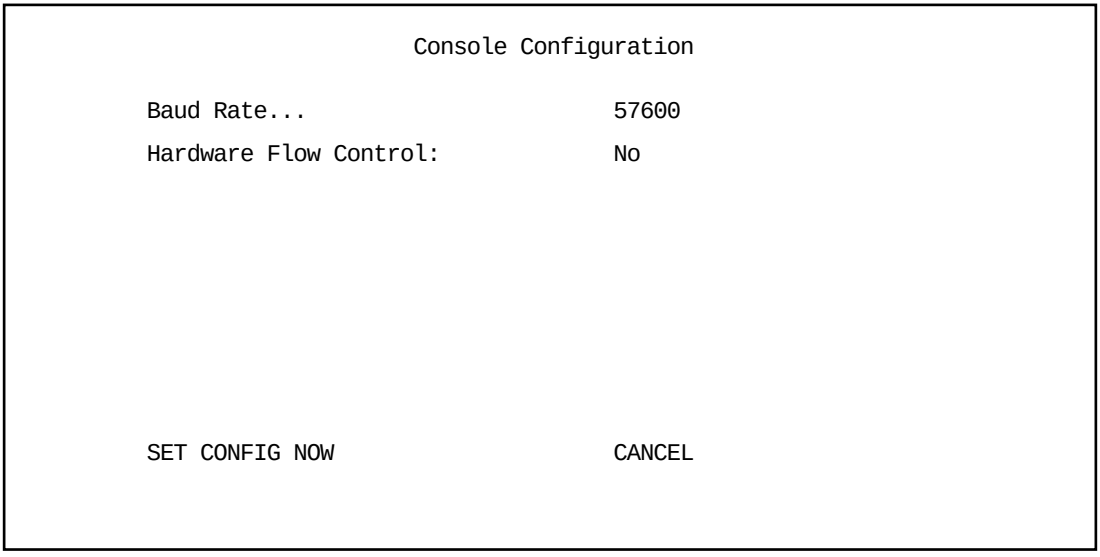
Follow these steps to set the system's date and time:

1. 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 (/).
2. 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.
3. Select **AM or PM** and choose **AM** or **PM**.

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.



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 12-12.

Security

These screens allow you to add users and define passwords on your network.

- Details are given in "Security" on page 13-1.

Upgrade feature set

You can upgrade your Netopia R9100 by adding new feature sets through the Upgrade Feature Set utility.

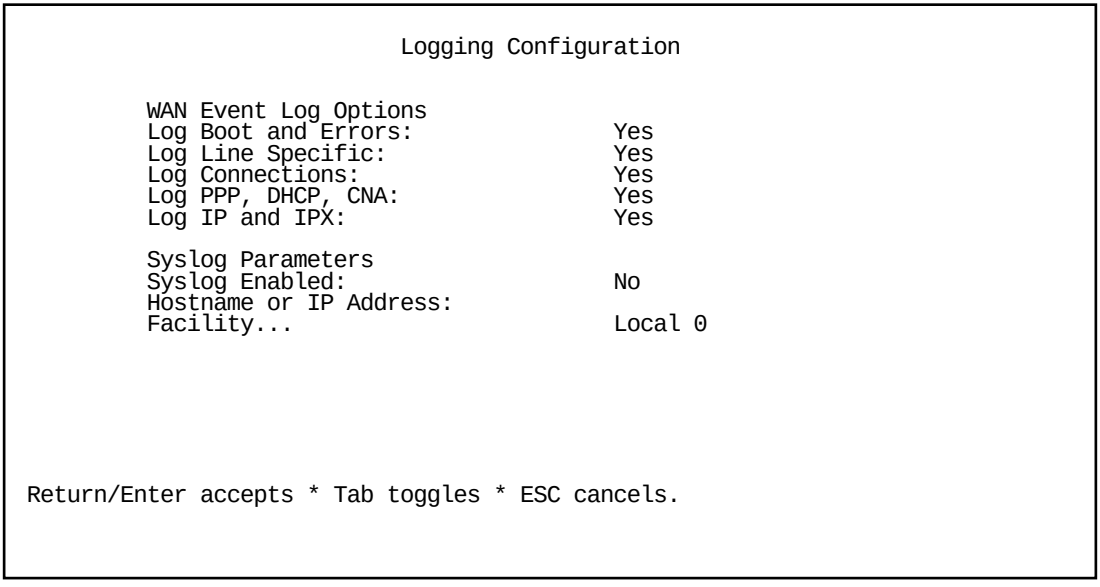
See the release notes that came with your router or feature set upgrade, or visit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Netopia R9100.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the router's WAN Event History. See "WAN Event History" on page 12-6.The Syslog client (for the PC only) is supplied as a .ZIP file on the Netopia CD.

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

The Logging Configuration screen appears.



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 Netopia 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 Netopia 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:

```
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: PPP PAP failure
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Manual disconnect
Nov  5 10:14:06 tsnext.netopia.com >>Issued Speech Setup Request from our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Requested Disc. from DN: 917143652500
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Confirm for our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: No answer
Nov  5 10:14:06 tsnext.netopia.com --Device restarted----------------------------------------
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
Nov  5 10:14:06 tsnext.netopia.com   Requested Connect to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   ASYNC: Modem carrier detected (more) Modem reports: 26400
V34
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 activated at 115 Kbps
Nov  5 10:14:06 tsnext.netopia.com   Connect Confirmed to our DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   PPP: Channel 1 up, Answer Profile name: Default Profile
Nov  5 10:14:06 tsnext.netopia.com    PPP: NCP up, session 1, Channel 1 Final (fallback)
negotiated auth: Local PAP , Remote NONE
Nov  5 10:14:06 tsnext.netopia.com   PPP: PAP  we accepted remote, Channel 1 Remote name: guest
Nov  5 10:14:06 tsnext.netopia.com    PPP: MP negotiated, session 1 Remote EDO: 06 03
0000C5700624 0
Nov  5 10:14:06 tsnext.netopia.com   PPP: CCP negotiated, session 1, type: Ascend LZS Local
mode: 1, Remote mode: 1
Nov  5 10:14:06 tsnext.netopia.com   PPP: BACP negotiated, session 1 Local MN: FFFFFFFF, Remote
MN: 00000001
Nov  5 10:14:06 tsnext.netopia.com   PPP: IPCP negotiated, session 1, rem: 192.168.10.100 local:
192.168.1.1
Nov  5 10:14:06 tsnext.netopia.com >>WAN: 56K Modem 1 deactivated
Nov  5 10:14:06 tsnext.netopia.com   Received Clear Ind. from DN: 5108645534, Cause: 0
Nov  5 10:14:06 tsnext.netopia.com   Issued Clear Response to DN: 5108645534
Nov  5 10:14:06 tsnext.netopia.com   Link 1 down: Remote clearing
Nov  5 10:14:06 tsnext.netopia.com   PPP: IPCP down, session 1
Nov  5 10:14:06 tsnext.netopia.com >>Received Speech Setup Ind. from DN: (not supplied)
```

Chapter 9

IP Setup and Network Address Translation

The Netopia R9100 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the Router to route IP traffic. You also learn how to configure the router to serve IP addresses to hosts on your local network.

Netopia's SmartIP features IP address serving and Network Address Translation. For a detailed discussion of Network Address Translation, see Appendix C, "Understanding Netopia NAT Behavior" This chapter describes how to use the Network Address Translation feature of SmartIP.

This section covers the following topics:

Network Address Translation allows communication between the LAN connected to the Netopia R9100 and the Internet using a single IP address instead of a routed account with separate IP addresses for each computer on the network.

Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia R9100 from the outside world.

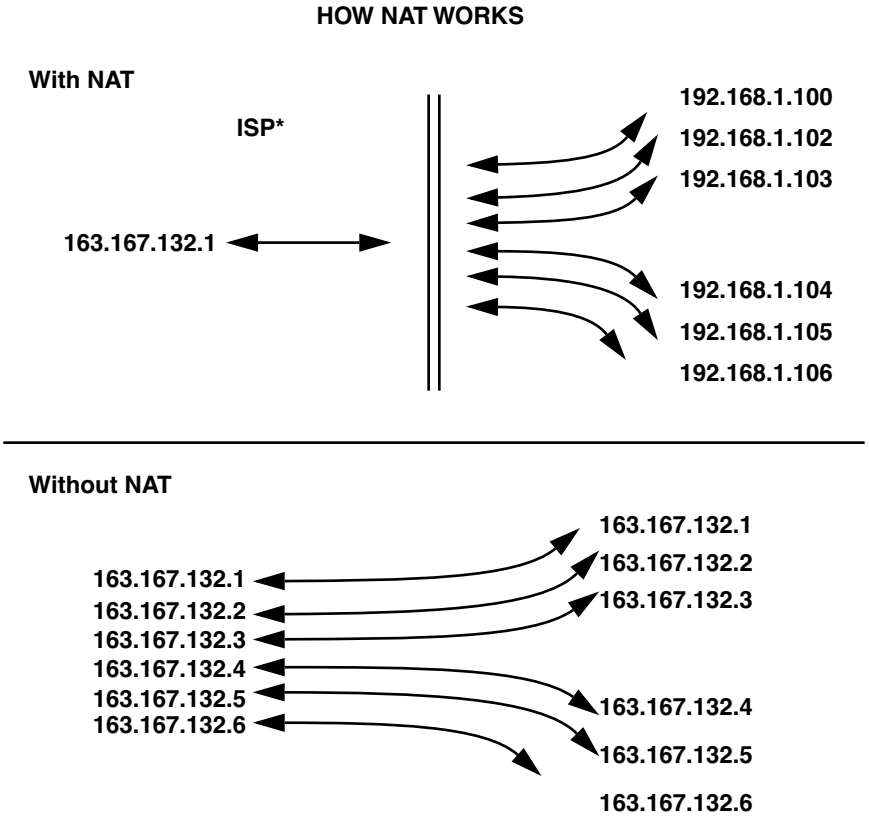
With SmartIP, the setup is simpler, so Internet service providers typically offer internet accounts supporting Network Address Translation at a significant cost savings.

Network Address Translation features

Network Address Translation (NAT) offers users the following features:

- The single proxy address is acquired at connection time from the answering side. The address can be assigned by the remote router from either a dynamic pool of addresses or a fixed, static address.
- Static NAT Security is simpler and more reliable because only one IP address needs a firewall, and because the internal network structure is not visible from the Internet.

Network Address Translation works by remapping the source IP address of traffic from the LAN to a single static or dynamically assigned IP address shown to the remote side of the router.



When NAT is enabled, the Netopia R9100 can use either a statically assigned IP address or one dynamically assigned each time the router connects to the ISP. While a dynamically assigned IP address offers the ISP more flexibility, it does have an important limitation: the router requires a static IP address to support Web, FTP, or other services available to the WAN. To support these services with NAT enabled, a service can be associated with only one machine on the LAN.

When connected to the Internet or some other large network using Network Address Translation, the individual machines on your LAN are not directly accessible from the WAN. NAT provides an inherently secure method of connection to the outside world.

Using Network Address Translation

The following procedure describes how to use Network Address Translation.

1. Pick a network number for your local network (referred to as the internal network). This can be any IP address range you want. The Netopia R9100 Ethernet Router has a default IP address of 192.168.1.1. You may choose to change this address to match a pre-existing addressing scheme. For this example, we will use 10.0.0.0.

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

2. Using the internal network number, assign addresses to the local nodes on your LAN. For example, you could assign

   - 10.0.0.1 to your Netopia R9100
   - 10.0.0.2 to a node running as a World Wide Web server
   - 10.0.0.3 to an FTP server
   - 10.0.0.4 to a Windows NT PC
   - 10.0.0.5 to a Windows 95 PC

   Note: See "Associating port numbers with nodes" on page 9-5.

3. By default, Network Address Translation is enabled in the Netopia R9100. If you disabled it and now want to reenable it:

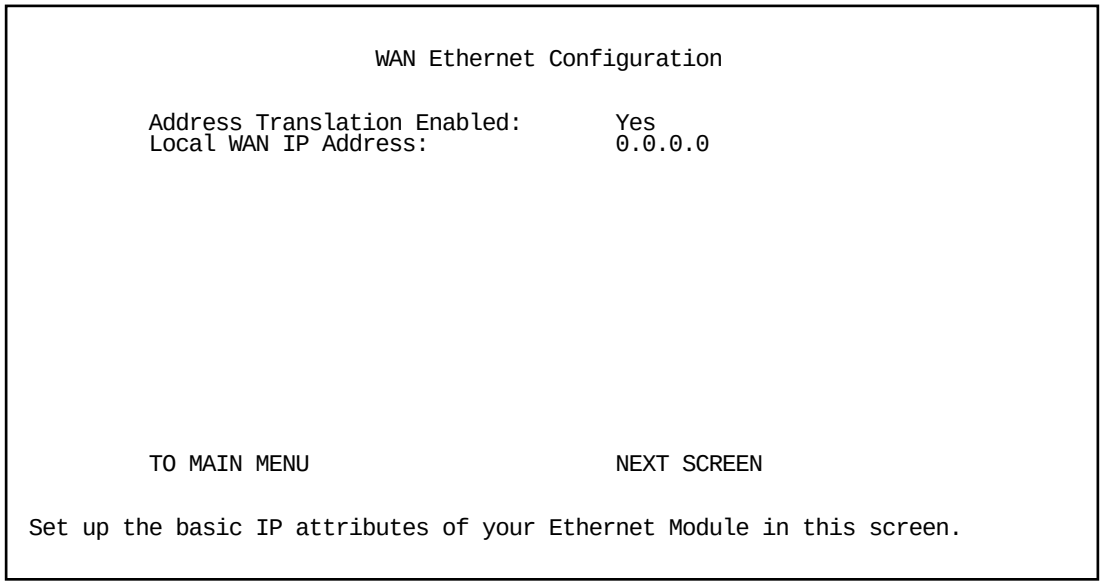
   From the WAN Configuration menu in the Main Menu screen, select **WAN (Wide Area Network) Setup**.

   The WAN Ethernet Configuration screen appears.

```
                          WAN Ethernet Configuration

          Address Translation Enabled:       Yes
          Local WAN IP Address:              0.0.0.0


          Filter Set...
          Remove Filter Set

          Receive RIP:                       Both



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



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

   Toggle **Address Translation Enabled** to **Yes** or **No** (Yes to enable NAT) and press Return.

Or, from the Main Menu, select **Easy Setup**. The Easy Setup WAN Ethernet Configuration screen appears.



Toggle **Address Translation Enabled** to **Yes** or **No** (Yes to enable NAT) and press Return.

For more information see Appendix B, "Understanding IP Addressing" and Appendix C, "Understanding Netopia NAT Behavior"

4. If your ISP uses numbered (interface-based) routing, select **Local WAN IP Address** and enter the local WAN address your ISP gave you. Then select **Local WAN IP Mask** and enter the WAN subnet mask of the remote site you will connect to.

   The default address is 0.0.0.0, which allows for dynamic addressing, meaning that your ISP assigns an address via DHCP each time you connect. However, if you want to use static addressing, enter a specific address.

Associating port numbers with nodes

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

For example, a Web browser locates a Web server by using a combination of the IP address and TCP port that the client machine has set up. Just as an IP address specifies a particular computer on a network, ports are addresses that specify a particular service in a computer. There are many universally agreed-upon ports assigned to various services. For example:

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

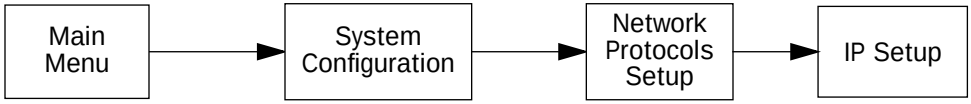
To help direct incoming IP traffic to the appropriate server, the Netopia R9100 lets you associate these and other port numbers with distinct IP addresses on your internal LAN using exported services. See “IP setup” on page 9-6 for details.

Network Address Translation guideline

Observe the following guideline when using Network Address Translation.

The router can export only one local IP address per UDP/TCP port, so you can have just one machine available for a given service, such as one FTP server. However, some services, such as Web servers (www-http servers), allow you to change the UDP/TCP port on both the server and client. With two different UDP/TCP ports exported, you can have Web servers on two different IP hosts.

IP setup



The IP Setup options screen is where you configure the Ethernet side of the Netopia R9100. The information you enter here controls how the router routes IP traffic.

Consult your network administrator or Internet service provider to obtain the IP setup information (such as the Ethernet IP address, Ethernet subnet mask, default IP gateway and Primary Domain Name Server IP address) you will need before changing any of the settings in this screen. Changes made in this screen will take effect only after the Netopia R9100 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**.

The IP Setup screen appears.

```
                                IP Setup

        Ethernet IP Address:              192.128.117.162
        Ethernet Subnet Mask:             255.255.255.0
        Define Additional Subnets...

        Default IP Gateway:               192.128.117.163

        Primary Domain Name Server:       0.0.0.0
        Secondary Domain Name Server:     0.0.0.0
        Domain Name:

        Receive RIP:                      Both
        Transmit RIP:                     v2 (multicast)
        Static Routes...

        Address Serving Setup...
        Exported Services...
        Filter Sets...

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

Follow these steps to configure IP Setup for your Netopia R9100:

- Select **Ethernet IP Address** and enter the IP address for the Netopia R9100's Ethernet port.
- Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP address that you entered in the last step.
- For unlimited-user models, if you desire multiple subnets select **Define Additional Subnets**. 12-user models do not offer this option. If you select this item you will be taken to the IP Subnets screen. This screen allows you to define IP addresses and masks for additional subnets. See "IP subnets" on page 9-10 for details.

The Netopia R9100 Ethernet Router supports multiple IP subnets on the Ethernet interface. You may want to configure multiple IP subnets to service more hosts that are possible with your primary subnet. It is not always possible to obtain a larger subnet from your ISP. For example, if you already have a full Class C subnet, your only option is multiple Class C subnets, since it is virtually impossible to justify a Class A or Class B assignment. This assumes that you are not using NAT.

If you are using NAT, you can use the reserved Class A or Class B subnet.

- 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 R9100.

  A default gateway should be able to successfully route packets when the Netopia R9100 cannot recognize the intended recipient's IP address. A typical example of a default gateway is the ISP's router.

- Select **Primary Domain Name Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP routers (for example, 163.7.8.202).

- If a secondary DNS server is available, select **Secondary Domain Name Server** and enter its IP address. The secondary DNS server is used by the Netopia R9100 when the primary DNS server is inaccessible. Entering a secondary DNS is useful but not necessary.

- Select **Domain Name** and enter your network's domain name (for example, netopia.com).

- Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia R9100 needs to recognize. If this is the case select **Receive RIP** and select **v1**, **v2**, or **Both** from the popup menu. With Receive RIP set to "v1," the Netopia R9100's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia R9100 will accept routing information provided by RIP packets from other routers that use different subnet masks. Set to "Both," the Netopia R9100 will accept information from either RIP v1 or v2 routers.

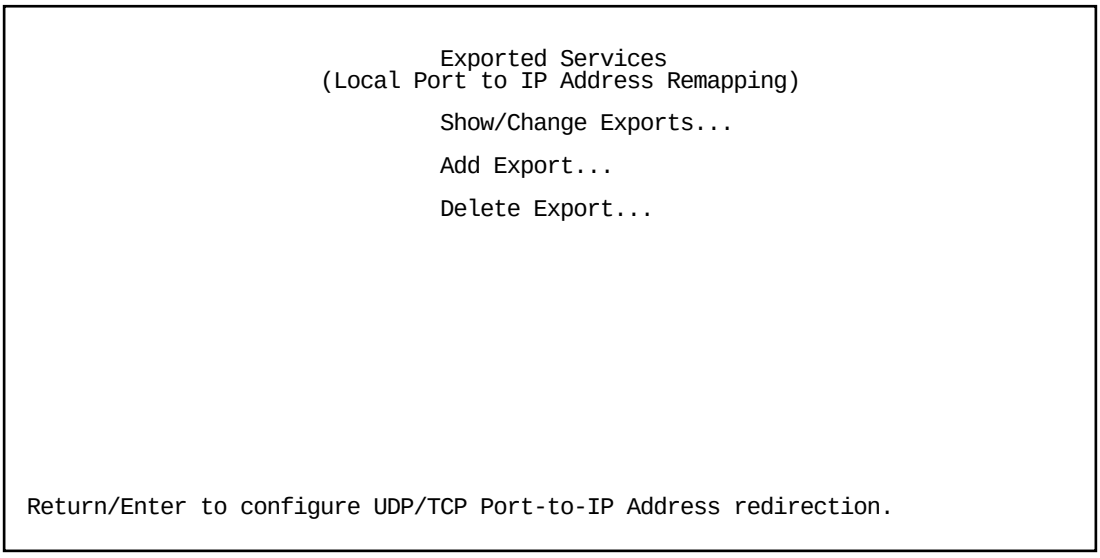
- If you want the Netopia R9100 to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia R9100 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia R9100 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia R9100 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

- Select **Static Routes** to manually configure IP routes. See the section "Static routes," below.

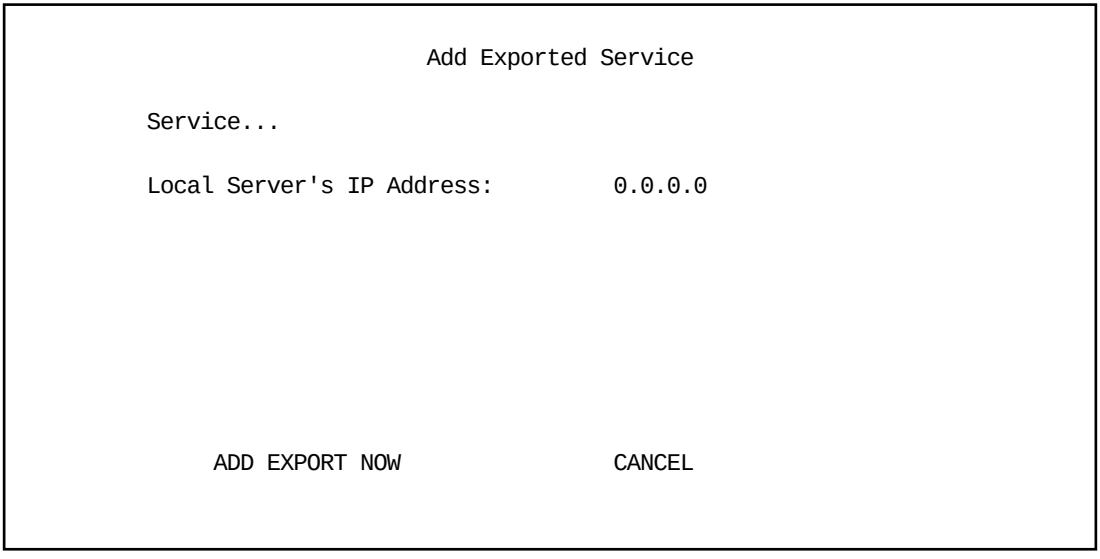
- If you select **Address Serving Setup** you will be taken to the IP Address Serving screen (see "IP address serving" on page 9-16. Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R9100, and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

- Select **Exported Services.** The Exported Services screen appears with three options: Show/Change

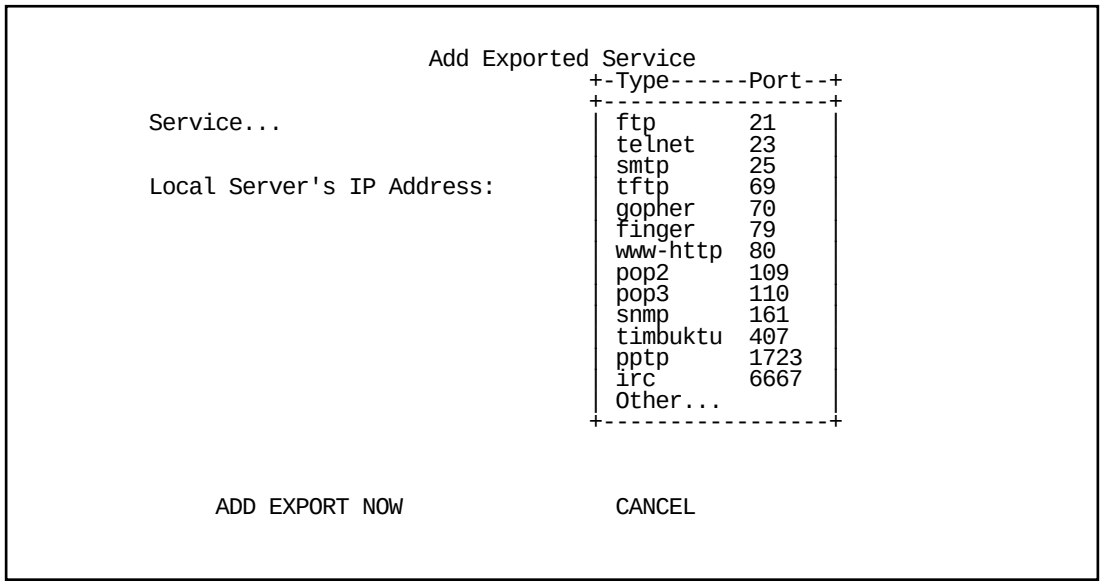
Exports, Add Export, and Delete Export.



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



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



5. Select any of the services/ports and press Return to associate it with the address of a server on your local area network. For example, if we select **www-http 80**, press Return, and type **10.0.0.2**, the Netopia R9100 redirects any incoming traffic destined for a Web server to address 10.0.0.2.

   Some services such as Timbuktu require the export of multiple TCP ports. When you associate Timbuktu with a local server (or Timbuktu host) all of the major Timbuktu services are exported, i.e., Observe, Control, Send, and Exchange.

Note: If the TCP port of a service you want to use is not listed, you can add it by selecting **Other...** on the pop-up menu.

Press Escape when you are finished configuring exported services. You are returned to the IP Setup screen.

```
                              IP Setup

Ethernet IP Address:                  192.128.117.162
Ethernet Subnet Mask:                 255.255.255.0
Define Additional Subnets...

Default IP Gateway:                   192.128.117.163

Primary Domain Name Server:           0.0.0.0
Secondary Domain Name Server:         0.0.0.0
Domain Name:

Receive RIP:                          Both
Transmit RIP:                         v2 (multicast)
Static Routes...

Address Serving Setup...
Exported Services...
Filter Sets...
```

- If you select **Filter Sets** you will be taken directly to the screen for configuring IP packet filters. For information see "About filters and filter sets," beginning on page 13-4.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets on unlimited-user models, one "primary" subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:

```
                          IP Subnets

      IP Address          Subnet Mask
      ---------------     --------------
#1:   192.128.117.162     255.255.255.0
#2:   0.0.0.0             0.0.0.0
#3:
#4:
#5:
#6:
#7:
#8:
```

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Netopia R9100's IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

  For example:

```
                        IP Subnets

      IP Address          Subnet Mask
      ---------------     --------------
#1:   192.128.117.162     255.255.255.0
#2:   192.128.152.162     255.255.0.0
#3:   0.0.0.0             0.0.0.0
#4:
#5:
#6:
#7:
#8:
```

- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return or Enter to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

Note that the subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:

```
                              IP Setup



        Subnet Configuration...

        Default IP Gateway:                192.128.117.163

        Primary Domain Name Server:        0.0.0.0
        Secondary Domain Name Server:      0.0.0.0
        Domain Name:

        Receive RIP:                       Both
        Transmit RIP:                      v2 (multicast)
        Static Routes...

        Address Serving Setup...
        Exported Services...
        Filter Sets...
```

The IP address and Subnet mask items are hidden, and the "Define Additional Subnets..." item becomes "Subnet Configuration...". If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

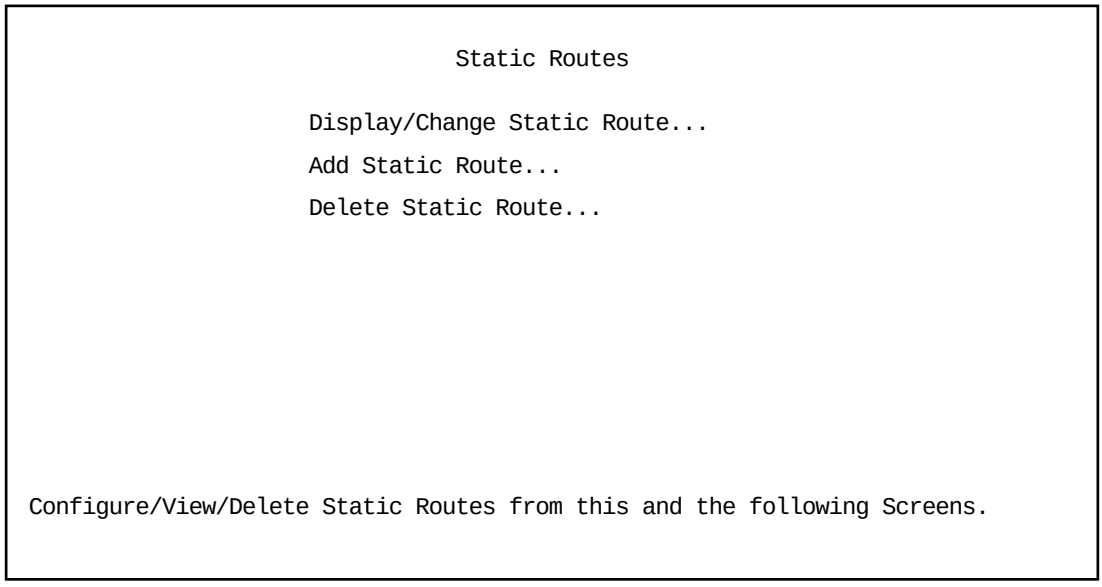
Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Netopia R9100 how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Netopia R9100 (see "IP routing table" on page 12-8).

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

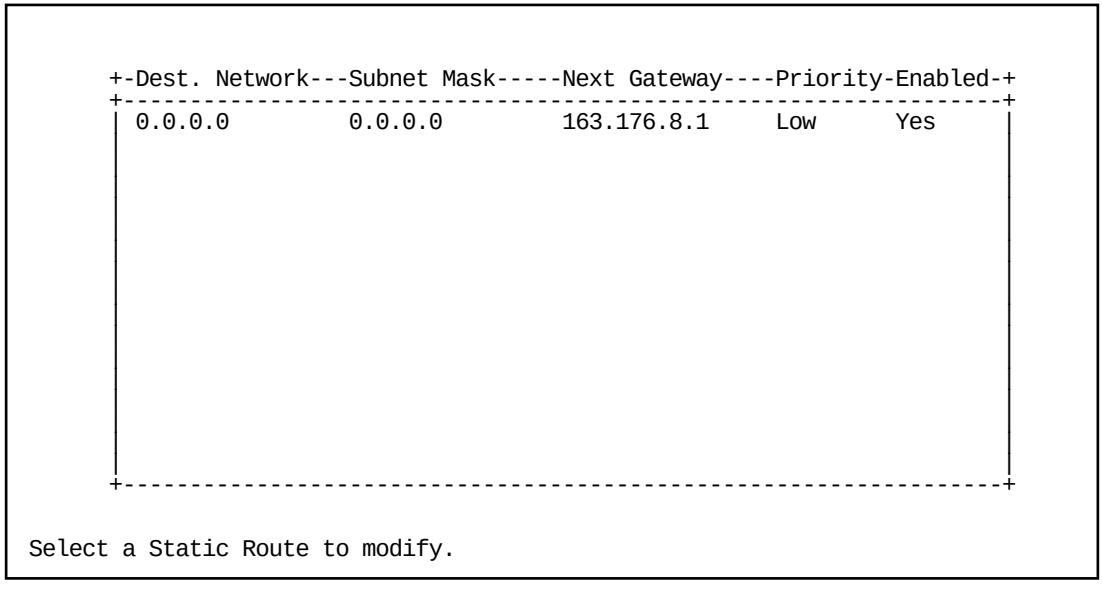
To go to the Static Routes screen, select **Static Routes** in the **IP Setup** screen.

The Static Routes screen will appear.



Viewing static routes

To display a view-only table of static routes, select **Display / Change Static Route**. The table shown below will appear.



The table has the following columns:

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

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

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

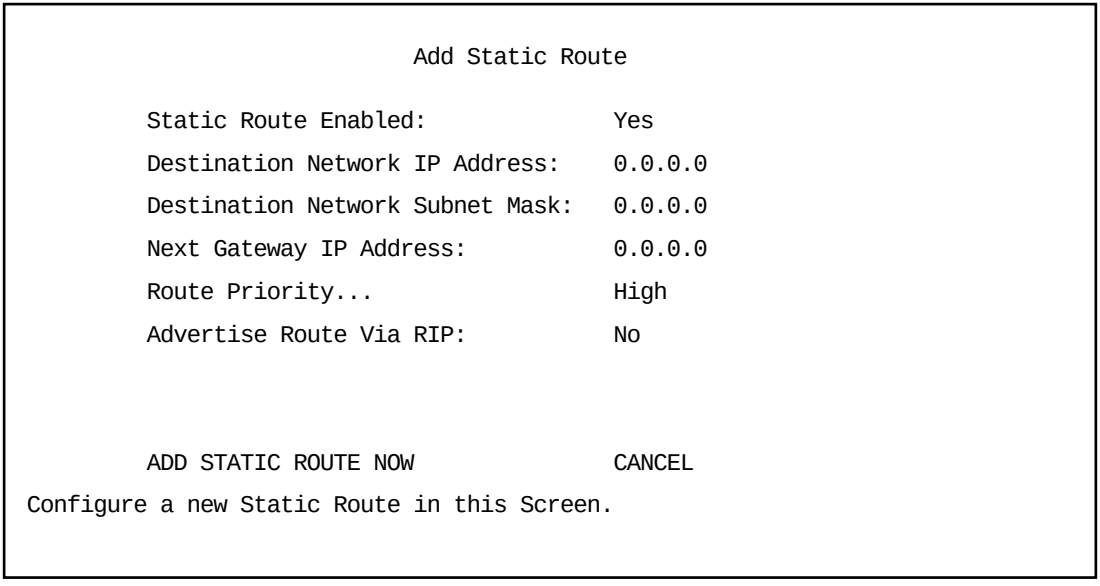
Priority: An indication of whether the Netopia R9100 will use the static route when it conflicts with information received from RIP packets.

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

To return to the Static Routes screen, press Escape.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen. The Add Static Route screen will appear.



- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See "Rules of static route installation" on page 9-15.
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the router that the Netopia R9100 will use to reach the destination network. This router does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. **High** means that the static route takes precedence over RIP information; **Low** means that the RIP information takes precedence over the static route.
- To make sure that the static route is known only to the Netopia R9100, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable routers to know about the static route, select **Advertise**

Route Via RIP and toggle it to **Yes**. When Advertise Route Via RIP is toggled to Yes, a new item called RIP Metric appears below Advertise Route Via RIP.

With RIP Metric you set the number of routers, from 1 to 15, between the sending router and the destination router. The maximum number of routers on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 routers, while setting it to **15** means a route can only involve one router.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 16 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in system configuration.

Modifying a static route

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

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see "Adding a static route" on page 9-14).

Deleting a static route

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

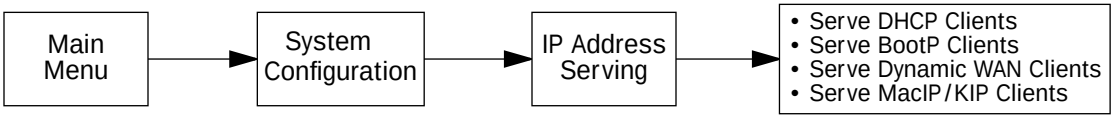
Rules of static route installation

The Netopia R9100 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches the IP address used by the Netopia R9100's Ethernet port.
- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by MacIP or DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Netopia R9100.

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

IP address serving



In addition to being a router, the Netopia R9100 is also an IP address server. There are four protocols it can use to distribute IP addresses.

- The first, called **Dynamic Host Configuration Protocol (DHCP)**, is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are "leased" or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called **BootP** (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BootP address assignments are "permanent" since there is no lease renewal mechanism in BootP.
- The third protocol, called **Dynamic WAN**, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled routers to be assigned a temporary IP address for the duration of their connection.
- The fourth protocol, called **MacIP**, is used only for computers on AppleTalk networks. MacIP provides a protocol translation (or gateway) function between IP and AppleTalk as well as an IP address assignment mechanism. Like DHCP, MacIP address assignments are normally temporary, although you can also use static IP addresses with MacIP.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Netopia R9100 and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

Go to the System Configuration screen. Select **IP Address Serving** and press Return. The IP Address Serving screen will appear.

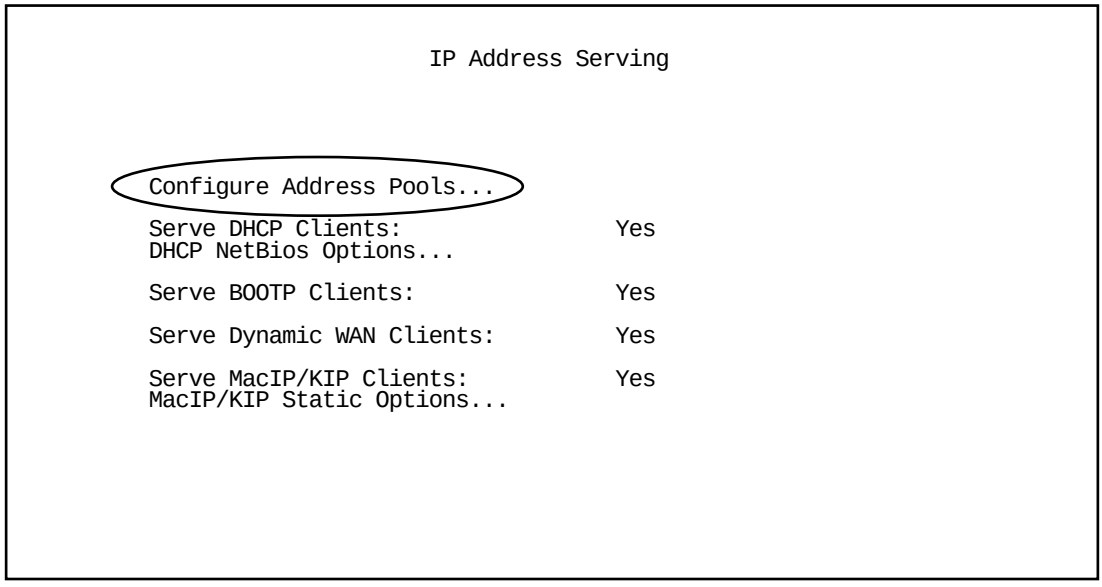
```
                        IP Address Serving

Number of Client IP Addresses:     5
1st Client Address:                176.163.222.10
Client Default Gateway...          176.163.222.1


Serve DHCP Clients:                Yes
DHCP NetBios Options...

Serve BOOTP Clients:               Yes



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

Follow these steps to configure IP Address Serving:

- If you enabled IP Address Serving, DHCP, BootP clients, Dynamic WAN clients, and MacIP/KIP clients (if you have the AppleTalk kit installed) are automatically enabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Netopia R9100 will distribute to the client machines on your local area network. 12-user models are limited to twelve IP addresses.
- In the screen example shown above, five Client IP addresses have been allocated.
- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may want to first figure out what machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BootP, Dynamic WAN, and/or MacIP.

  Example: Your ISP has given your Netopia R9100 the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet (for more information on IP addressing refer to Appendix B, “Understanding IP Addressing”). Your address range will be from **.137-.143**. In this example you would enter **192.168.6.138** as the 1st Client Address, since the router itself must have an IP address.
- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.

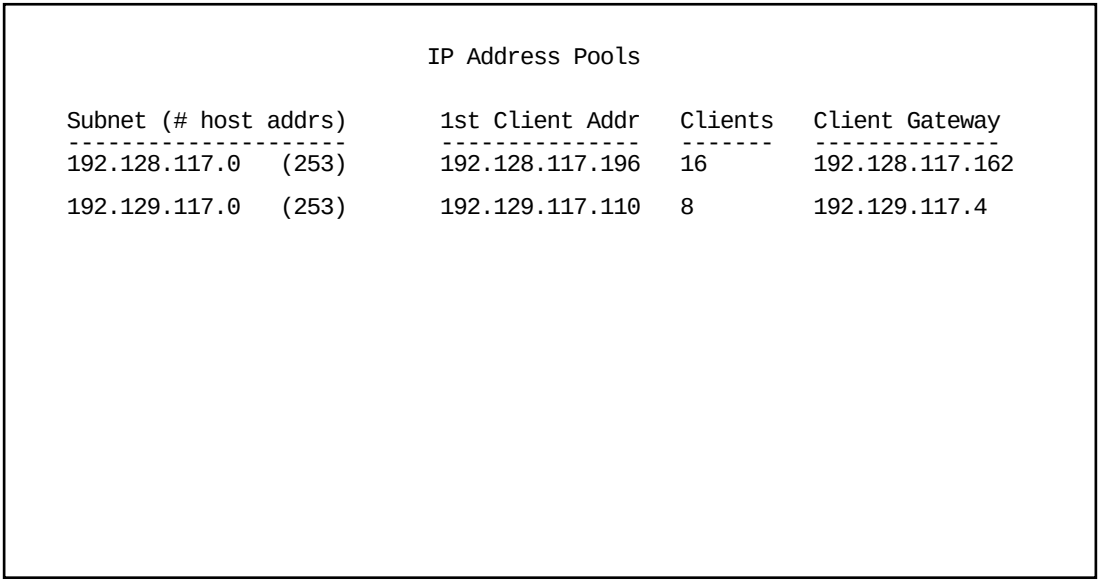
If you have configured multiple Ethernet IP subnets, the appearance of the IP Address Serving screen is altered slightly:



The first three menu items are hidden, and Configure Address Pools appears instead. If you select **Configure Address Pools** you will be taken to the IP Address Pools screen that allows you to configure an address serving pool for each of the configured Ethernet IP subnets. See "IP Address Pools," in the next section.

IP Address Pools

The IP Address Pools screen allows you to configure a separate IP address serving pool for each of up to eight configured Ethernet IP subnets:



This screen consists of between two and eight rows of four columns each. There are exactly as many rows as there are Ethernet IP subnets configured on the IP Subnets screen.

- The Subnet (# host addrs) column is non-selectable and non-editable. It indicates the network address of the Ethernet IP subnet for which an address pool is being configured and the number of host addresses available on the subnet. The network address is equal to the router's IP address on the subnet bitwise-ANDed with the subnet mask. The host address count is equal to the subnet size minus three, since one address is reserved for the network address, one for the subnet broadcast address, and one for the router's interface address on the subnet.

  You can edit the remaining columns in each row.

- The 1st Client Addr and Clients columns allow you to specify the base and extent of the address serving pool for a particular subnet. Entering 0.0.0.0 for the first client address or 0 for the number of clients indicates that no addresses will be served from the corresponding Ethernet IP subnet.

- The Client Gateway column allows you to specify the default gateway address that will be provided to clients served an address from the corresponding pool. The value defaults to the Netopia R9100's IP address on the corresponding subnet (or the Netopia R9100's default gateway, if that gateway is located on the subnet in question). You can override the value by entering any address that is part of the subnet.

  DHCP, BootP, dynamic WAN, and dynamic MacIP clients may receive an address from any one of the address serving pools configured on this screen. Static MacIP clients are not "served" addresses, but must be manually configured with addresses from within the specific range of addresses reserved for that purpose on the MacIP (KIP) Forwarding Setup screen See "MacIP (KIP forwarding) setup" on page 9-23.

Numerous factors influence the choice of served address. It is difficult to specify the address that will be served to a particular client in all circumstances. However, when the address server has been configured, and the clients involved have no prior address serving interactions, the Netopia R9100 will generally serve the first unused address from the first address pool with an available address. The Netopia R9100 starts from the pool on the first row and continues to the pool on the last row of this screen.

Once the address server and/or the clients have participated in address serving transactions, different rules apply:

- When requesting an address, a client will often suggest an address to be assigned, such as the one it was last served. The Netopia R9100 will attempt to honor this request if the address is available. The client stores this address in non-volatile storage, for example, on disk, and the specific storage method/location differs depending on the client operating system.
- When requesting an address, a client may provide a client identifier, or, if it does not, the Netopia R9100 may construct a pseudo-client identifier for the client. When the client subsequently requests an address, the Netopia R9100 will attempt to serve the address previously associated with the client identifier. This is normally the last address served to the client.
- Otherwise, the Netopia will select the least-recently used available address, starting from the first address in the first pool and ending with the last address in the last pool.

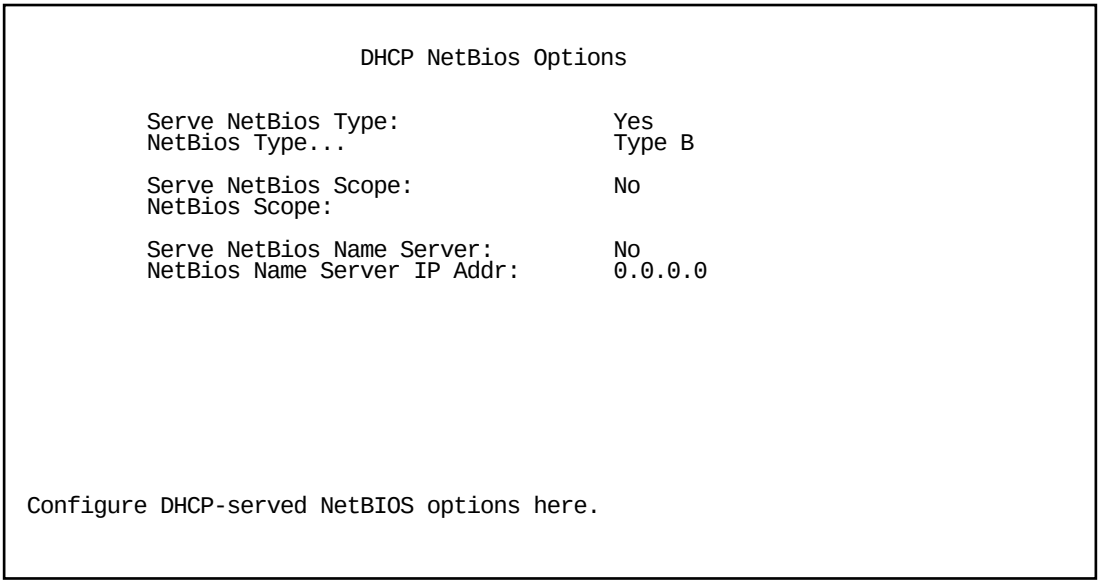
Note that the address serving pools on this screen are tied to the IP subnets configured on the IP Subnets screen. Changes to the IP Subnets screen may affect this one. In particular, deleting a subnet on the IP Subnets screen will delete the corresponding address serving pool, if any, on this screen.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Netopia R9100 to use DHCP to distribute NetBIOS information.

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

- Select **DHCP NetBios Options** and press Return. The DHCP NetBIOS Options screen appears.



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

- From the **NetBios Type** pop-up menu, select the type of NetBIOS used on your network.

```
                    DHCP NetBios Options

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

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

  Select **NetBios Scope** and enter the scope.

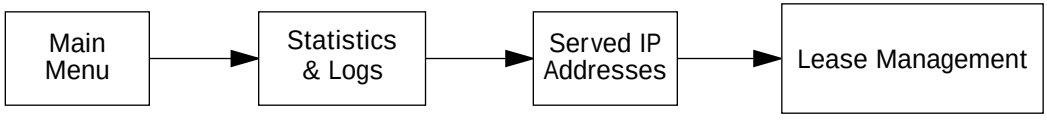
- To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

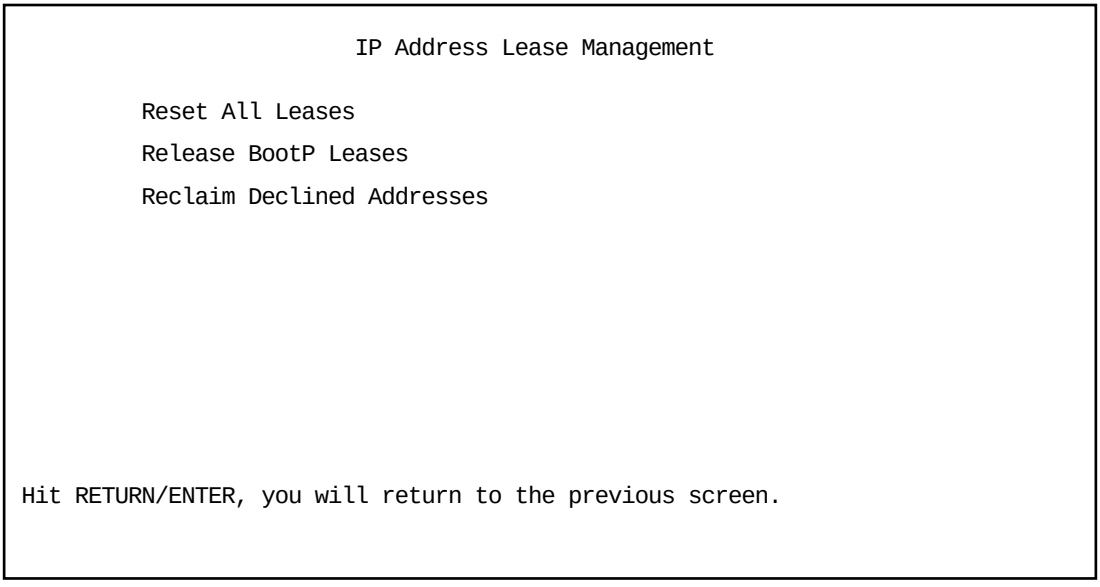
  Select **NetBios Name Server IP Addr** and enter the IP address for the NetBIOS name server.

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

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

  Note: Addresses assigned through BootP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and **Lease Management**.





Select **Release BootP Leases** and press Return.

MacIP (KIP forwarding) setup

When hosts using AppleTalk (typically those using LocalTalk) are not directly connected to an IP network (usually an Ethernet), they must use a MacIP (AppleTalk–IP) gateway.

The optional Netopia AppleTalk feature enhancement kit provides for this service. A MacIP gateway converts network traffic into the correct format for AppleTalk or IP, depending on the traffic's destination. The MacIP gateway can also distribute IP addresses to AppleTalk computers on the network.

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

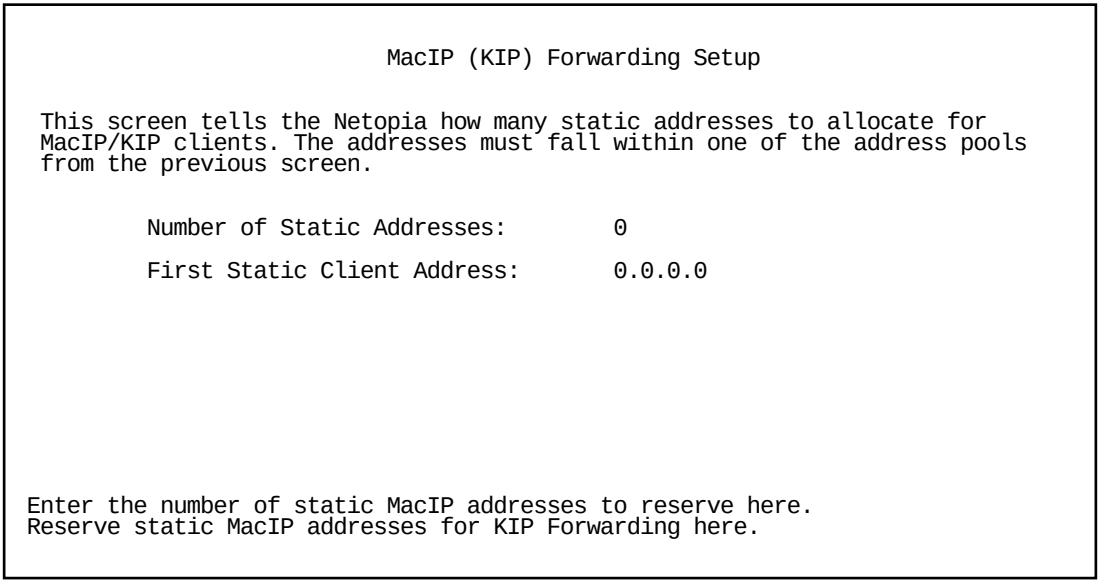
Setting up MacIP involves choosing MacIP dynamic address serving and then configuring that type. KIP forwarding is simply a method for distributing IP addresses to AppleTalk clients.

- In the IP Address Serving screen, select **Serve Mac IP/KIP Clients** and toggle to **Yes** to enable MacIP/KIP address serving capability. This option is automatically enabled if the AppleTalk kit is installed and IP Address Serving is enabled.
- Select **MacIP/KIP Static Options** and press Return. The MacIP/KIP Forwarding screen appears.

The MacIP (KIP) Forwarding Setup screen tells the Netopia R9100 how many static addresses to allocate for MacIP/KIP clients. The addresses must fall within the address pool from the previous screen.

- Enter the number of static MacIP addresses to reserve.

  Note that the address pool IP range is listed for your referral in this screen.



You have finished your IP setup.

Chapter 10

IPX Setup

Internetwork Packet Exchange (IPX) is the network protocol used by Novell NetWare networks. This chapter shows you how to configure the Netopia R9100 for routing data using IPX. You also learn how to configure the router to serve IPX network addresses.

Note: Most cable modems do not currently support the IPX protocol over the WAN. The Netopia R9100 supports IPX routing over the Auxiliary port with an attached asynchronous modem. This requires the optional add-on dial-in kit (order TER/AD1).

This section covers the following topics:

IPX features

The Netopia R9100 supports the following IPX features:

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

IPX definitions

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

Internetwork Packet Exchange (IPX)

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

IPX address

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

Socket

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

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

Routing Information Protocol (RIP)

RIP, which was also derived from XNS, is a protocol that allows for the bidirectional transfer of routing tables and provides timing information (ticks), so that the fastest route to a destination can be determined. IPX routers use RIP to create and dynamically maintain databases of internetwork routing information. See "IPX routing tables" on page 10-5 for more information.

Service Advertising Protocol (SAP)

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

The following is a list of common SAP server types:

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

NetBIOS

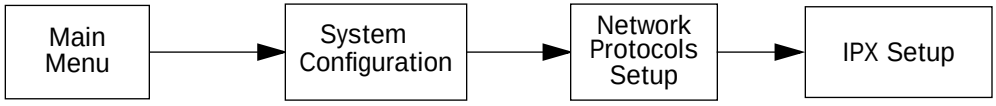
NetBIOS is a protocol that performs tasks related to the Transport and Session layers of the OSI model. It can operate over IPX using a special broadcast packet known as “IPX Packet type 20” to communicate with IPX NetBIOS servers.

IPX spoofing

The Netopia R9100 has several IPX features designed to restrict the traffic on the dial-up link when the unit is not sending or receiving IPX data. When the link is idle and a user is logged into a Novell server, the server will send “keep-alive” packets to ensure that the user is still there. If the link is idle, the keep-alive packets will be sent back to the server by the locally connected Netopia R9100 as though they came back from the user without bringing up the dial-up link.

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

IPX setup screen



You will use the IPX Setup screen to configure the Ethernet side of the Netopia R9100. The information you enter controls how the router routes IPX traffic.

Before changing any of the settings in this screen, consult your network administrator for the IPX setup information you will need. Changes made in this screen will take effect only after the Netopia R9100 is reset.

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

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

```
                                IPX Setup

        IPX Routing:                                On

        Ethernet Encapsulation...                   802.3
        Ethernet Network Address:                   00000000

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


        Default Gateway Address:                    00000000

        Filters and Filter Sets...

        IPX Wan Pool Base Address                   00000000



Return/Enter accepts * Tab toggles * ESC cancels.
Set up the basic IPX attributes of your Netopia in this screen.
```

1. To enable IPX routing, select **IPX Routing**, toggle it to **On**, and press Return.
2. To change Ethernet encapsulation from the commonly used 802.3 standard, select **Ethernet Encapsulation** and choose a different encapsulation method.
3. Select **Ethernet Network Address** and enter the network address of the IPX network connected to the Netopia R9100's Ethernet port.

   Note: If the Ethernet network address is set to zero, the router will attempt to learn the address from any configured IPX device on the Ethernet network or from the remote IPX network when a call is established.
4. To change the default path delay, select **Ethernet Path Delay** and enter a value (in ticks). This value is used to determine the port cost of using the Ethernet port in IPX RIP calculations.
5. To enable NetBIOS packet forwarding, select **Ethernet NetBios Forwarding** and toggle it to **Yes**. This parameter will determine whether IPX Packet type 20 packets are forwarded on the Ethernet interface. These packets are used by NetBIOS and some other applications.
6. Select **Ethernet Inbound SAP Filter Set** to filter incoming IPX SAP advertisements on the Ethernet. By attaching an incoming SAP filter on the Ethernet, you can restrict the number of SAP entries learned on a large IPX network to only those required by remote users connecting to the Netopia R9100. An Ethernet SAP filter *must* be used with networks that have so many servers advertised that the Netopia R9100 would otherwise exhaust its internal memory storing server entries.

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

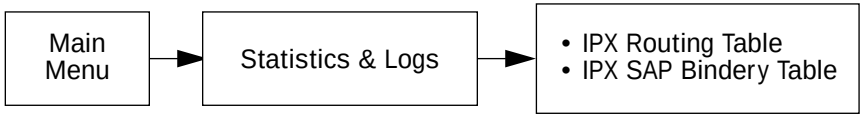
7. Select **Default Gateway Address** and enter the network address of the IPX network to which all packets of unknown destination address should be routed.

   Note: The default gateway address is usually set up to match the IPX Address in your network connection profile.

8. To configure filters and filter sets, select **Filters and Filter Sets** and go to the IPX filters and filter sets screens. For information on how to configure IPX filters and filter sets, see "IPX filters" on page 13-21.

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

IPX routing tables



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

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

```
                                  IPX Routing Table

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









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

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

Chapter 11

AppleTalk Setup

This chapter discusses the concept of AppleTalk routing and how to configure AppleTalk setup for a Netopia R9100 with the AppleTalk kit installed.

AppleTalk support is available as a separate kit for the Netopia R9100 Ethernet Router. Skip this chapter if you do not have the AppleTalk kit.

This section covers the following topics:

Note: To take effect, all changes to AppleTalk options require a restart.

AppleTalk networks

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

AppleTalk protocol

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

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

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

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

However, networks can be connected together through **routers**, such as the Netopia R9100 Ethernet Router, into an **internetwork** (often shortened to **internet**). Because devices on different networks can have duplicate node numbers, AppleTalk tells them apart according to an additional part of their addresses: the **network number**.

The Netopia R9100 assigns a unique network number to each member network. In terms of the city street metaphor, the network number is similar to the name of the street. Putting a network number together with a node number fully specifies the address of a node on an internet.

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

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

You can use the information in the AppleTalk routing table to observe and diagnose the Netopia R9100's current connections to other AppleTalk routers. To go to the AT Routing Table screen from the Netopia R9100's console, select **Statistics & Logs** from the Main Menu and then select **AppleTalk Routing Table**. An AT Routing Table similar to the one shown below appears.

```
                          AT Routing Table

-Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
 ---------------------------------SCROLL UP--------------------------
  1     --     Admin                  2    Good  46.131          0
  2     --     AdMan                  2    Good  46.131          0
  3     --     Aspirations            2    Good  46.131          0
  4     --     Sales                  2    Good  46.131          0
  5     --     Marketing              2    Good  46.131          0
  6     --     Molluscs               2    Good  46.131          1
  7     --     Customer Service       2    Good  46.131          1
  8     --     Telemarketing          2    Good  46.131          0
  10    --     Rio                    2    Good  46.131          0
  11    --     Regiment               2    Good  46.131          0
  12    --     Rhinos                 2    Good  46.131          0
  16    --     Unique Services        2    Good  46.131          0
 *24    27     Aspirations            1    Good  46.131          79
  28    31     Rhinos                 1    Good  46.131          15
 ---------------------------------SCROLL DOWN------------------------
UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

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

MacIP

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

See "IP address serving" on page 9-16 for more information on how to set up MacIP and other IP addressing schemes.

AURP

AppleTalk Update-Based Routing Protocol (AURP) allows AppleTalk networks to communicate across an IP network. Your local AppleTalk networks (connected to the Netopia R9100) can exchange data with remote AppleTalk networks that are also connected to an AURP-capable router.

When two networks using AppleTalk communicate with each other through a network based on the Internet Protocol, they are said to be "tunneling" through the IP network. The Netopia R9100 uses AURP to allow your AppleTalk network to tunnel to designated AppleTalk partner networks, as well as to accept connections from remote AppleTalk networks tunneling to your AppleTalk LAN.

Routers and seeding

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

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

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

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

Soft seeding: When a router that uses soft seeding is turned on or reset, it requests network number and zone name information from any existing routers on the networks it will serve. If no other routers reply, the router uses the network numbers and zone names specified in its own configuration. If other routers reply, the router uses the information they provide, regardless of whether or not there are conflicts between the information received and its configured information. Once a soft- or hard-seeding router begins to route, it can serve as a seed router, providing network number and zone name information to other routers upon request. The default state of the Netopia R9100's AppleTalk ports is soft seeding.

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

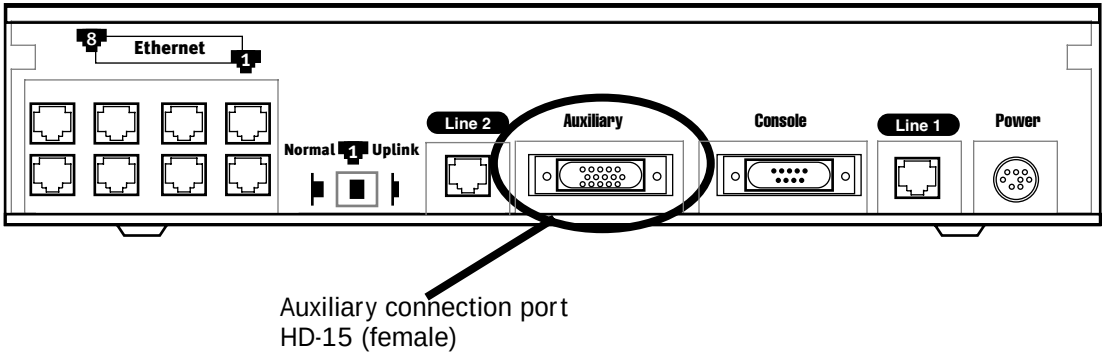
It is important to set the Netopia R9100's seeding action to work best in your particular network environment. These scenarios may guide you in deciding how to set the router's seeding:

- If the Netopia R9100 is the only router on your network, you must set it to either hard seeding or soft seeding. The default is soft seeding.
- If there is another active router on your network and you want that router to configure the Netopia R9100's EtherTalk or LocalTalk parameters, you can set the Netopia R9100 to non-seeding.
- If there is another active router on your network, you could set the Netopia R9100 to be soft seeding if you are unsure whether the second router will always be available to configure the Netopia R9100's EtherTalk or LocalTalk parameters.
- If you want the Netopia R9100 to configure the EtherTalk or LocalTalk parameters of other routers on your network, you must set it to hard seeding. In this case, the other routers must be soft seeding or non-seeding, and the Netopia R9100 must already be active when those other routers are rebooted.
- If you want the Netopia R9100 and all other routers on your network to use only their own configurations, set the Netopia R9100 and all other routers to hard seeding. In this case, any router (including the Netopia R9100) that is rebooted will not begin routing if it detects a routing conflict between itself and any other router. This last scenario could be useful for detecting and locating routing errors on your network.

Installing AppleTalk

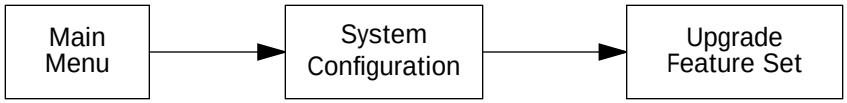
The AppleTalk kit consists of hardware and firmware components that you enable on your router in order to connect an AppleTalk network. The AppleTalk cable supplied in the AppleTalk feature expansion kit cable connects to the Auxiliary port on the Netopia R9100.

Netopia R9100 Ethernet Router back panel



You then enable AppleTalk routing through the console-based management screens.

To install the AppleTalk features from the Main Menu, go to System Configuration and select **Upgrade Feature Set**.



The **Netopia Feature Set Upgrade** screen appears.

```
                    Netopia Feature Set Upgrade

You may be able to extend the features of your Netopia by purchasing a
'Software Upgrade'.  For a list of available upgrades, please see the release
notes that came with your Netopia or visit the Netopia Communications web
site at www.netopia.com.

To purchase an upgrade, you must provide your Serial Number, which is:

        xx-xx-xx

You will receive an Upgrade Key, which you should enter below.

        Upgrade Key:



        UPGRADE NOW                         CANCEL
```

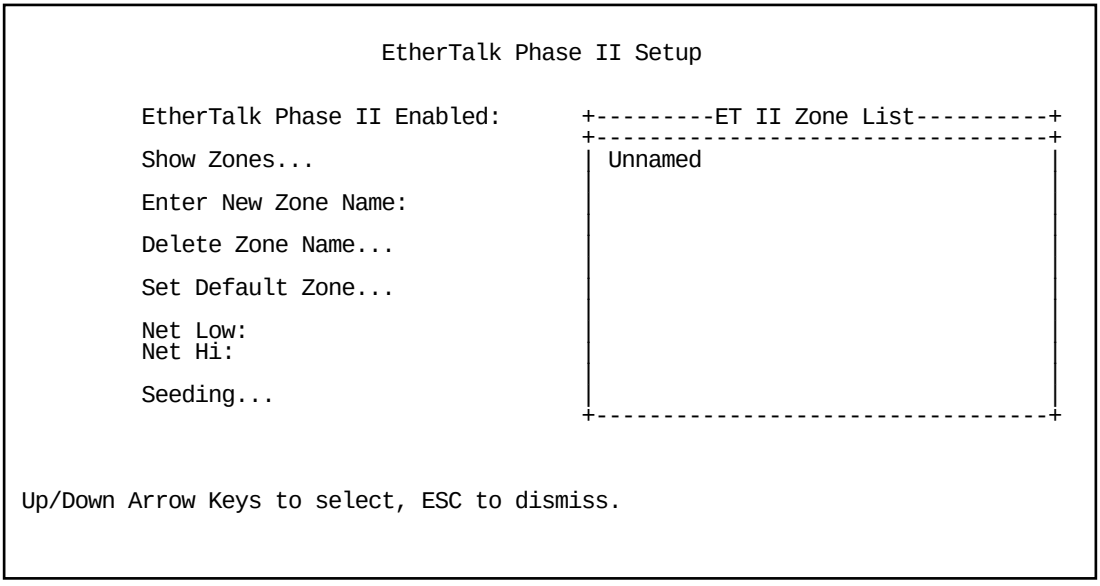
Follow the instructions to enable AppleTalk on your router. Once AppleTalk is enabled, you can configure your network as described in the following sections.

Configuring AppleTalk

AppleTalk setup for Netopia R9100s consists of configuring EtherTalk, LocalTalk, and AURP.

EtherTalk setup

In the System Configuration screen, select **Network Protocols Setup** and then select **AppleTalk Setup**. Select **EtherTalk Phase ll Setup** and press Return.



- If you are using EtherTalk Phase ll on the Ethernet network connected to the Netopia R9100, select **EtherTalk Phase ll Enabled** and toggle it to **On**.
- To view the zones available to EtherTalk Phase ll, select **Show Zones** and press Return. You can dismiss the list of zones by pressing Return or Escape.
- Select **Enter New Zone Name** to enter a new zone name.

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

  If another router is already present on the EtherTalk network that you will be connecting to the Netopia R9100, use the zone names and network numbers used by that router for that EtherTalk network. Otherwise, your EtherTalk network may experience routing conflicts. The Netopia R9100 supports creating up to 32 zone names.

  As an alternative, you can set EtherTalk seeding to soft seeding and let the Netopia R9100 receive the zone name and network number from the other router.
- To remove zones from the list, select **Delete Zone Name** and press Return to see the zones list. Use the Up and Down Arrow keys to select the zone to delete. Press Return to delete it and exit the list. Press Escape to exit the list without deleting any zones.
- Select **Set Default Zone** to choose a different default zone. This is the zone where the Netopia R9100's

EtherTalk Phase II port is visible to other AppleTalk nodes. The default zone is also where new AppleTalk nodes will appear. If you do not set a default zone, the first zone you create will be the default zone.

- You can also set the range of EtherTalk Phase II network numbers. Select **Net Low** and enter the lower limit of the network number range. Select **Net High** and enter the upper limit of the range.
- Select the **Seeding** pop-up menu and choose the seeding method for the Netopia R9100 to use. (See "Routers and seeding" on page 11-3).

You have finished configuring EtherTalk Phase II.

LocalTalk setup

Note: For instructions on making the physical connections for LocalTalk, see "Connecting to a LocalTalk network" on page 4-8.

In the AppleTalk Setup screen, select **LocalTalk Setup** and press Return. The LocalTalk Setup screen appears.

```
                              LocalTalk Setup

        LocalTalk Enabled:                On
        LocalTalk Zone Name:              Unnamed
        LocalTalk Net Number:             33126
        Seeding...                        Soft-Seeding









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

- If you are using LocalTalk with the Netopia R9100, select **LocalTalk Enabled** and make sure LocalTalk is set to **On,** which is the default.

Note: Since the LocalTalk connector attaches to the Auxiliary port on the router, that port will no longer be available for a third external modem.

- Select **LocalTalk Zone Name** and enter a new or existing zone name.

  Note: Your LocalTalk network may already have a zone and network number in place. For the Netopia R9100's LocalTalk port to be part of your LocalTalk network, it must have a network number and zone name that matches the values in use on the LocalTalk network.

  If another router is already present on the LocalTalk network that you will be connecting to the Netopia R9100, use the zone name and network number used by that router for that LocalTalk network. Otherwise, your LocalTalk network may experience routing conflicts.

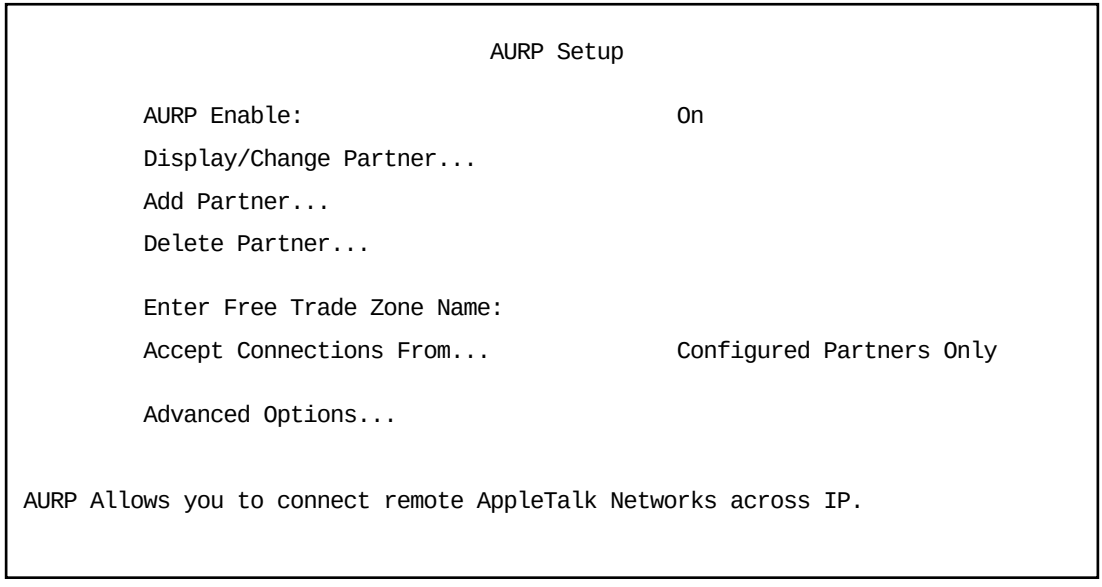
As an alternative, you can set LocalTalk seeding to soft seeding and let the Netopia R9100 receive the zone name and network number from the other router.

- Select **LocalTalk Net Number** and enter the desired network number.
- Select **Seeding.** From the pop-up menu, choose the type of seeding for the Netopia R9100's LocalTalk port to use (see "Routers and seeding" on page 11-3).

You have finished configuring LocalTalk.

AURP setup

From the Network Protocols screen, select AppleTalk Setup. Then select **AURP Setup** and press Return. The AURP Setup screen appears.



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

Viewing AURP partners

- To see a table of existing AURP partners, select **Display / Change Partner** and press Return.

  Note: The Netopia R9100 can define a total of 32 AURP partners.

AURP Free Trade Zone

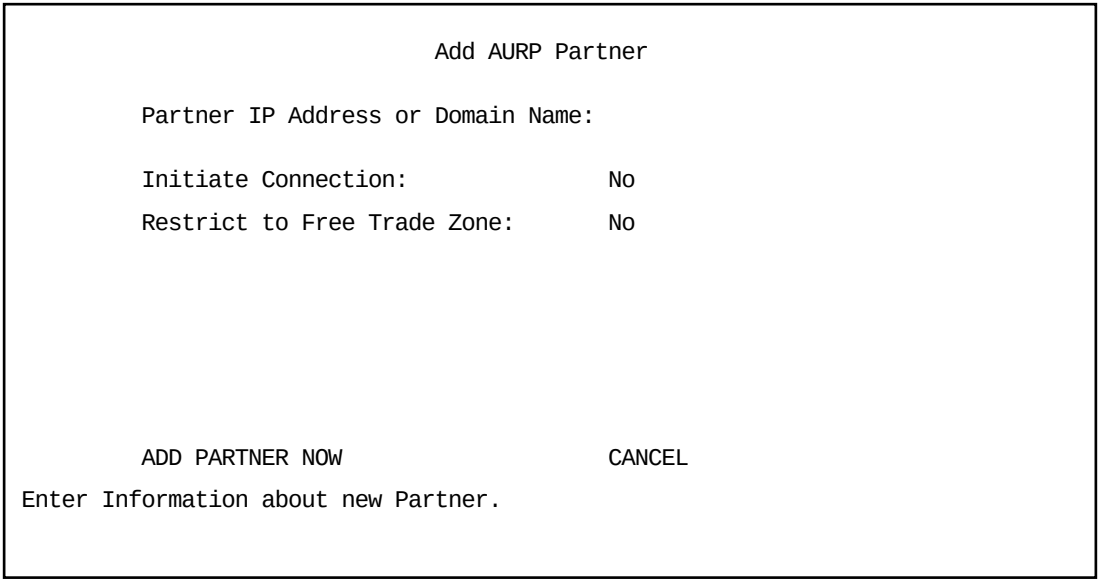
The Free Trade Zone is an AURP security feature. It allows the Netopia administrator to specify a single AppleTalk zone that will be the only one visible to the remote side for partners that have this option enabled.

Example:

Site A has an AURP tunnel to site B. Both sides have multiple zones defined on the EtherTalk port and a unique zone on their LocalTalk ports. If side A has indicated that one of its EtherTalk zones is the Free Trade Zone and has opted to use the Free Trade Zone option for its tunnel to B, then only this Free Trade Zone will show up on side B and only those machines or services in the Free Trade Zone will be accessible to side B. All of side A will be able to see all of side B.

Adding an AURP partner

- To add a new AURP partner, select **Add Partner** and press Return. The Add AURP Partner screen appears.

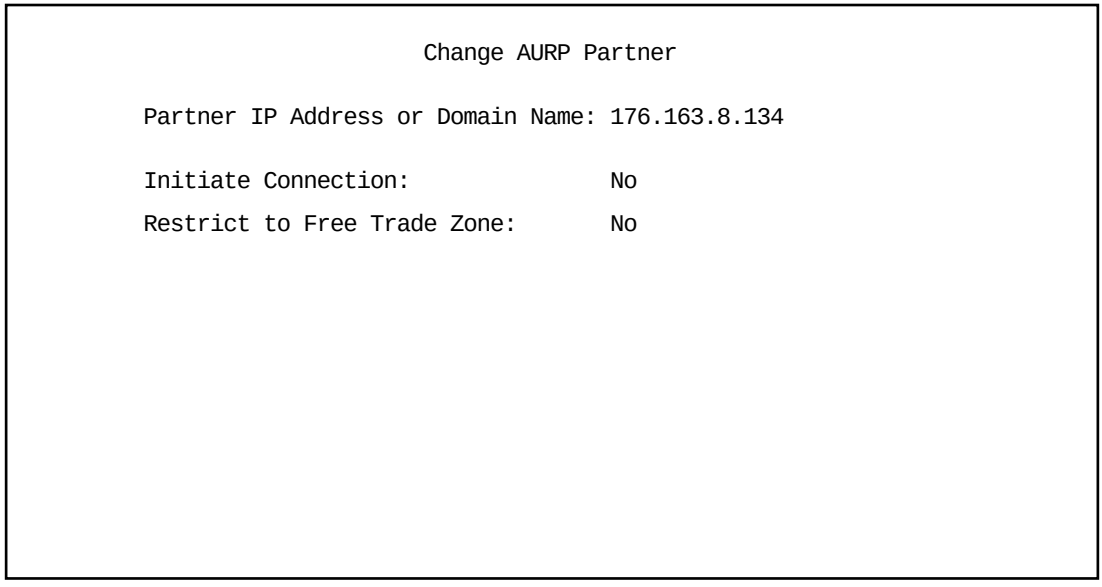


- Select **Partner IP Address or Domain Name** and enter the new AURP partner's IP address. If you do not know the remote network's IP address, enter its domain name. Domain names are the Internet addresses favored by people (for example, chagall.arts.edu). Domain names are matched to the IP addresses actually used by IP routers (for example, 163.7.8.202).
- To initiate a connection with an AURP partner, select **Initiate Connection** and toggle it to **Yes**. This will open a connection to the remote AppleTalk network after rebooting.
- You can choose to restrict this partner to the Free Trade Zone by toggling **Restrict to Free Trade Zone** to **Yes**. See "AURP Free Trade Zone" on page 11-8 for more information.
- To add the new AURP partner, select **ADD PARTNER NOW**. To discard the new AURP partner, select **CANCEL**.

Modifying an AURP partner

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

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



The Change AURP Partner screen has all the values you entered when you added that partner. All of these values may be modified in this screen.

Deleting an AURP partner

- To delete an AURP partner, in the AURP Setup screen select **Delete Partner** and press Return. A table of existing partners appears.

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

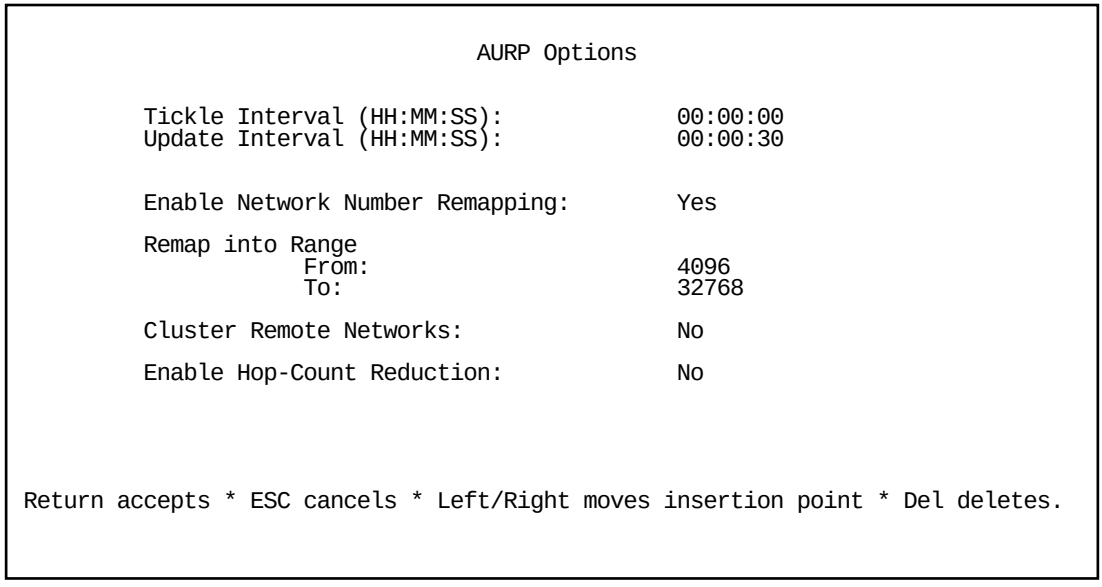
Receiving AURP connections

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

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

Configuring AURP Options

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



- Select **Tickle Interval (HH:MM:SS)** and set the timer to indicate how often a tickle or "Are you still there" packet will be sent to the remote AppleTalk network.

  The AURP tickle timer is a parameter that you can set anywhere between 0 and 100 hours. This parameter tells the AURP partners when to send out an AURP tickle packet. If this value is set to 0, the Netopia R9100 will never send out a tickle packet. Tickle packets verify that the remote router is working. The minimum tickle interval is 90 seconds. The maximum tickle interval setting is 99:59:59 (100 hours), which is the recommendation for small networks.

  Raising the tickle packet interval does not ensure that the AURP tunnel is dropped or not brought up. If any application on the local network generates AppleTalk traffic destined for the network at the remote end of the AURP tunnel, the tunnel remains up. For example, if a host on the local network connects to a host on the remote network using remote access software, the AURP tunnel remains up. The AURP tunnel also remains up if a local user selects the Chooser and uses an AppleTalk service that involves a remote zone, such as mounting a remote AppleShare volume.

- In many AppleTalk internets, individual AppleTalk networks come and go. Routers are designed to notify each other at the end of their Update Interval every time there's such a change in the network topology. This will cause the Netopia's WAN link to be brought up. To minimize what may be unnecessary calls, change the **Update Interval** value to some larger value. At the end of this time window, if there has been a local AppleTalk network change, the Netopia R9100 will call any remote AURP partner and forward the new network information.

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

  You should enable network number remapping if you plan to use AURP when connecting to unknown AppleTalk networks; for example, when "Accept Connections from Anyone" is enabled. With remapping, the Netopia R9100 will substitute network numbers not used by your network for the numbers of other remote networks. These safe remappings will only be used by local routers on your network; remote routers will not be aware of the remapping.

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

- To choose a destination range for the remapping, select **From** under **Remap into Range** and enter a starting value. Then select **To** and enter an ending value. Make sure the range you choose is large enough to accommodate all expected incoming AURP network numbers.
- To improve the efficiency of remapping network numbers into a safe range, select **Cluster Remote Networks** and toggle it to **Yes**. This setting takes any number of remote networks being remapped and causes them to be remapped into a continuous range.
- To override the AppleTalk maximum limit of 15 hops, select **Enable Hop-Count Reduction** and toggle it to **Yes**. Hosts on a local AppleTalk network will then "see" AppleTalk destinations across the IP tunnel as being only one hop away.

  AppleTalk allows a packet up to 15 hops (going through 15 AppleTalk routers) to reach its destination. Packets that must reach destinations more than 15 hops away will not succeed; therefore, tunneling from one large AppleTalk network to another could exceed that limit. In such a case, hop count reduction enables full network to network communication.

You have finished configuring AURP.

Chapter 12

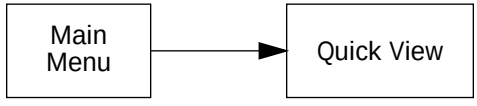
Monitoring Tools

This chapter discusses the Netopia R9100'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

You can get a useful, overall status report from the Netopia R9100 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.

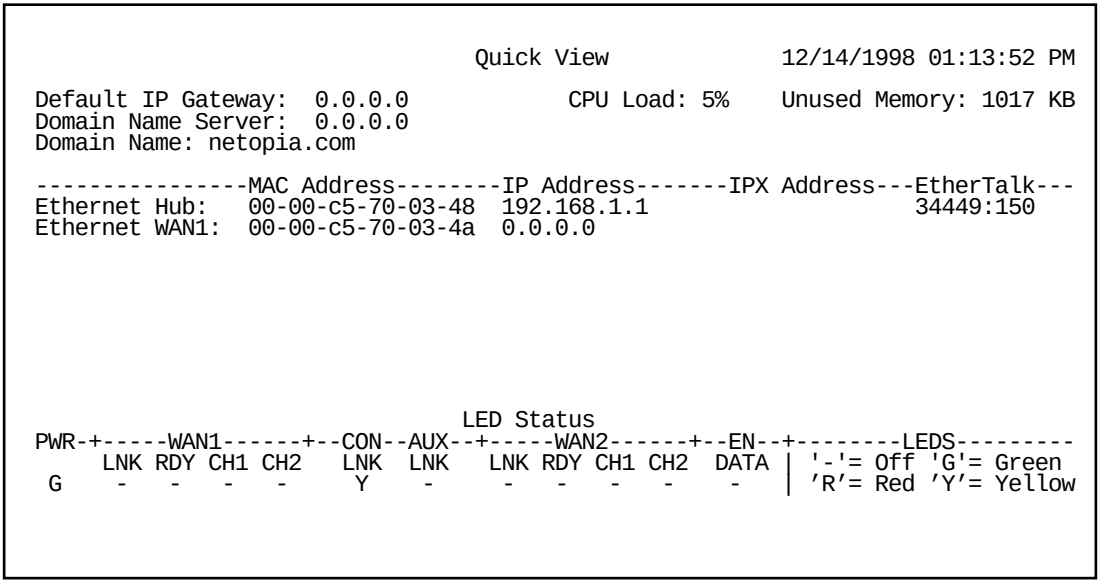


The Quick View screen has three status sections:

- General status
- Current WAN Connection Status
- LED Status

The status sections vary according to the interface of your Netopia R9100.

General status



Current Date: The current date; this can be set with the Date and Time utility (see "Date and time" on page 8-12).

Default IP Gateway: Actual IP address of the default gateway, if entered. 0.0.0.0 indicates automatic addressing.

Domain Name Server: IP address of your DNS server.

Domain Name: Domain name you have entered, usually your ISP, such as netopia.com.

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

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

Ethernet Address: The Netopia R9100's hardware address.

IP Address: The Netopia R9100's IP address, entered in the IP Setup screen.

IPX Address: The Netopia R9100's IPX address, entered in the IPX Setup screen.

EtherTalk Address: The Netopia R9100's AppleTalk address on its EtherTalk Phase II interface, entered in the EtherTalk Phase II Setup screen (only if the optional AppleTalk feature set is installed).

LocalTalk Address: The Netopia R9100's AppleTalk address on its LocalTalk interface, entered in the LocalTalk Setup screen (only if the optional AppleTalk feature set is installed).

Status lights

This section shows the current real-time status of the Netopia R9100's status lights (LEDs). It is useful for remotely monitoring the router's status. The Quick View screen's arrangement of LEDs corresponds to the physical arrangement of LEDs on the router.

```
-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 “Netopia R9100 Ethernet Router status lights” on page 3-4 describes the meanings of the colors for each LED.

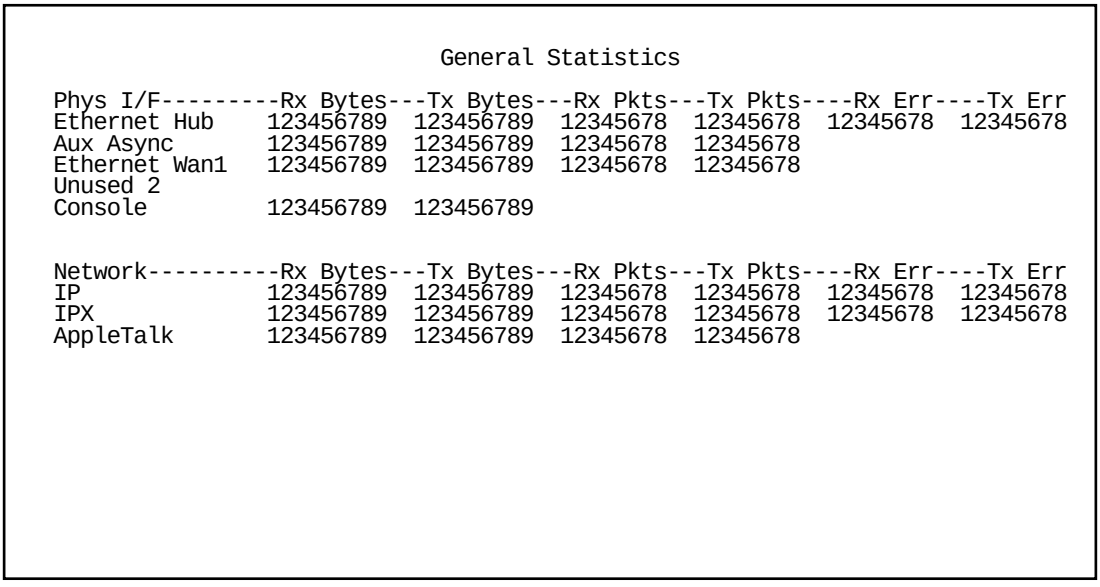
Statistics & Logs

When you are troubleshooting your Netopia R9100, the Statistics & Logs screens provide insight into the recent event activities of the router.

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.



The General Statistics screen displays information about data traffic on the Netopia R9100'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 Async or LocalTalk (if the optional AppleTalk feature set is installed)
- 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)
- IPX (IPX packets on the Ethernet) if IPX is enabled
- AppleTalk (AppleTalk packets on Ethernet using EtherTalk Phase II if the optional AppleTalk feature set is installed)

- LT (LocalTalk on the PhoneNET) if the optional AppleTalk feature set is installed

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

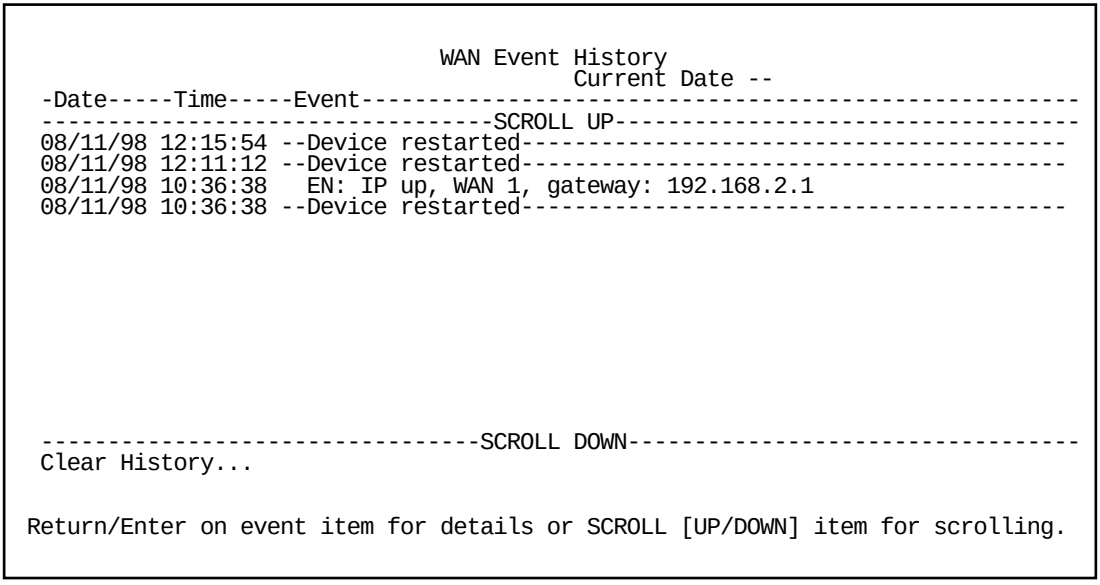
The Netopia R9100 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R9100's built-in battery backup prevents loss of event history from a shutdown or reset.

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

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

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.



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 --  12/11/98 12:26:39 PM
 -Date-----Time-----Event-----------------------------------------------
 ---------------------------------SCROLL UP-------------------------------
 08/11/98 12:25:28   Telnet connection up, address 163.176.8.134
 08/11/98 12:25:05 * IP address server configuration error; server disabled
 08/11/98 12:25:05 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:25:05 --BOOT: Warm start v4.3 ------------------------------
 08/11/98 12:19:17 * IP address server configuration error; server disabled
 08/11/98 12:19:17 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:19:17 --BOOT: Warm start v4.3 ------------------------------
 08/11/98 12:18:15 * IP address server configuration error; server disabled
 08/11/98 12:18:15 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:18:15 --BOOT: Warm start v4.3 ------------------------------
 08/11/98 12:16:34   Telnet connection up, address 163.176.8.134
 08/11/98 12:15:54   IP address server initialization complete
 08/11/98 12:15:54 * IP: Route 0.0.0.0/0.0.0.0 not installed
 08/11/98 12:15:54 --BOOT: Warm start v4.3 ------------------------------
 -------------------------------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.

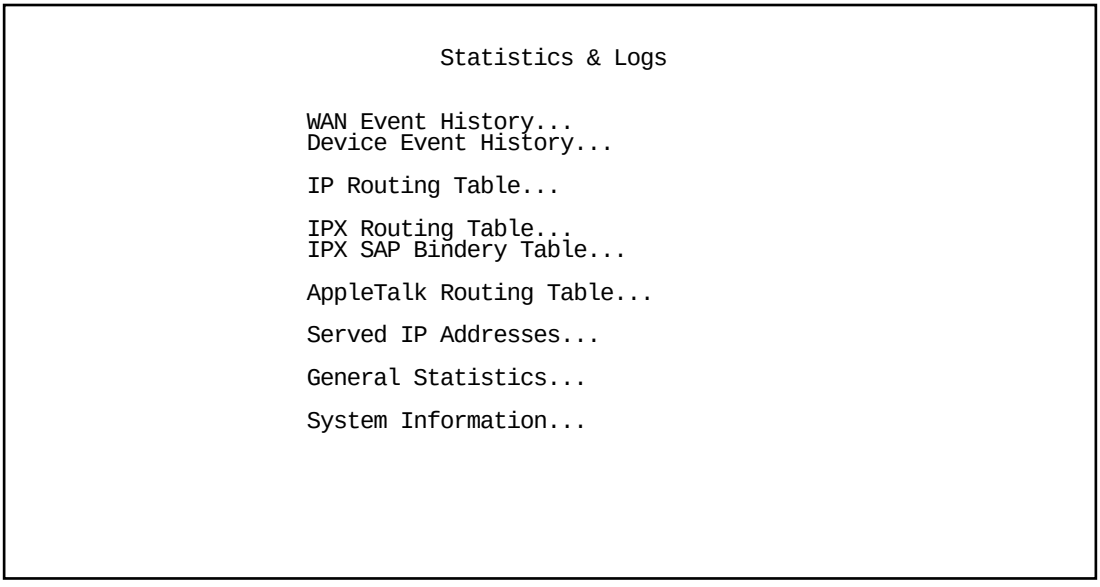
To clear the Device Event History, select **Clear History** and press Return.

Routing tables

You can view all of the IP, IPX, and AppleTalk routes in the Netopia R9100's IP, IPX, and AppleTalk routing tables, respectively.

To go to a routing table screen, select the routing table you are interested in from the **Statistics & Logs** screen.

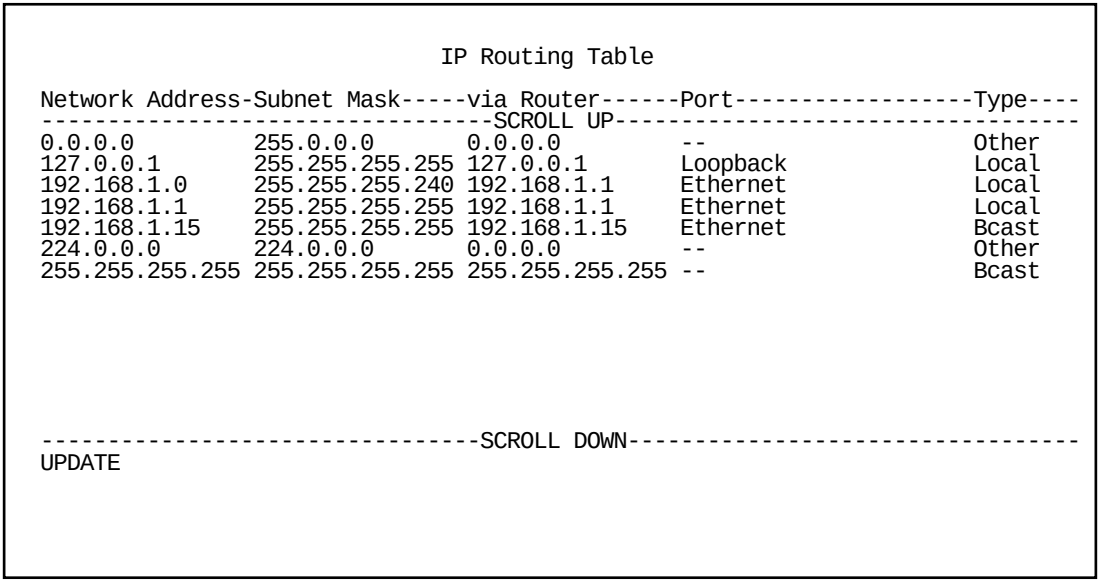
Each of the routing table screens represents a "snapshot" of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.



IP routing table

In the Statistics & Logs screen, select **IP Routing Table** and press Return.

The IP routing table displays all of the IP routes currently known to the Netopia R9100.



IPX routing table

In the Statistics & Logs screen, select **IPX Routing Table** and press Return.

The IPX routing table displays all of the IPX routes currently known to the Netopia R9100.

IPX Sap Bindery table

In the Statistics & Logs screen, select **IPX Sap Bindery Table** and press Return.

The IPX Sap Bindery table displays all of the IPX Sap Bindery routes currently known to the Netopia R9100.

AppleTalk routing table

In the Statistics & Logs screen, select **AppleTalk Routing Table** and press Return. An AT Routing Table similar to the one shown below will appear.

The AppleTalk routing table displays information about the current state of AppleTalk networks connected to the Netopia R9100, including remote AppleTalk networks connected with AURP. This information is gathered from other active AppleTalk routers.

```
                              AT Routing Table

-Net---Range--Def Zone Name----------Hops-State-Next Rtr Addr.--Pkts Fwded
 ---------------------------------SCROLL UP-------------------------
  1     --     Admin                    2    Good  46.131          0
  2     --     AdMan                    2    Good  46.131          0
  3     --     Aspirations              2    Good  46.131          0
  4     --     Sales                    2    Good  46.131          0
  5     --     Marketing                2    Good  46.131          0
  6     --     Molluscs                 2    Good  46.131          1
  7     --     Customer Service         2    Good  46.131          1
  8     --     Telemarketing            2    Good  46.131          0
  10    --     Rio                      2    Good  46.131          0
  11    --     Regiment                 2    Good  46.131          0
  12    --     Rhinos                   2    Good  46.131          0
  16    --     Unique Services          2    Good  46.131          0
 *24    27     Aspirations              1    Good  46.131          79
  28    31     Rhinos                   1    Good  46.131          15
 ---------------------------------SCROLL DOWN-----------------------
UPDATE

'*' Entries have multiple zone names. Return/Enter on these to see zone list.
```

Each row in the AppleTalk routing table corresponds to an AppleTalk route or network range. If the list of routes shown exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

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

The table has the following columns:

Net: Displays the starting network number supplied by the AppleTalk router in the “Next Rtr Addr.” column. If a network number is preceded by an asterisk (*), it has multiple zones. To display the zones, select the network entry and press Return.

Range: Displays the ending network number for the extended network.

Def Zone Name: Displays the zone or zones associated with the specified network or network range. The zone name shown is either the only zone or the default zone name for an extended network. To see the complete list of zones for an extended network with multiple zones, select the entry in the table and press Return. Press Return again to close the list of zones.

Hops: Displays the number of routers between the Netopia R9100 and the specified network.

State: Displays the state of the specified route, based on the frequency of Routing Table Maintenance Protocol (RTMP) packets received for the route. The state can be Good, Suspect, or Bad. AppleTalk routers regularly exchange RTMP packets to update AppleTalk routing information.

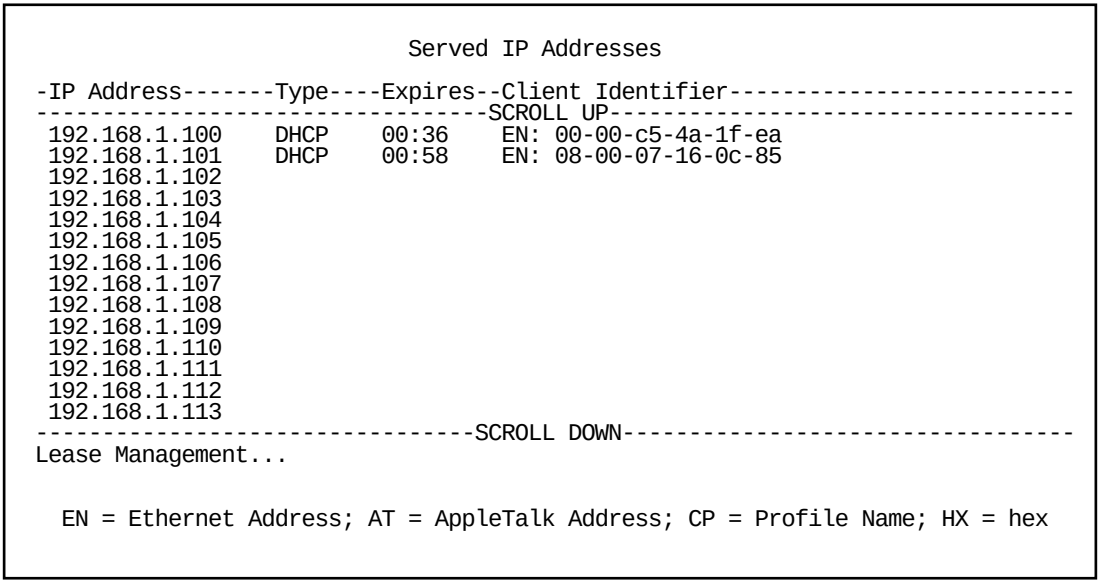
Next Rtr Addr.: Displays the DDP or IP address of the next hop for the specified route. A DDP address is displayed if the router shown is on the local AppleTalk network. DDP address means that a connection to the next-hop router is by a native AppleTalk network (e.g.: LocalTalk or EtherTalk Phase II). An IP address is displayed if the Netopia R9100 is connected to the router shown using AURP. IP address means a connection transports over AURP (AppleTalk encapsulated IP).

Pkts Fwded: The number of packets sent to the router shown.

Served IP Addresses

You can view all of the IP addresses currently being served by the Netopia R9100 Ethernet Router from the **Served IP Addresses** screen.

From the Statistics & Logs menu, select **Served IP Addresses**. The Served IP Addresses screen appears.



To manage DHCP leases, select **Lease Management** in this screen.

The IP Address Lease Management screen appears.

```
                        IP Address Lease Management

         Reset All Leases
         Release BootP Leases
         Reclaim Declined Addresses









Hit RETURN/ENTER, you will return to the previous screen.
```

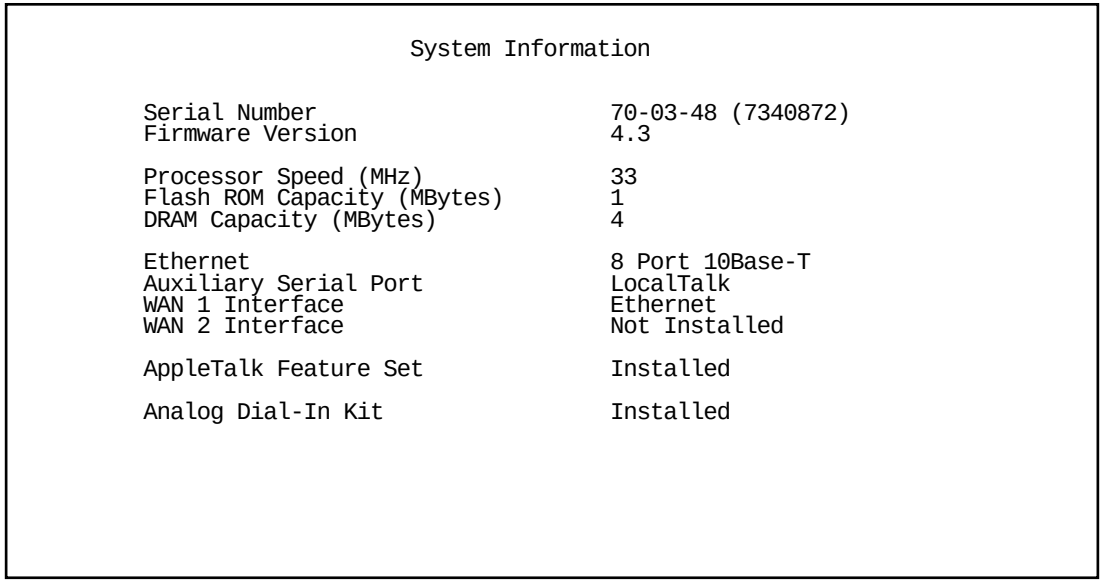
This screen has three options:

- **Reset All Leases**: Resets all current IP addresses leased through DHCP without waiting for the default one–hour lease period to elapse
- **Release BootP Leases**: Releases any BootP leases that may be in place, and which may no longer be required.
- **Reclaim Declined Addresses**: Reclaims served leases that have been declined; for example by devices that may no longer be on the network.

System Information

The System Information screen gives a summary view of the general system level values in the Netopia R9100 Ethernet Router.

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



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 R9100 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager.

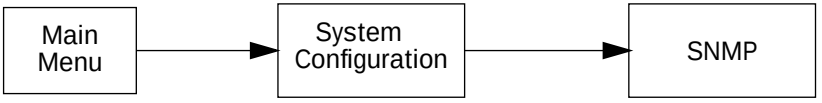
The Netopia R9100 supports the following management information base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- AppleTalk MIB I (RFC 1243)
- Netopia MIB

These MIBs are on the Netopia R9100 CD included with the Netopia R9100. 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.




```
                                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 R9100's SNMP agent.
2. Select **System Location** and enter the router's physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the router.

System Name, System Location, and System Contact set the values returned by the Netopia R9100 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 R9100. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the router, but cannot modify the router's configuration. An SNMP manager using the **Read / Write Community String** can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to "public" and "private," respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

Starting with the version 4.3 firmware, setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the router. (The router may still send SNMP Traps if those are properly enabled.)

Previously, if either community string was the empty string, SNMP Requests specifying an empty community string were accepted and processed.

This change is designed to allow the administrator to block SNMP access to the router, and to provide more granular control over the allowed SNMP operations to the router.

- Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the router, 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.

To change a community string, select it and enter a new value.

Caution! Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Netopia R9100 through SNMP. For more information on security issues, see "Suggested security measures" on page 13-1.

SNMP traps

An SNMP **trap** is an informational message sent from an SNMP agent (in this case, the Netopia R9100) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

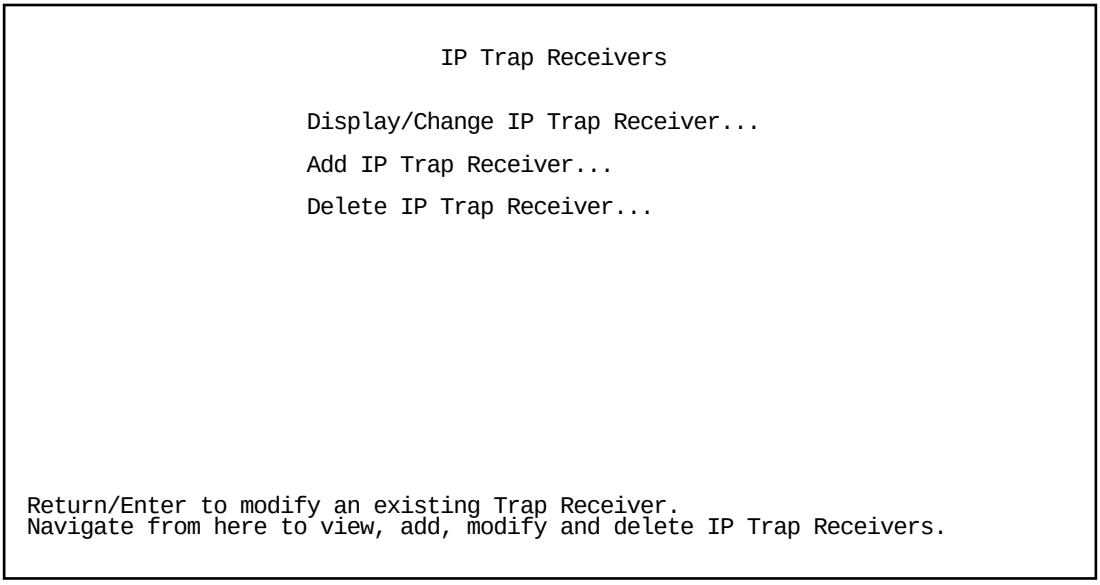
Standard traps generated by the Netopia R9100 include the following:

- An authentication failure trap is generated when the router 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 router is reset.
- An interface down trap (ifDown) is generated when one of the router's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the router's interfaces, such as a port, begins functioning.

The Netopia R9100 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia R9100. 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.



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**. Enter whatever community string is appropriate for the traps to be sent to the management station whose IP address or domain name you entered on the previous line.
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.

SmartView

This section discusses SmartView, the Netopia R9100's device and network web-based monitoring tool. This tool can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

SmartView overview

SmartView is a Java-based applet that runs in a Web browser window. It intermittently polls the router for information to monitor the router's state and event histories. SmartView should run under any Java Virtual Machine (JVM)–enabled browser, and is therefore platform independent.

Note: The SmartView applet will only run under Java-enabled browsers. Be sure that the browser you are using is at least Microsoft Internet Explorer Version 3.0 or higher, or Netscape Navigator Version 3.0 or Communicator Version 4.0 or higher. If your browser does not meet this requirement, you can upgrade with a browser supplied on the Netopia CD.

The information you can view about your router using SmartView is shown in the table below:

Machine Information	History Logs
Model	Device
Firmware version	WAN
Ethernet IP address	Update
Date	
Time	
LED status	

Navigating SmartView

You access the SmartView monitor by launching your web browser and entering the URL:

http://*router_IP_Address*/smartview.html

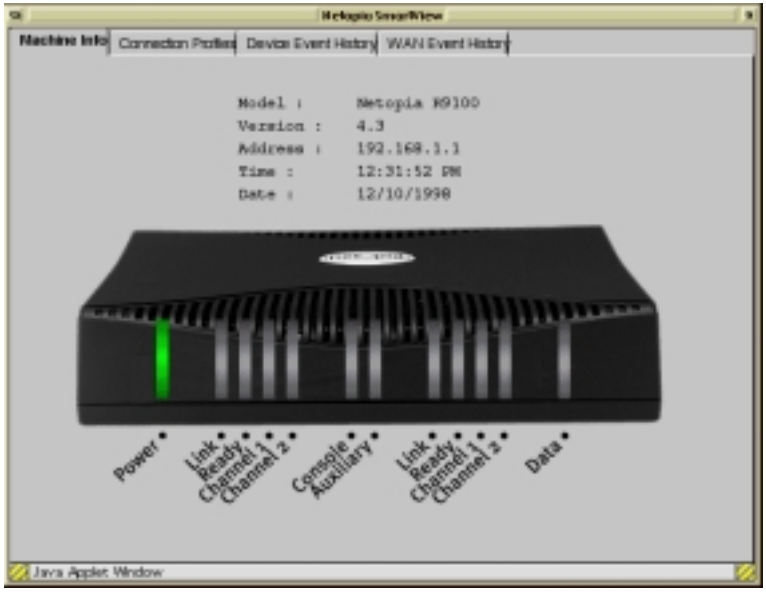
where *router_IP_address* is the address of your router.

Once you have invoked the SmartView pages, bookmark SmartView in your browser for easy access.

General Machine information page

SmartView uses tabbed pages to categorize information and reduce the amount of information displayed at once. Click on the tabs to display the different informational categories.

In addition to the static machine information about your router, such as model and firmware version, SmartView displays a real-time visual representation of the Netopia R9100's status lights (LEDs). This is particularly useful if the router is located out of visual range, such as in a wiring closet.

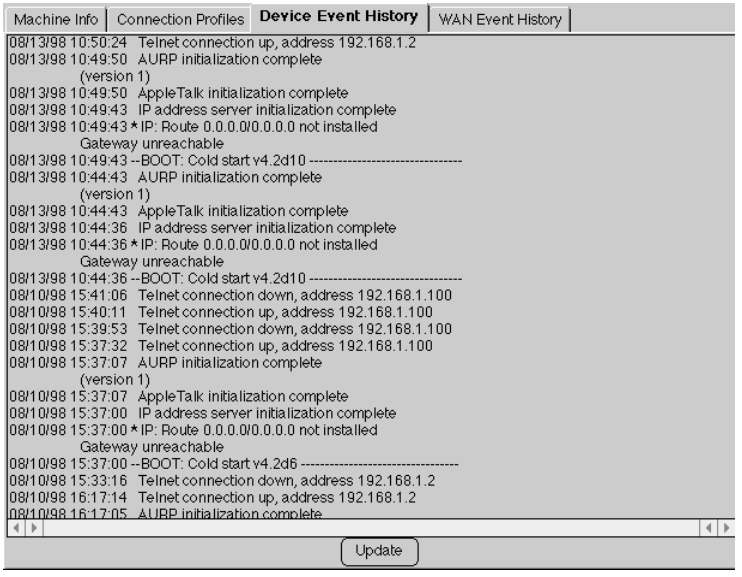


Event history pages

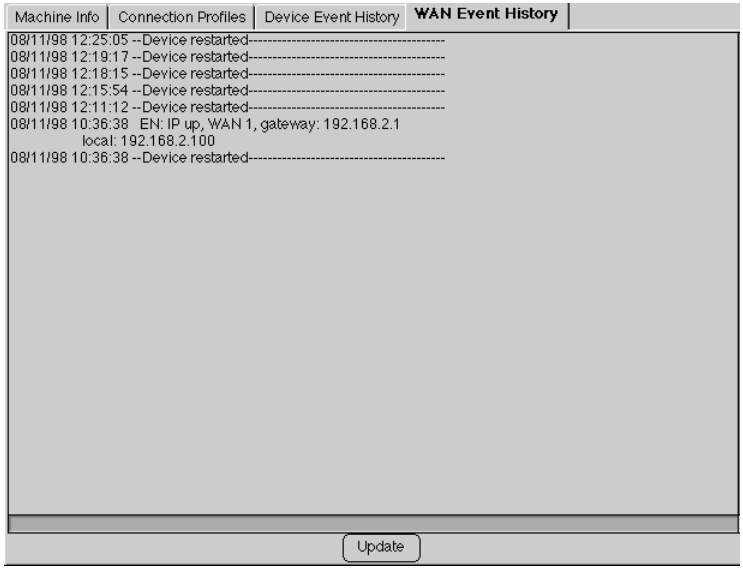
The Netopia R9100 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the router's system and one for the WAN. The Netopia R9100's built-in battery backup prevents loss of event history from a shutdown or reset.

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

Device Event History page



WAN Event History page



You can refresh the Event history logs by clicking the Update button.

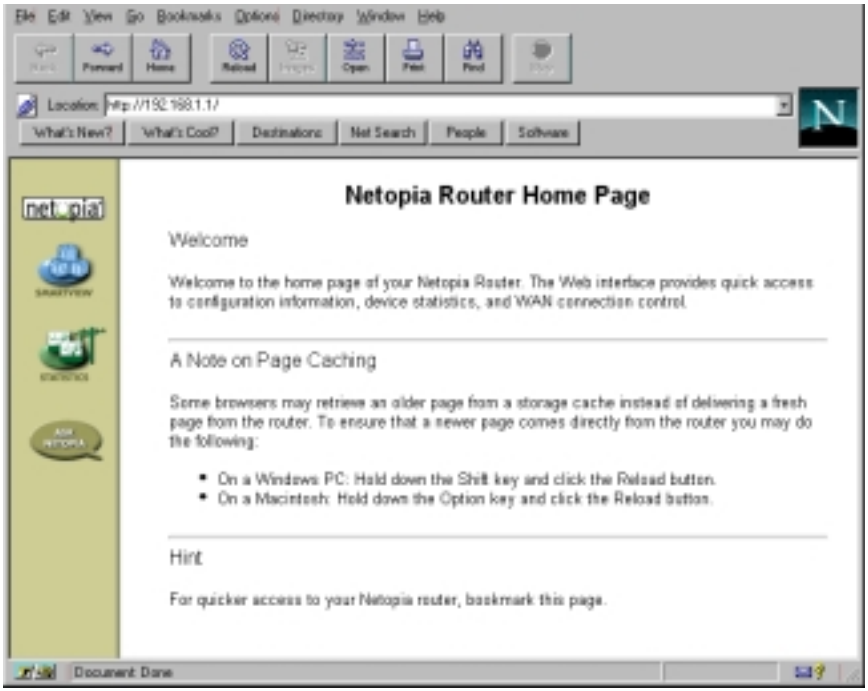
Standard HTML web-based monitoring pages

You can also view connection profile information and event histories in the Web-based monitoring pages. These pages are provided for users without Java-enabled browsers. Unlike the SmartView pages, they are not dynamically updated.

You access the Web-based monitoring pages by launching your Web browser and entering the URL:

http://*router_IP_address*

where *router_IP_address* is the address of your router.



- To view event histories, click the **Statistics** icon.
- To go to SmartView if your browser is Java-enabled, click the **SmartView** icon.

Chapter 13

Security

The Netopia R9100 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 R9100 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.
- Set the answer profile so it must match incoming calls to a connection profile.
- Set the Enable Dial-in Console Access option to No.
- When using AURP, accept connections only from configured partners.
- Configure the Netopia R9100 through the serial console port to ensure that your communications cannot be intercepted.

User accounts

When you first set up and configure the Netopia R9100, no passwords are required to access the configuration screens. Anyone could tamper with the router's configuration by simply connecting it to a console.

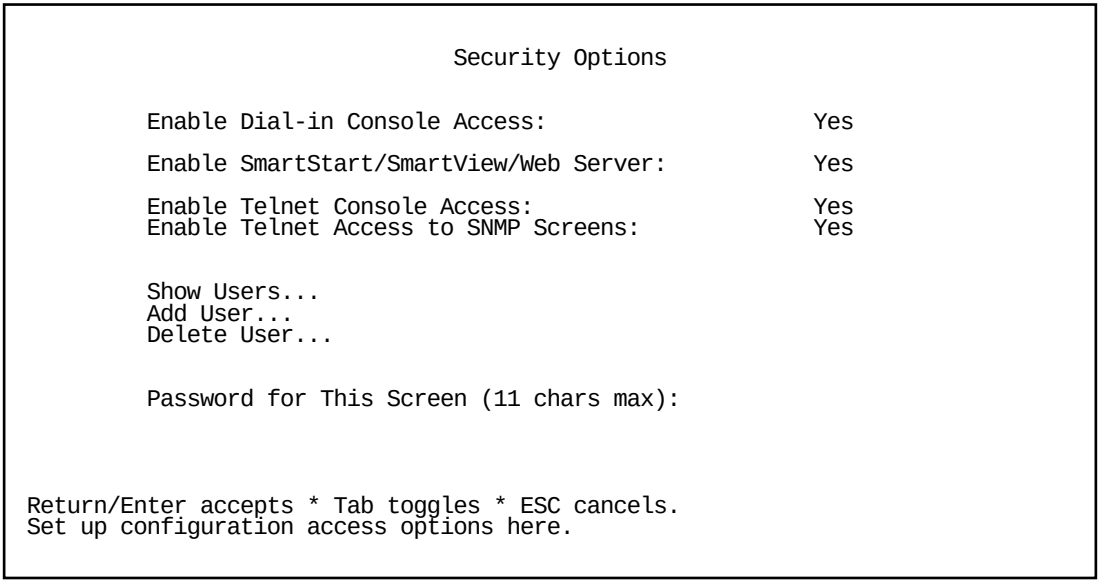
However, by adding user accounts, you can protect the most sensitive screens from unauthorized access. User accounts are composed of name/password combinations that can be given to authorized users.

Caution!

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

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. The Security Options screen appears.



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.

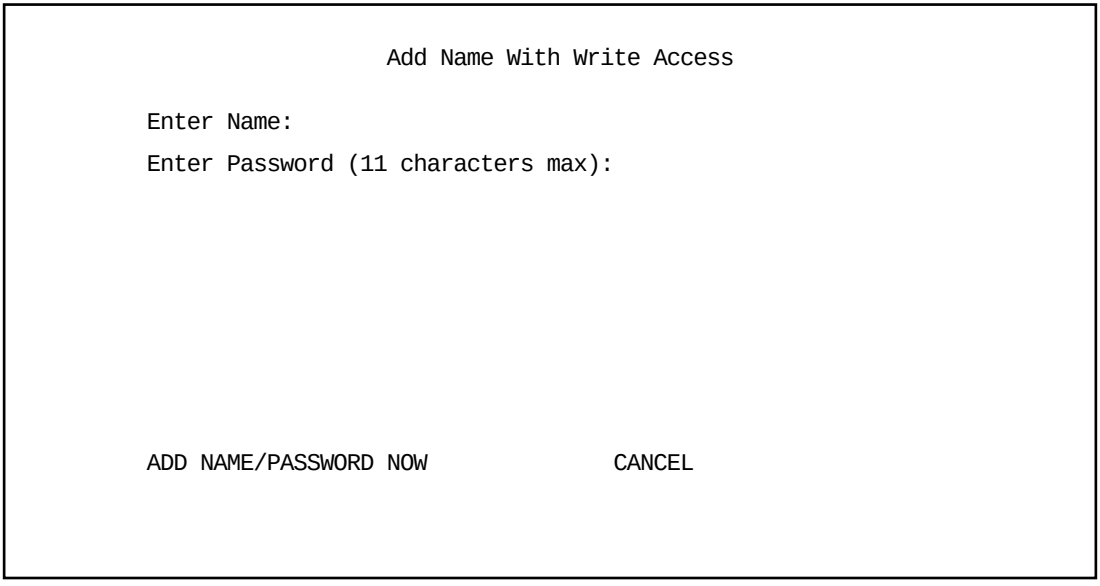
Select **Password for This Screen** in the Security Options screen and enter a password. Make sure this password is secure and is different from any of the user account passwords.

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.



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.

Dial-in console access

Remote modem terminal emulator setups can dial in to the modem line and establish a remote console session, even though they are not using PPP. This allows Netopia Inc.'s "Up and Running, Guaranteed!" department or other administrator with the appropriate security to remotely configure your router for you.

- To prevent any remote caller from establishing a remote session, set the option **Enable Dial-in Console Access** to **No**.
- To allow access for Up and Running, Guaranteed! with the default name and password in place, toggle this option to **Yes**.

Enable SmartStart/SmartView/Web server

You may want to restrict access to the Web-based screens to prevent inadvertent switching or connecting and disconnecting of connection profiles. Since SmartStart can be used to reconfigure the router, you may want to block inadvertent damage resulting from unauthorized use of SmartStart. To prevent access to these features toggle this option to **No**.

Telnet access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. The Netopia R9100 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Netopia R9100 if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the **Easy Setup Security Configuration** screen. By entering a name and password pair in this screen, all access via serial, Telnet, SNMP, and Web server will be password-protected.

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 12-14.)

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

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 R9100's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the router's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called firewalling your network.

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

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

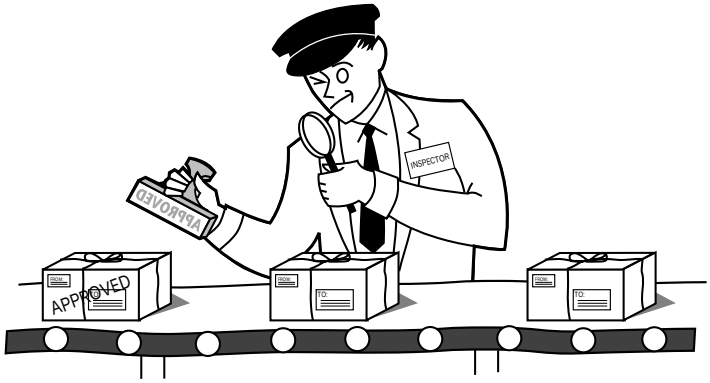
A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can be either an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network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

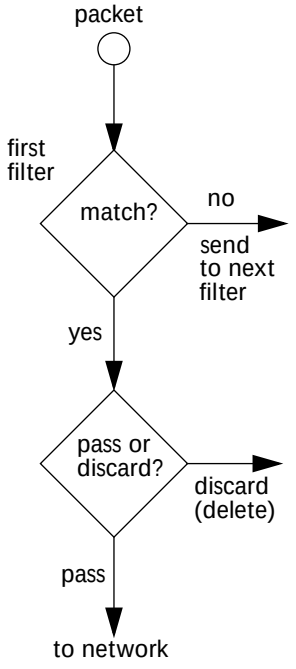
Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to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



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 R9100:

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

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

Parts of a filter

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

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

Port numbers

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

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

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

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

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

Port number comparisons

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

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

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

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

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

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

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

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

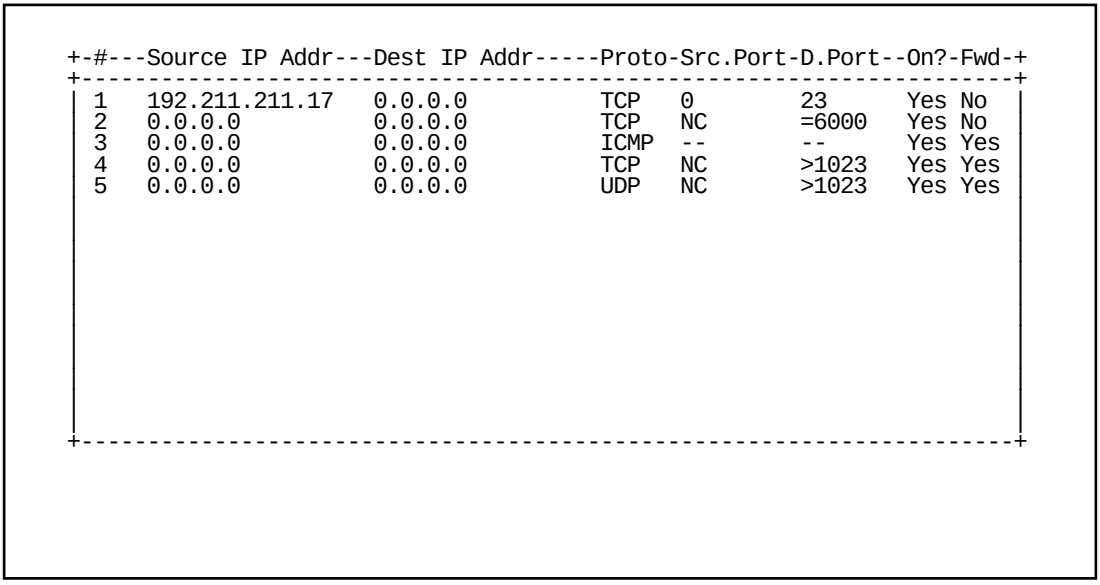
Other filter attributes

There are three other attributes to each filter:

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

Putting the parts together

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



```
+-#---Source IP Addr---Dest IP Addr-----Proto-Src.Port-D.Port--On?-Fwd-+
+-------------------------------------------------------------------+
| 1   192.211.211.17   0.0.0.0          TCP   0        23      Yes No  |
| 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 page 13-7), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

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

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

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

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

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

3. Using the tables on page 13-8, find the destination port and protocol numbers (the *local* Telnet port):

   - Proto = TCP (or 6)
   - D. Port = 23

4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:

   - On? = Yes
   - Fwd = No

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

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

Filtering example #2

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

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

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

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

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

Design guidelines

Careful thought 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.

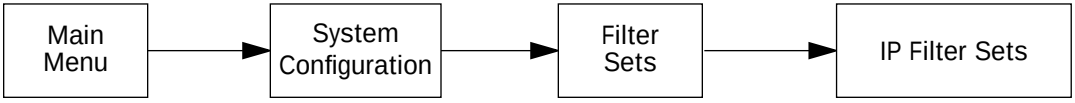
Each filter set you design will be based on one of the following approaches:

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

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

Working with IP filters and filter sets

This section covers IP filters and filter sets. For working with IPX filters and filter sets, see "IPX filters" on page 13-21.



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 13-4.

```
                              IP Filter Sets

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









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

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

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

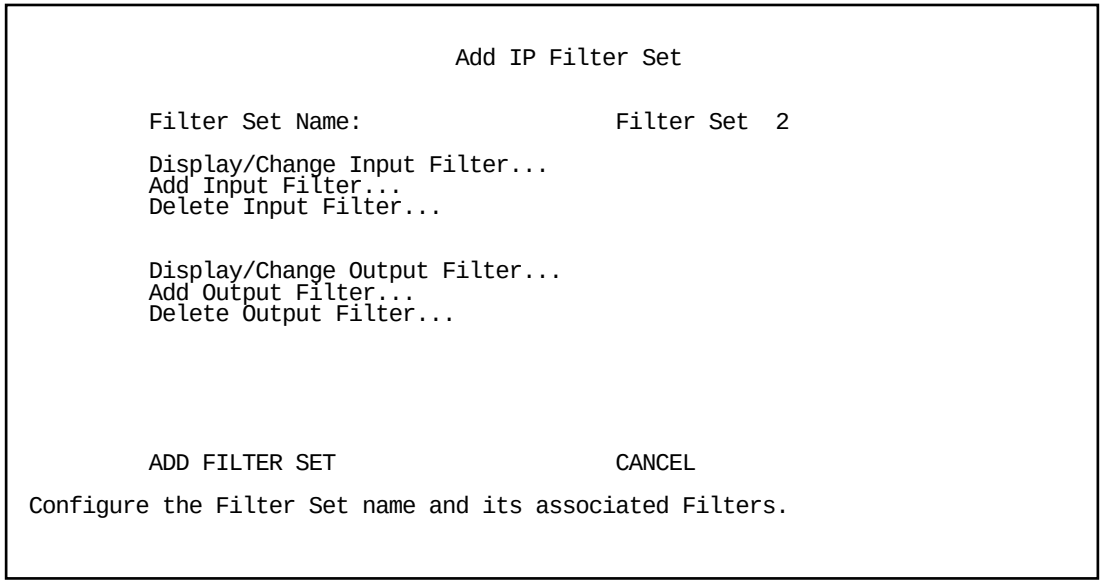
The sections below explain how to execute these steps.

Adding a filter set

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

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

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



Naming a new filter set

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

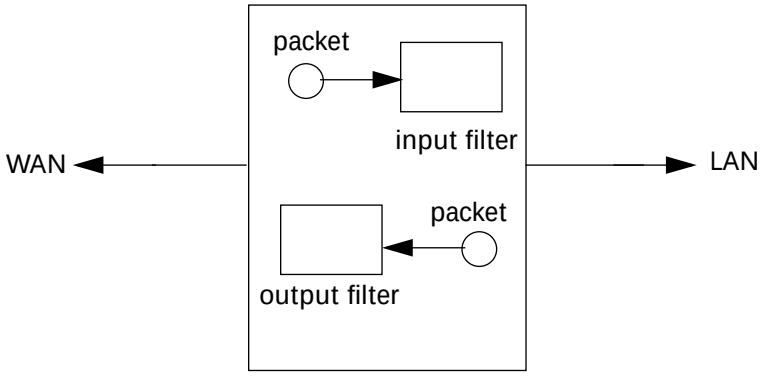
To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see "Modifying filter sets" on page 13-17). Or you can add filters to your new set before saving it (see "Adding filters to a filter set" on page 13-14).

To leave the Add Filter Set screen without saving the new filter set Select **CANCEL**. You are returned to the IP 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 R-Series Router

Packets in the Netopia R9100 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

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

Type of filter	"Source" means	"Destination" means
Input filter	The remote network	The local network
Output filter	The local network	The remote network

Adding filters to a filter set

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

To add an input filter, select **Add Input Filter** in the Add IP Filter Set screen. The Add Filter screen appears. (To add an output filter, select **Add Output Filter**.)

```
                                  Add Filter

                        Enabled:                    No
                        Forward:                    No

                        Source IP Address:          0.0.0.0
                        Source IP Address Mask:     0.0.0.0

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

                        Protocol Type:              0

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

                        ADD THIS FILTER NOW         CANCEL

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

1. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.
2. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.
3. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.
4. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
5. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
6. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
7. Select **Protocol Type** and enter **ICMP**, **TCP**, **UDP**, **Any**, or the number of another IP transport protocol (see the table on page 13-9).

   Note: If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.
8. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on page 13-8).
9. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on page 13-8).

10. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter and return to the Add IP Filter Set screen.

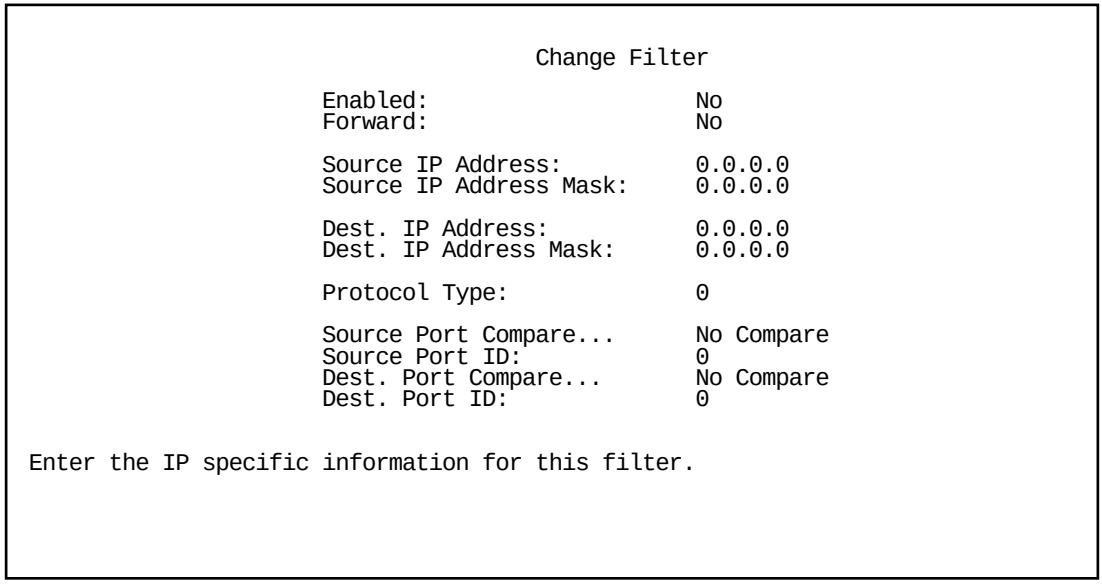
Viewing filters

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

Modifying filters

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

Select a filter from the table and press Return. 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 13-14).



Deleting filters

To delete a filter, select **Delete Input Filter** or **Delete Output Filter** in the Add IP 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.

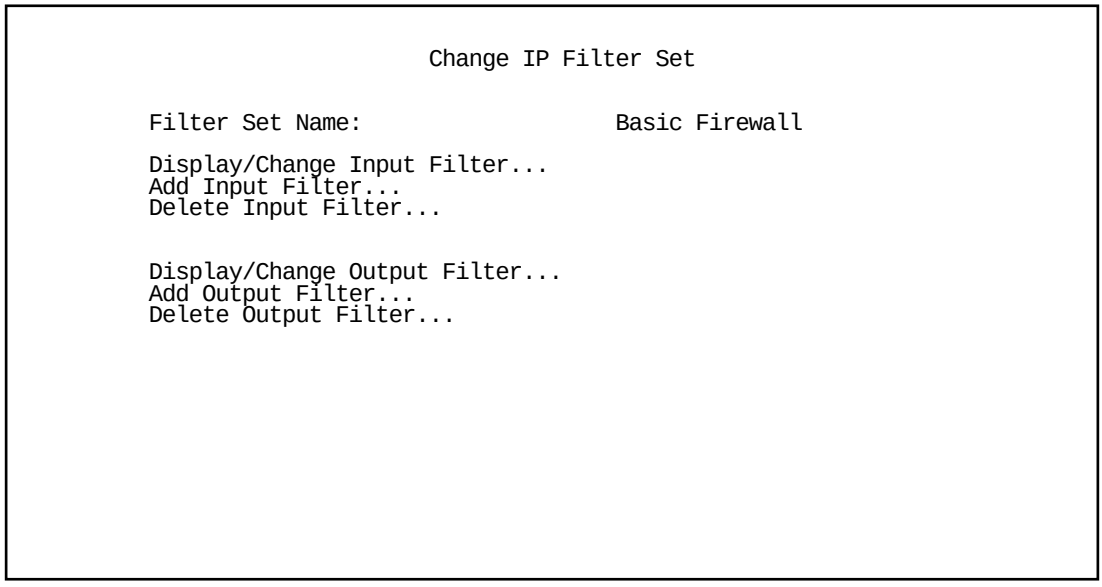
Viewing filter sets

To display a view-only list of filter sets, select **Display / Change IP Filter Set** in the IP Filter Sets screen.

Modifying filter sets

To modify a filter set, select **Display / Change IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return. The Change IP 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 13-14).



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 IP Filter Set** in the IP Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return to delete it. Press Escape to exit the list without deleting the filter set.

A sample IP filter set

This section contains the settings for a filter set called Basic Firewall, which is part of the Netopia R9100’s factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but passes all traffic originating from the LAN. It follows the conservative “that which is not expressly permitted is prohibited” approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall's filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect since filter 4 would have already passed OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly passes all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters pass all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter passes all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that want to access servers on the WAN, but not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly pass WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See the next section, "Possible modifications," for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if you are making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

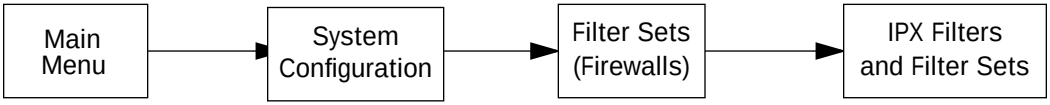
- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or to 80 for WWW.

AURP tunnel. To allow an AURP tunnel between a remote AURP router with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243) and a local AURP router (including the Netopia R9100 itself), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: UDP
- Source Port Comparison: Equal
- Source Port ID: 387
- Dest. Port Comparison: Equal
- Dest. Port ID: 387

IPX filters



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

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

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

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

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

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

```
                    IPX Filters and Filter Sets

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

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

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

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



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

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

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

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

IPX packet filters

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

Viewing and modifying packet filters

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

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

Adding a packet filter

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

```
                        Add Packet Filter

          Filter Name:                                IPX Filter 1

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

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









          ADD FILTER NOW                              CANCEL

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

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

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

Deleting a packet filter

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

IPX packet filter sets

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

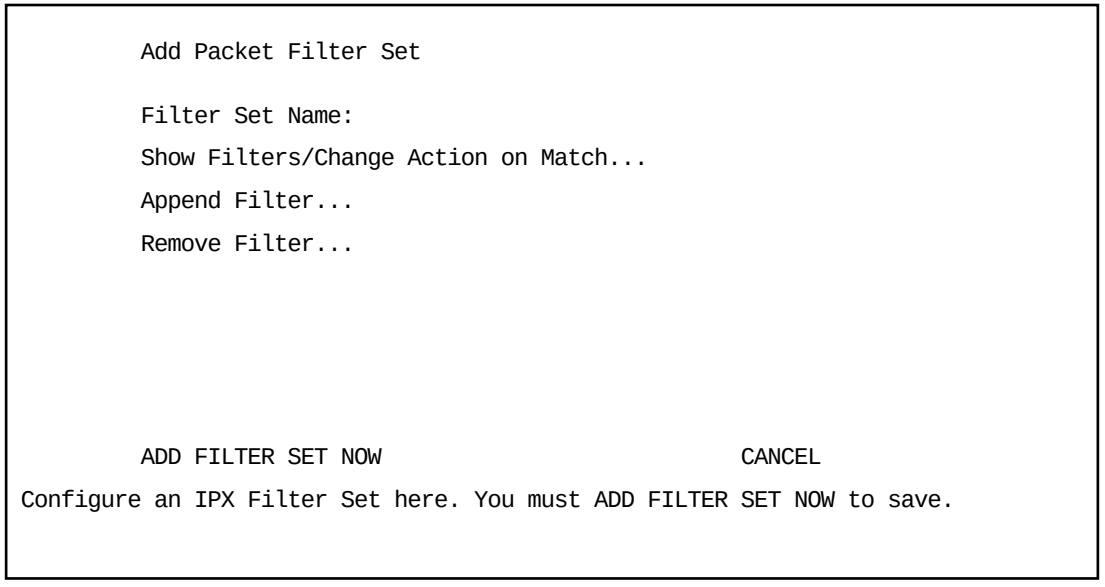
Viewing and modifying packet filter sets

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

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

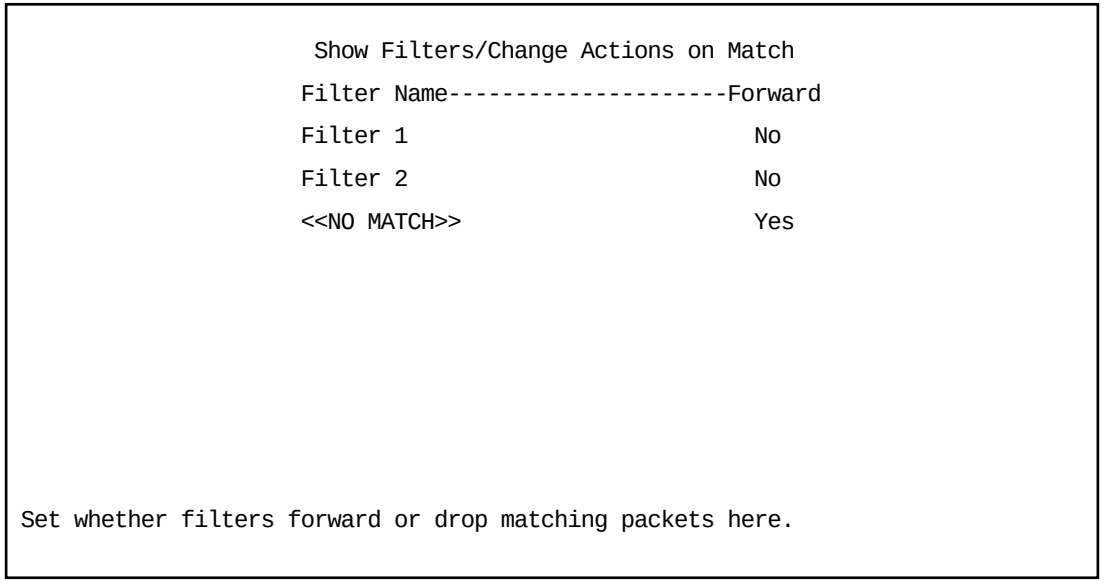
Adding a packet filter set

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



Follow these steps to configure the new packet filter set:

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



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

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

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

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

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

Deleting a packet filter set

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

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

IPX SAP filters

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

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

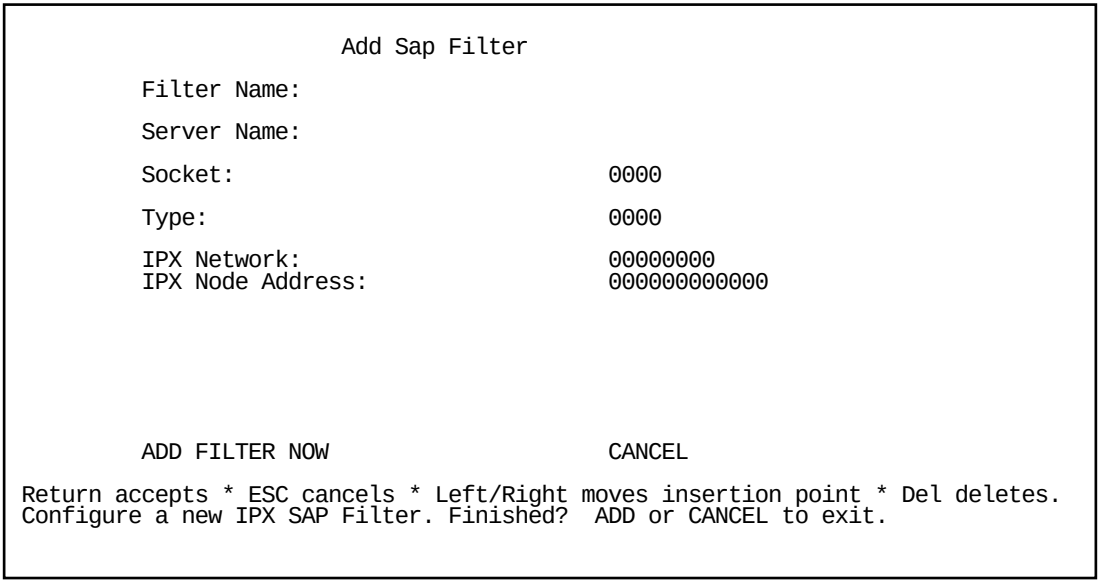
Viewing and modifying SAP filters

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

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

Adding a SAP filter

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



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

Follow these steps to configure the new SAP filter:

1. Select **Filter Name** and enter a descriptive name for the filter.
2. To specify a server name for the filter to match on, select **Server Name** and enter the name of an IPX server. You can use the wildcard characters * (asterisk) and ? (question mark). Use * to match any string, including a null string (no characters), and ? to match any single character in the server's name. For example, the filter could match on the server name "NETOPIA" with "NETO*", "NETO?IA", and "NETOPIA*".
3. To specify a socket for the filter to match on, select **Socket** and enter an IPX socket number.
4. To specify a type number for the filter to match on, select **Type** and enter an IPX type number.
5. To specify an IPX network address for the filter to match on, select **IPX Network** and enter an IPX network address.
6. To specify an IPX node address for the filter to match on, select **IPX Node Address** and enter an IPX node address.
7. Select **ADD FILTER NOW** to save the current filter. Select **CANCEL** to exit the Add SAP Filter screen without saving the new filter.

Deleting a SAP filter

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

IPX SAP filter sets

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

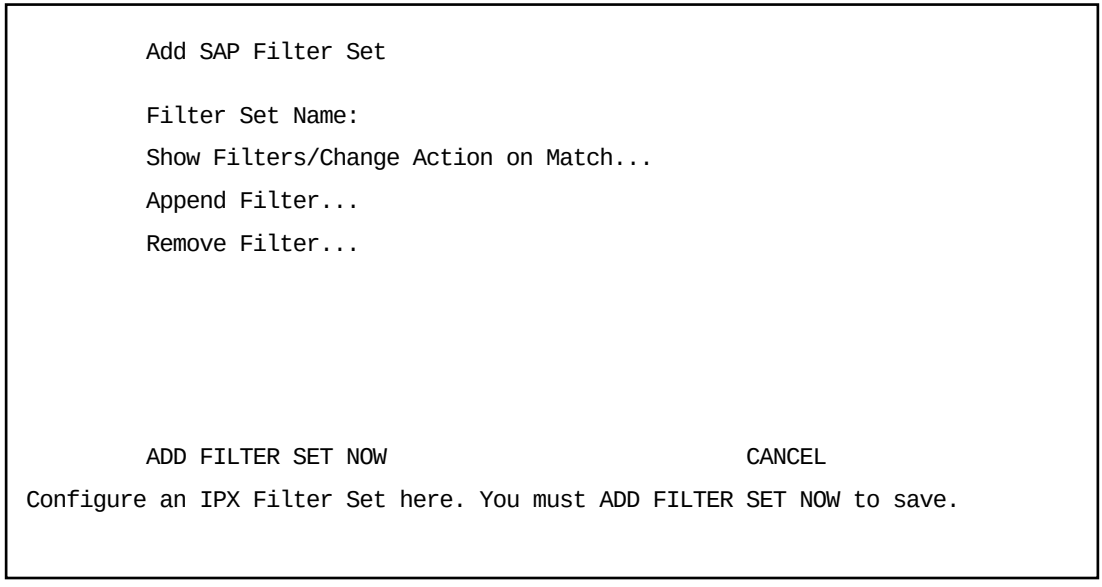
Viewing and modifying SAP filter sets

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

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

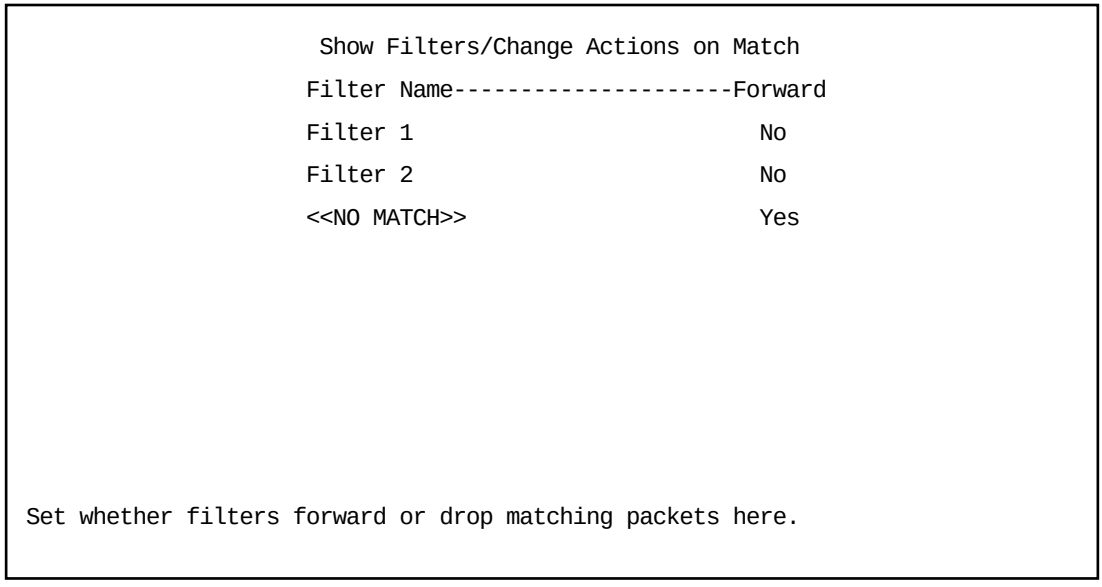
Adding a SAP filter set

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



Follow these steps to configure the new SAP filter set:

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



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

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

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

4. To remove a filter from the filter set, select **Remove Filter** in the Add SAP Filter Set screen to display a table of appended filters. Select a filter from the table and press Return to remove it from the set. To exit the table without removing the filter, press Escape.

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

Deleting a SAP filter set

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

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

Firewall tutorial

General firewall 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 a packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions.

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 table that follows shows some of these port assignments.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP	387	AURP
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- "What is not explicitly allowed is denied."

and

- "What is not explicitly denied is allowed."

The first rule is far more secure, and is the best approach to firewall 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.

Firewall Logic

Firewall 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:

0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255 BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15 BINARY: 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 firewall 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 IP filter set screen:

```
                                Change Filter

          Enabled:                          Yes
          Forward:                          No

          Source IP Address:                0.0.0.0
          Source IP Address Mask:           0.0.0.0

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

          Protocol Type:                    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 IP specific information for this filter.
```

Filter basics

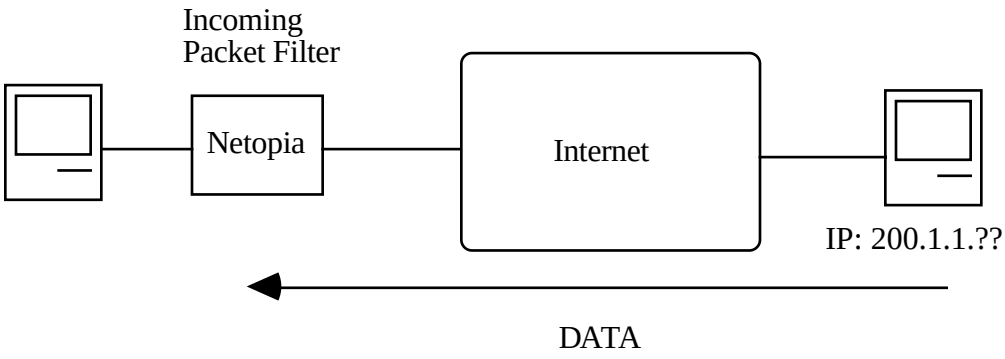
In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia R9100 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No Compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined

Less Than or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined

Example network



Example filters

Example 1

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

IP Address	Binary Representation	
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 (00000000) in the Netopia R9100. 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 R9100. 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	
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 R9100 is 01100000, 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 R9100 is 01100000, 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 R9100 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.

Chapter 14

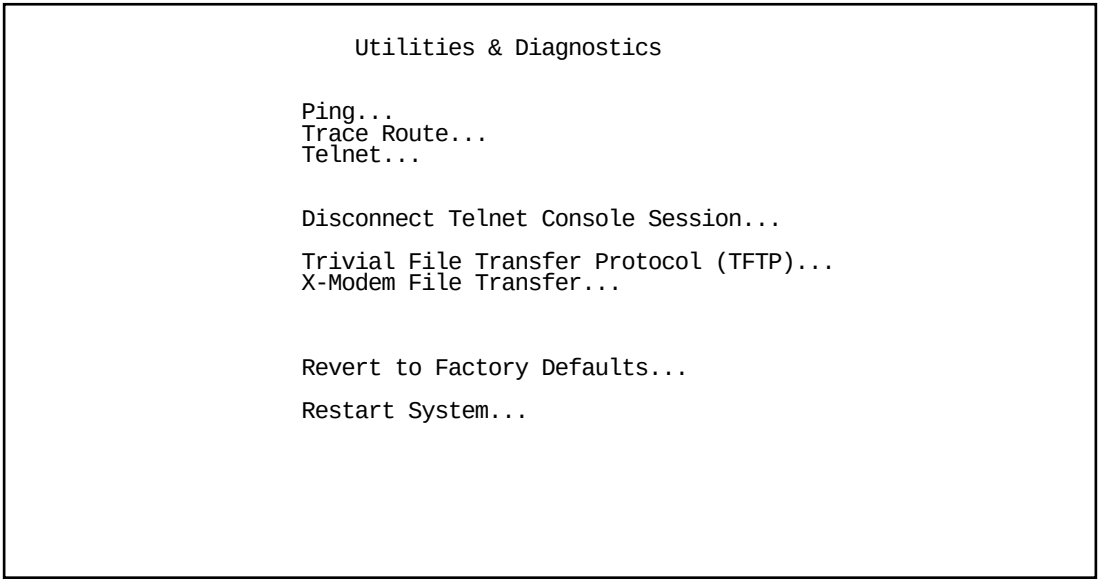
Utilities and Diagnostics

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 6, "Console-Based Management," for information on accessing the console-based management screens.

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

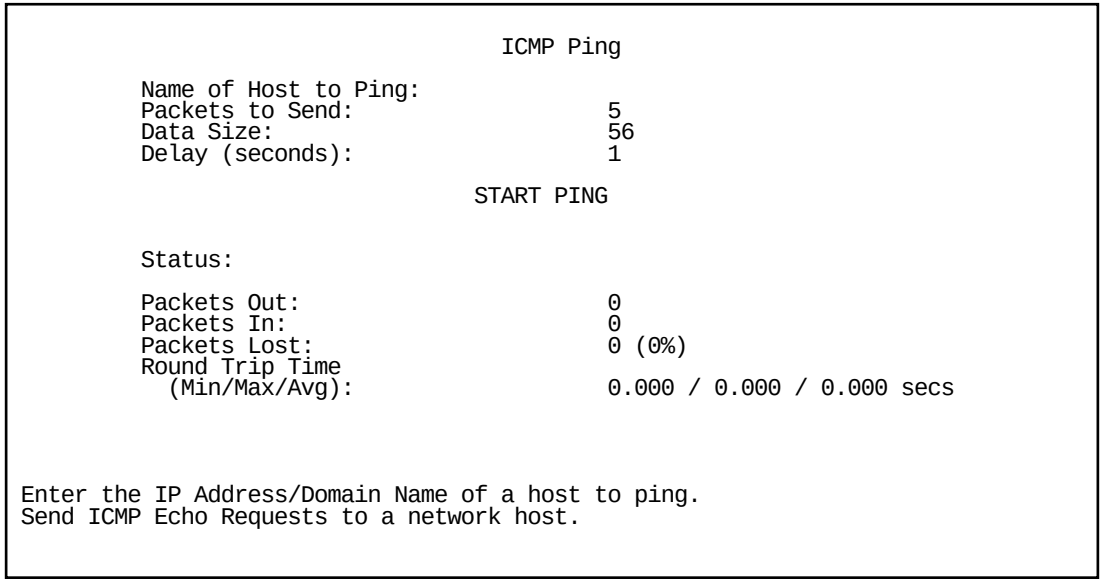


Ping

The Netopia R9100 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 R9100. 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.



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.

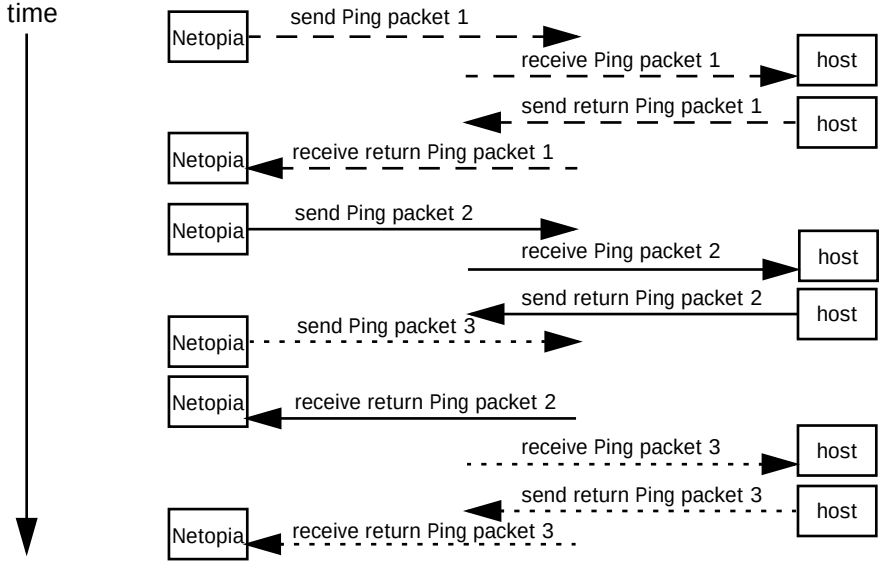
Status: The current status of the Ping test. This item can display the status messages shown in the able below:

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 R9100 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 R9100 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**.

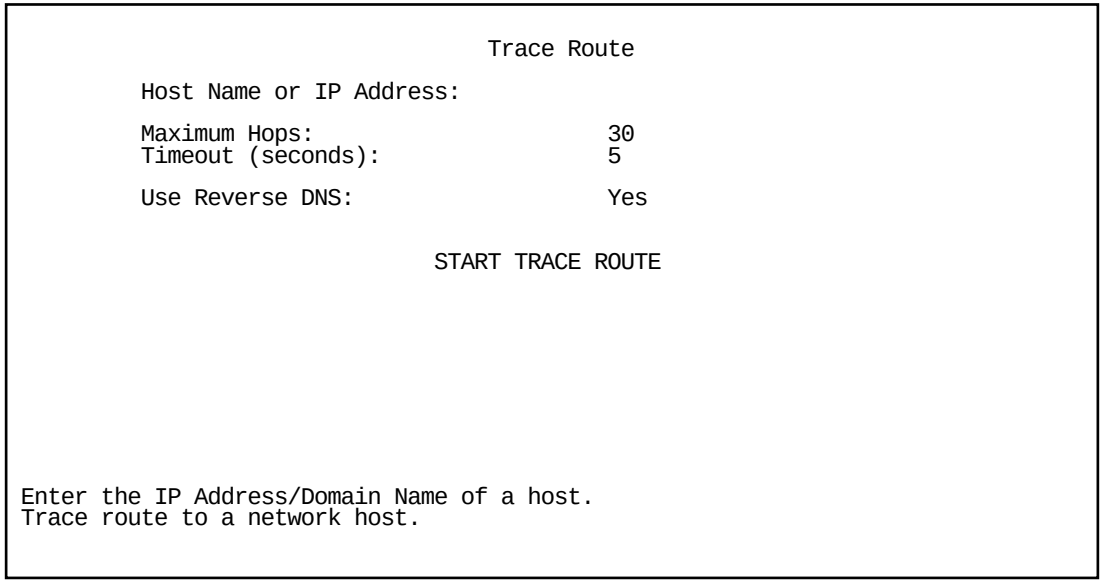
Round Trip Time (Min / Max / Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Netopia R9100 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 Router 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.



To trace a route, follow these steps:

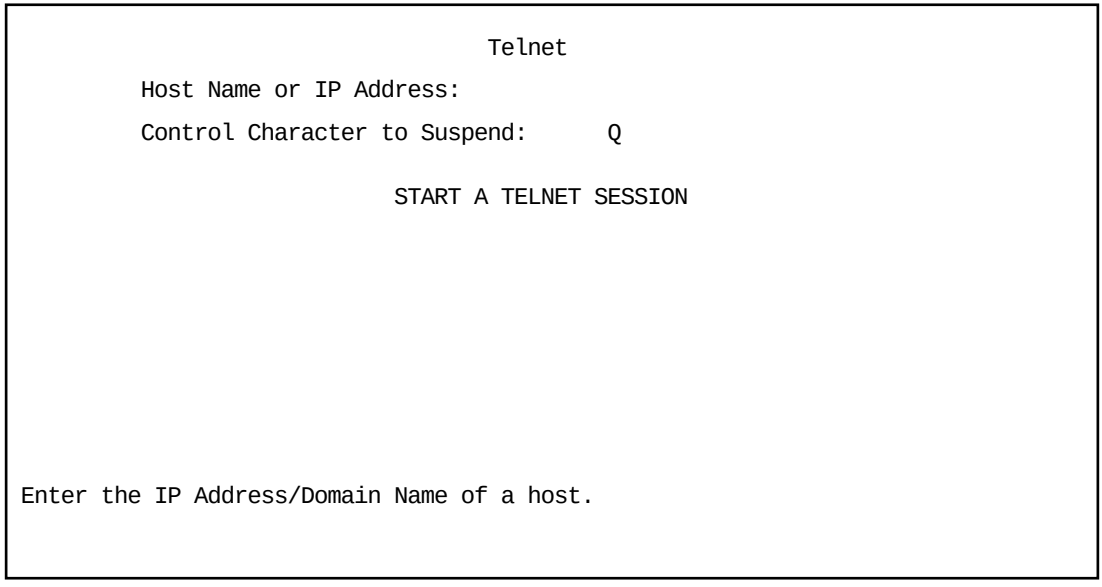
1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum Hops** to set the maximum number of routers to count between the Netopia Router and the destination router, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout (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 Router 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.



- 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):

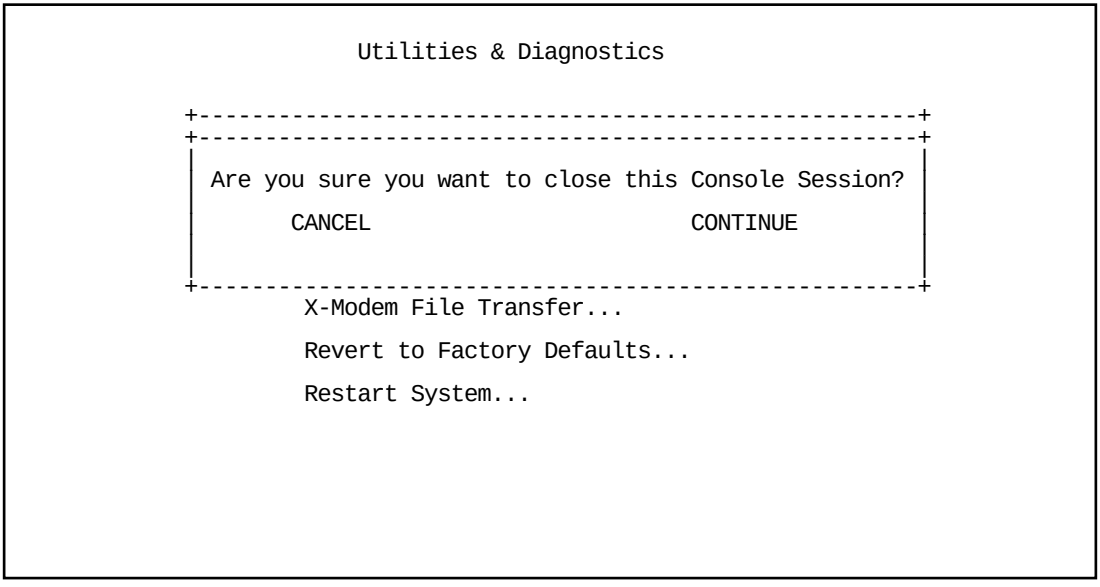
  Resume Suspended Session – select this one if you want to go back to your Telnet session

  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.



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

Factory defaults

You can reset the Netopia R9100 to its factory default settings. In the Statistics & Diagnostics screen, select **Revert to Factory Defaults** and press Return. Select **CONTINUE** in the dialog box and press Return. The Netopia R9100 will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset switch to return the router to its factory default settings. Call Netopia Tech Support for instructions on using the Reset switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all of your settings in the router.

Transferring configuration and firmware files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the router as the client. To use the Netopia R9100 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 R9100's firmware and how to download and upload configuration files.

Updating firmware

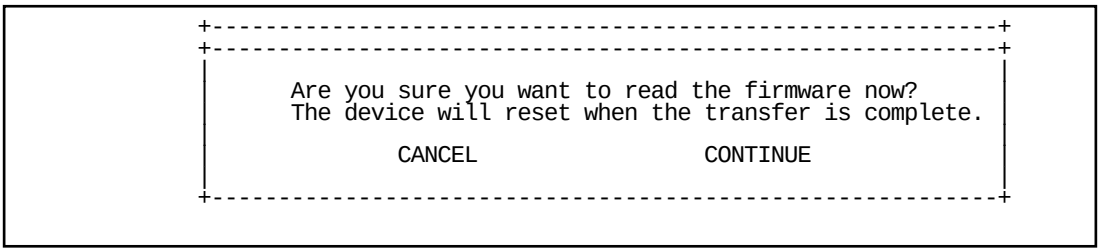
Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

There are two types of firmware in the Netopia R9100 Ethernet Router: router firmware and WAN module firmware. The router firmware governs how the router 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 Netopia 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 router'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:



- 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 router 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 R9100 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.

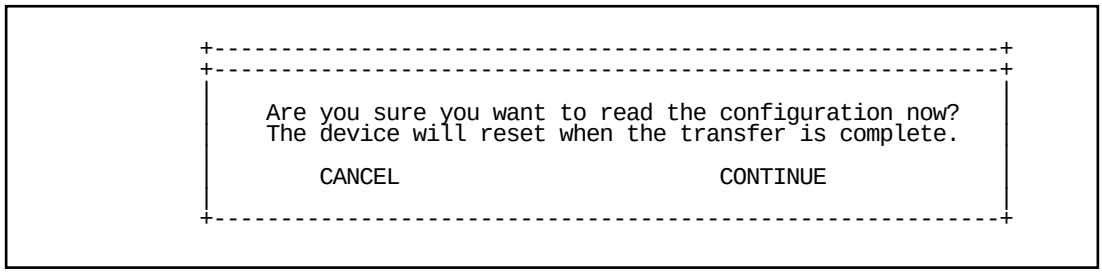
Downloading configuration files

The Netopia R9100 can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the router's parameters as if someone had manually done so through the console port.

To download a configuration file, follow these steps:

- 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:



- 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 router's current configuration to a TFTP server. The file can then be downloaded by a different Netopia R9100 unit to configure its parameters (see "Downloading configuration files" on page 14-8). 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 R9100 unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

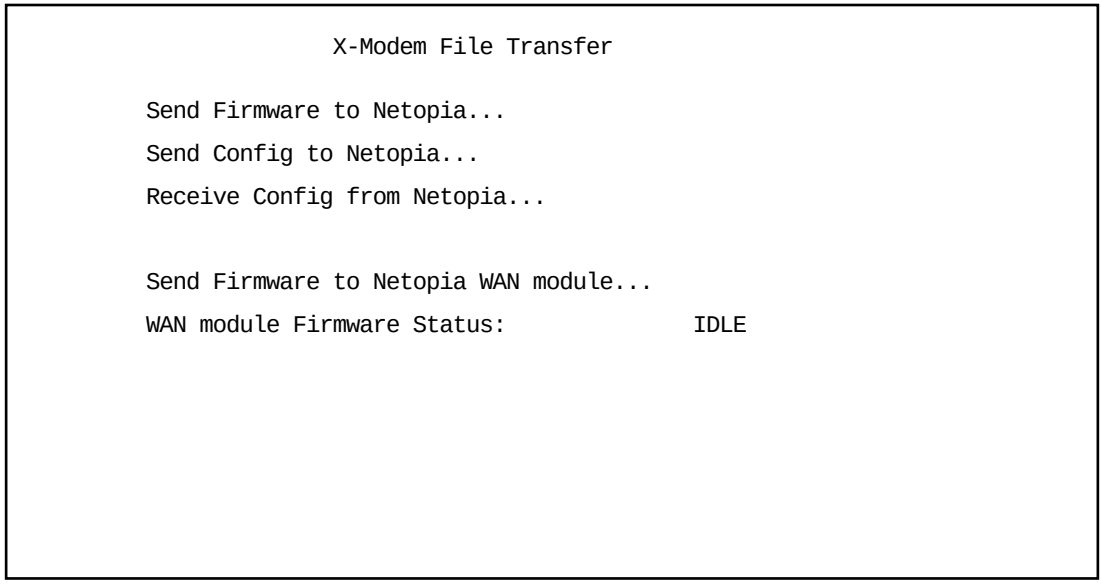
1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name 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 R9100'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.

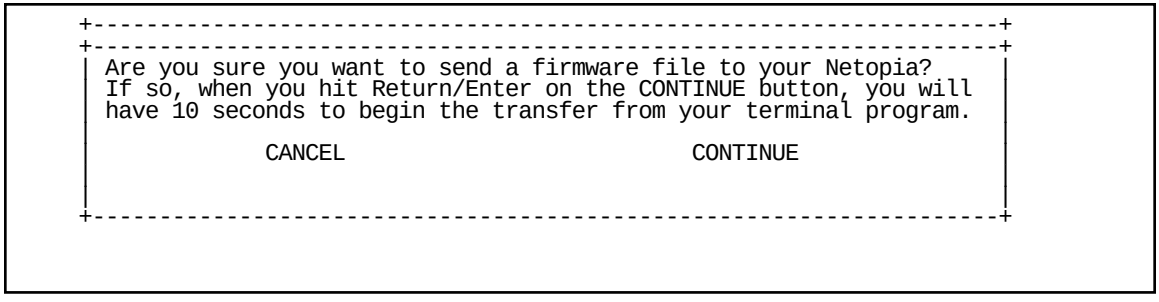


Updating firmware

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 R9100'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:



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 R9100 while it is automatically resetting or it could be damaged.

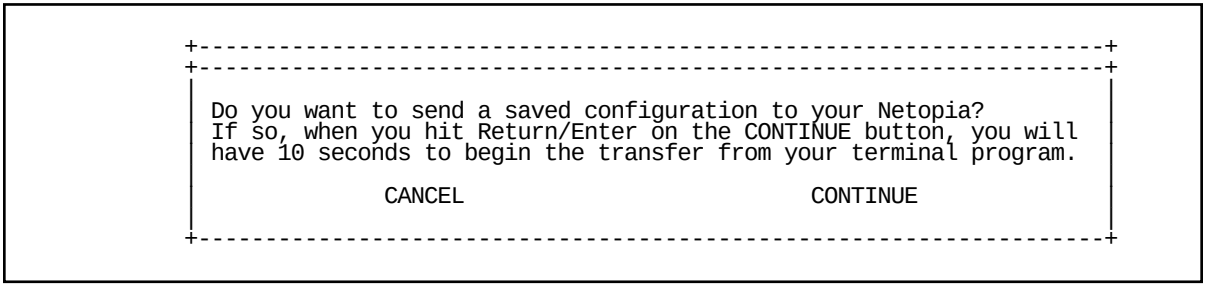
Downloading configuration files

The Netopia R9100 can be configured by downloading a configuration file. The downloaded file reconfigures all of the Router's parameters.

Configuration files are available from a site maintained by your organization's network administrator or from your local site (see "Uploading configuration files," below).

Follow these steps to download a configuration file:

1. Make sure you have the configuration file on disk and know the path to its location.
2. Select **Send Config to Netopia** and press Return. The following dialog box appears:



3. Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file.

   If you choose CONTINUE, you will have ten seconds to use your terminal emulation software to initiate an XMODEM transfer of the configuration file. If you fail to initiate the transfer in that time, the dialog box will disappear and the terminal emulation software will inform you of the transfer's failure. You can then try again.

   The system will reset at the end of a successful file transfer to put the new configuration into effect.

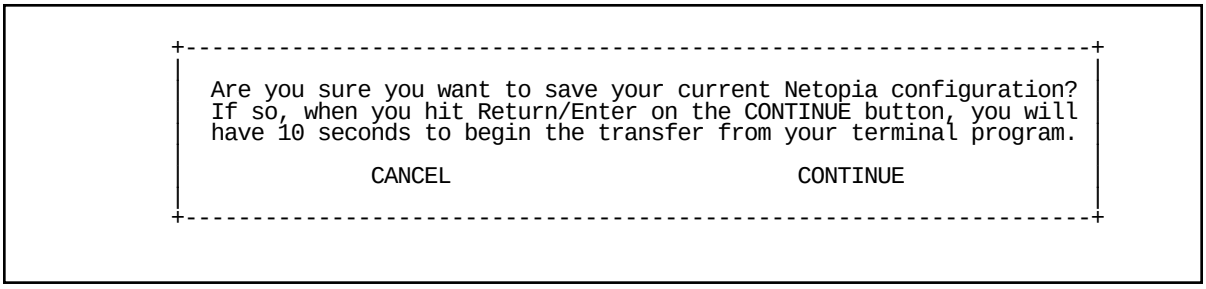
Uploading configuration files

A file containing a snapshot of the Netopia R9100's current configuration can be uploaded from the router to disk. The file can then be downloaded by a different Netopia R9100 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 R9100 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:



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 R9100 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 R9100. 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 R9100. These event histories can be accessed in the Statistics & Logs screen.

This section covers the following topics:

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 router
2. The router'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 router was not successful, verify that the following conditions are in effect:

- The Netopia R9100 is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Netopia R9100.
- The SmartStart application is running and able to access the Netopia R9100.
- 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 R9100'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 R9100 to the factory default before reinitiating the configuration process. For further information on resetting your Netopia R9100 to factory default, see "Factory defaults" on page 14-6.

Console connection problems

Can't see the configuration screens (nothing appears)

- Make sure the cable connection from the Netopia R9100'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 R9100'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 R9100's Ping utility, in the Utilities & Diagnostics screen, and try to ping local and remote hosts. See "Ping" on page 14-2 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 R9100 (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

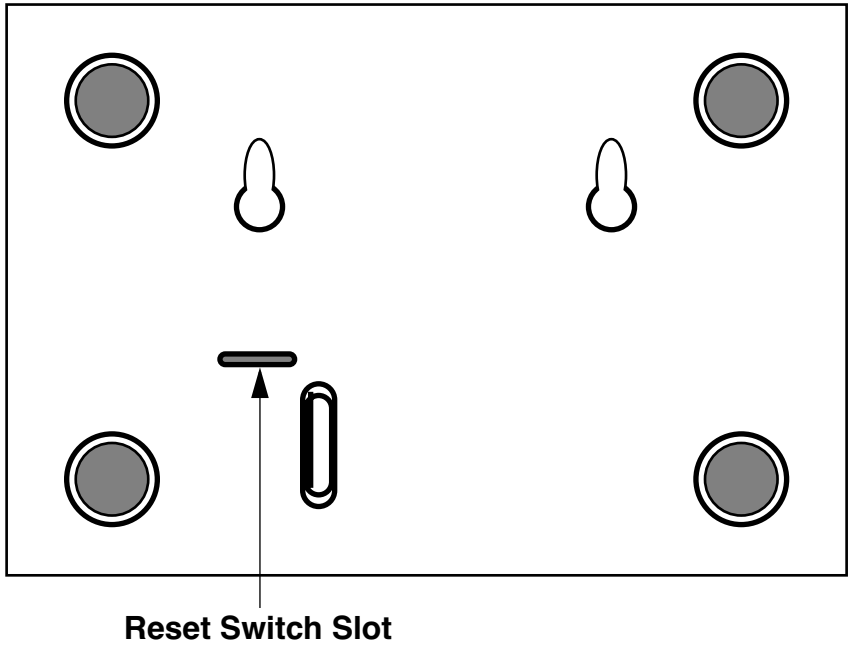
- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN statistics and LAN statistics screens to see more specific information on data traffic flow and address serving. See "Statistics & Logs" on page 12-3 for more information.

How to reset the router to factory defaults

Lose your password? This section shows how to reset the router 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 R9100 is the following:

1. Turn the router upside down.
2. Referring to the diagram below, find the paper clip size 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 router.

Power outages

If you suspect that power was restored after a power outage and the Netopia R9100 is connected to a remote site, you may need to switch the Netopia R9100 off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the router should reestablish the connection.

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 R9100's model number, product serial number, and firmware version. The serial number is on the bottom of the router, along with the model number. The firmware version appears in the Netopia R9100'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 R9100. 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

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia R9100 and using some of its powerful features, such as static routes and packet filtering.

In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

This section covers the following topics:

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate.

Note: This guide uses the term "IP" in a very general and inclusive way to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
- Packets that include an IP header within their structure
- Devices that send IP packets

About IP addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations that request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1–127	127	16,777,214	net.host.host.host	97.3.14.250
B	128–191	16,384	65,534	net.net.host.host	140.100.10.11
C	192–223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP routers, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP routers and gateways such as the Netopia R9100.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

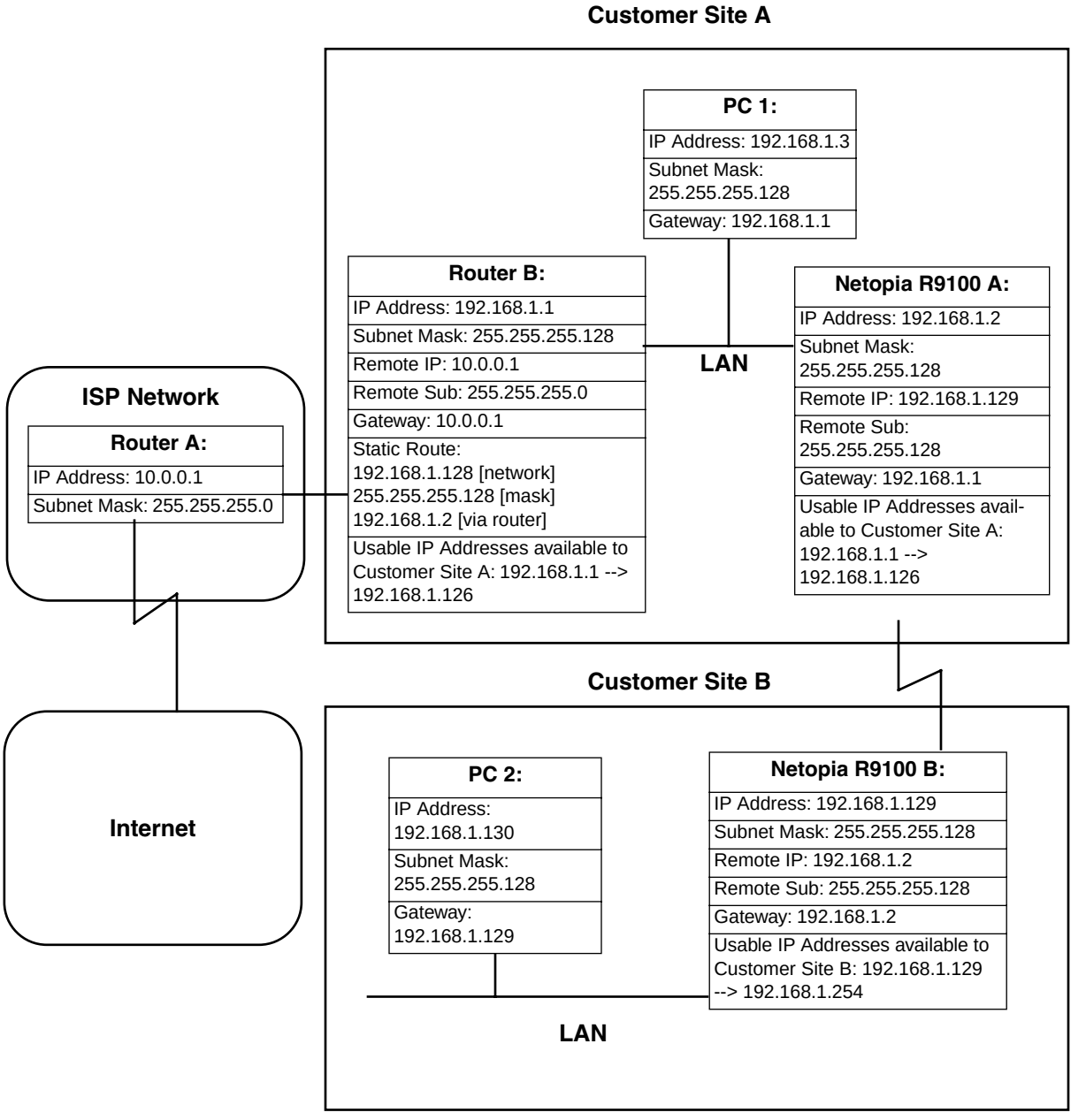
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A Address, or even with multiple Class C Addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia routers so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Netopia R9100 B connects to Netopia R9100 A and is provided Internet access through Routers A and B.



Background

The IP addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The IP Address and Subnet Mask fields define the IP address and subnet mask of the device's Ethernet connection to the network while the Remote IP and Remote Sub fields describe the IP address and subnet mask of the remote router. This information is entered in the connection profile of the Netopia R9100.

The Gateway field describes the router or workstation's default gateway, or where they will send their packets if the appropriate route is not known. The Static Route field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Netopia R9100 B. Finally, the Usable IP Address field shows the range of IP addresses available to the hosts of that network.

Note that the IP addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the static route defined on Router B. This tells Router B what path to take to get to the network defined by Netopia R9100 B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a static route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a static route, enable Transmit RIP on Netopia R9100 A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts, and no plans to add any new hosts. You don’t need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you might obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP’s network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages of this situation are the greater ease and lower cost of obtaining a subnet rather than a full Class C address from an ISP.

Distributing IP addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an Internet service provider. When configuring the Netopia R9100, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Netopia R9100 automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Netopia R9100. Using the router in this way allows it to function as an address server.

One reason to use the Netopia R9100 as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You need to enter information only once, rather than having to repeatedly enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Netopia R9100 as an address server is that it will distribute addresses only to hosts that need to use them.

All Netopia R9100s come with an integrated Dynamic Host Control Protocol (DHCP) server. Some routers also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Netopia R9100, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information is helpful in determining dynamic address allocation for a network.

The term "lease" describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term "renew" refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term "release" refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Netopia R9100 will be a unique number. You may want to replace this number with a number that your ISP supplies if you are configuring the router for a static IP address. The automatic IP mask supplied by SmartStart is a Class C address. However, the Netopia R9100 and all devices on the same local network must have the same subnet mask. If you require a different class address, you can edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Netopia R9100) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248
6-13	255.255.255.240
14-29	255.255.255.224

Number of Devices (other than Netopia R9100) on Local Network	Largest Possible Ethernet Subnet Mask
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP address serving

Windows 95 workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program from the Win95 machine, that is a command line program executable from the DOS prompt or from the START:RUN menu.

Windows 3.1 workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG/RELEASE from a DOS window within Windows or from the DOS prompt.

Macintosh workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation relinquishes its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at startup, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia R9100 DHCP server characteristics

- The Netopia R9100 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The number of devices a Netopia R9100 can serve DHCP to is 512. This is imposed by global limits on the size of the address serving database, which is shared by all address serving functions active in the router.

- The Netopia R9100 does release the DHCP address back to the available DHCP address pool precisely one hour after the last-heard lease request as some other DHCP implementations may hold on to the lease for an additional time after the lease expired, to act as a buffer for variances in clocks between the client and server.

MacIP serving

Macintosh workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Netopia R9100 actively checks for the workstation's existence once every minute.

- For a dynamic address, the Netopia R9100 releases the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a static address, the Netopia R9100 releases the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia R9100 MacIP server characteristics

The Mac workstation uses ATP to both request and receive an address from the Netopia R9100's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Netopia R9100 to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are sometimes called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. Appropriate candidates for a static address include: a network administrator's computer, a computer dedicated to communicating with the Internet, and routers.

Using address serving

The Netopia R9100 provides three ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. The third way, called Serve Dynamic WAN Clients (IPCP), is used to fulfill WAN client requirements

The Netopia R9100 can use both DHCP and MacIP. Whether you use one or both depends on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Serve dynamic WAN clients

The third method, used to fulfill WAN client requirements, is called Serve Dynamic WAN Clients. This is a subset of PPP. Originally, this would apply only to switched WAN interface routers, and not to leased line routers. However, a new feature can give you Asynchronous PPP dial-in support on the Auxiliary port on any router including leased line Netopia routers.

In any situation where a device is dialing into a Netopia router, the router may need to be configured to serve IP via the WAN interface. This is only a requirement if the calling device has not been configured locally to know what its address(es) are. So when a client, dialing into a Netopia router's WAN interface, is expecting addresses to be served by the answering router, you must set the answering Netopia router to serve IP via its WAN interface.

You can do this in either of two ways:

- use the Serve Dynamic WAN Clients option in the Address Serving Setup screen.

  Serve Dynamic WAN Clients enabled only allows a user to specify a pool of address from which the dial-in client may get an IP address from. It does not allow static addressing.

  If you want to obtain addresses dynamically, use Serve Dynamic WAN Clients.

- define the address that the user wants to serve in the Connection Profile's IP Setup screen.

  This method requires a static value to be used. Thus any user dialing in can obtain the same IP address for every connection to the profile.

  If you want to obtain addresses statically, define the address in the Connection Profile.

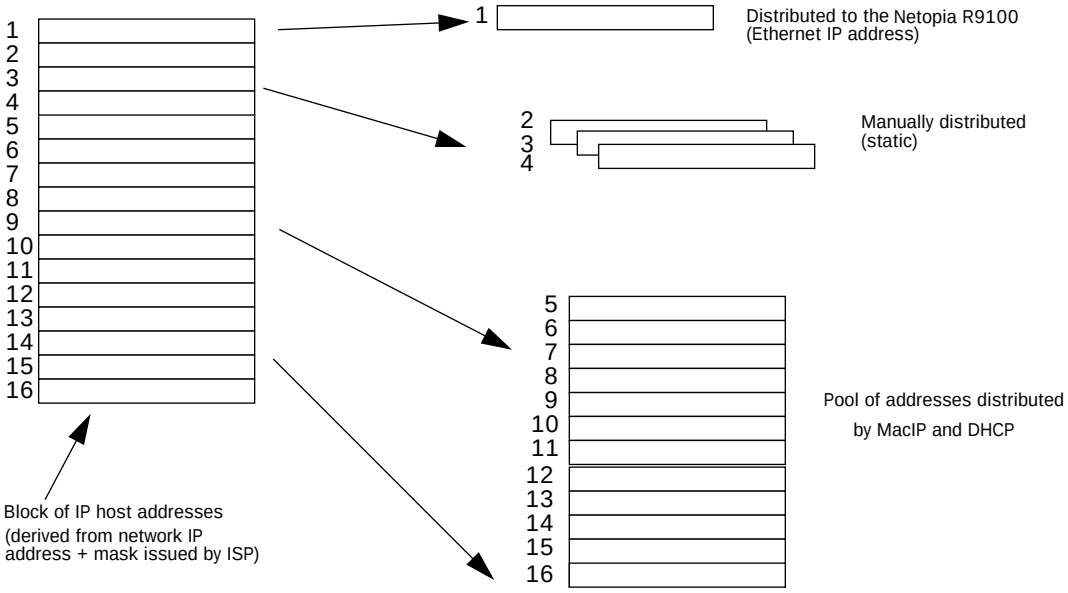
  Notes:

  - The addresses that are to be served cannot be used elsewhere. For example you wouldn't want to define a static address in a Connection Profile to be served via the WAN that is already defined in the DHCP pool of addresses.
  - In order to work correctly, you must define a “host” or “node” address in the IP Profile Parameters of the Connection Profile.

    This is accomplished by specifying the IP address that is to be statically served via the WAN, and then by entering a mask value of 255.255.255.255.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BootP, MacIP, and WAN clients, even though BootP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32 and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter "10" in the DHCP Setup screen's **Number of Addresses to Allocate** item. Then, in the same screen's **First Address** item, enter the first address in the sub-block to allocate so that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51).

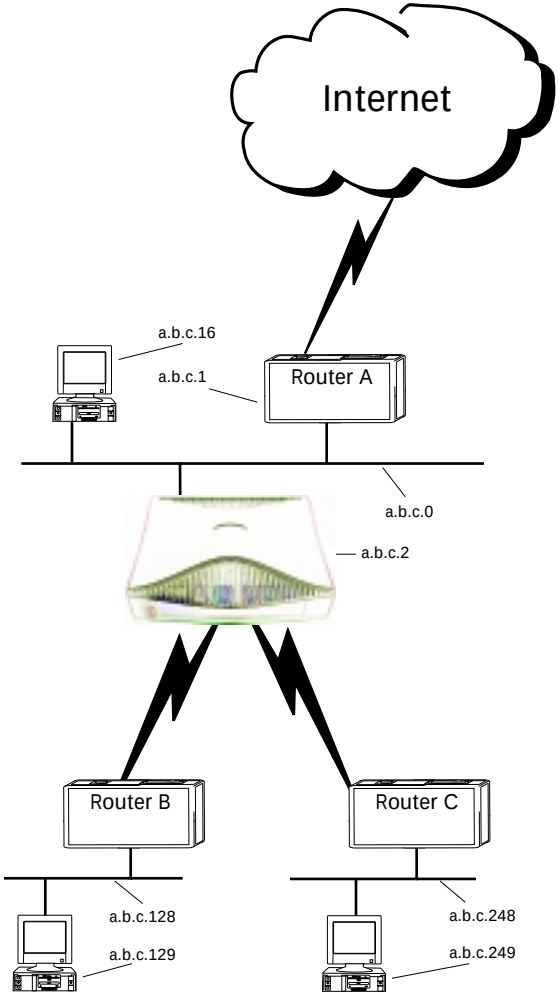
Nested IP subnets

Under certain circumstances, you may want to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network, while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure at left shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Netopia R9100), a Netopia R9100, and a number of other hosts. Router A maintains a link to the Internet, and can be used as the default gateway.



Routers B and C (which could also be Netopia R9100s) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Netopia R9100 with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
For Router B	a.b.c.128	255.255.255.192	7
For Router C	a.b.c.248	255.255.255.248	3

The Netopia R9100's connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

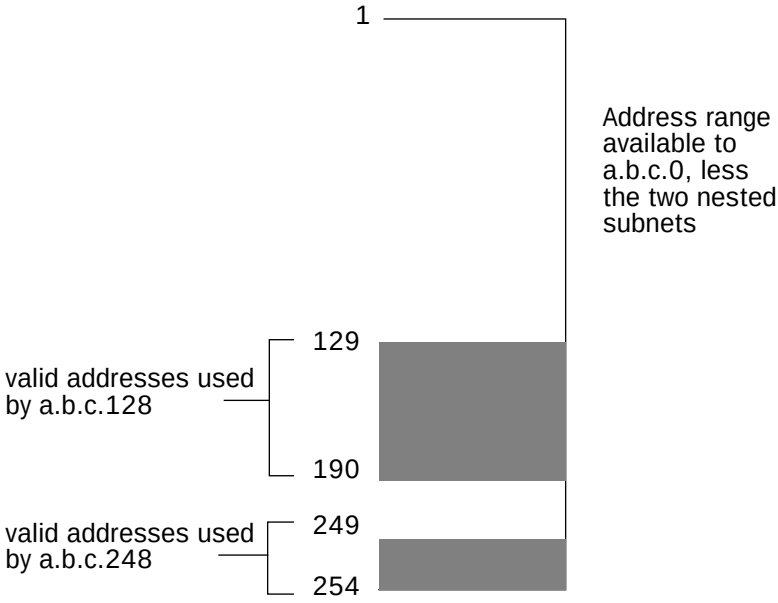
```
                              IP Routing Table

Network Address-Subnet Mask-----via Router------Port--Age--------Type------
---------------------------------SCROLL UP-------------------------------
0.0.0.0         0.0.0.0         a.b.c.1 WAN     3719              Management
127.0.0.1       255.255.255.255 127.0.0.1 lp1    6423              Local
a.b.c.128       255.255.255.192 a.b.c.128 WAN    5157              Local
a.b.c.248       255.255.255.248 a.b.c.248 WAN    6205              Local


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

Let's see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Netopia R9100, which examines its destination IP address.

The Netopia R9100 compares the packet's destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there's a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route's subnet mask, it yields a.b.c.248, which matches the network address in the route. The Netopia R9100 uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork if the host address is all ones or all zeros but the subnet address is a combination or zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Netopia R9100 uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

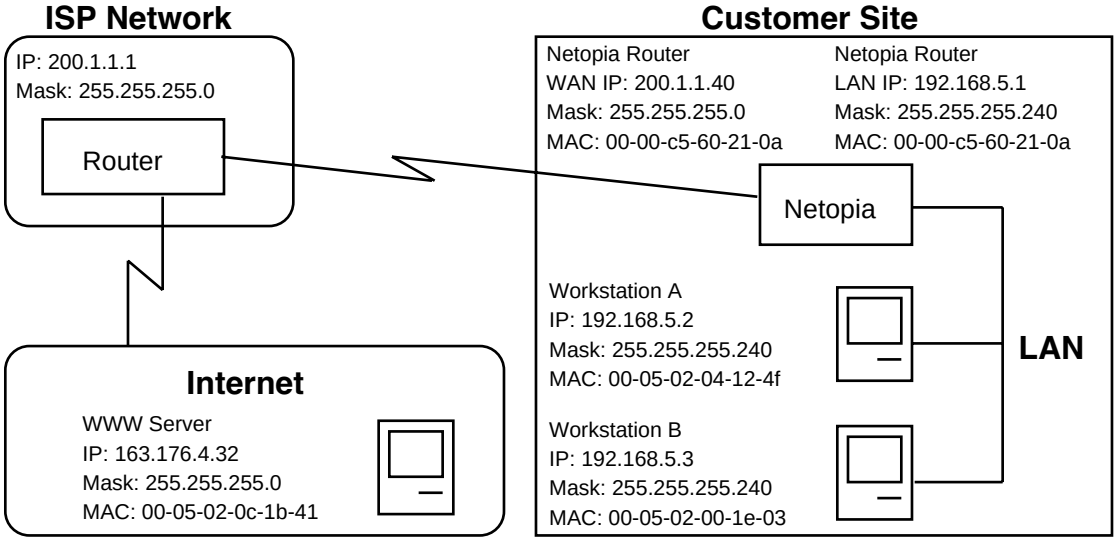
Appendix C

Understanding Netopia NAT Behavior

This appendix describes how Network Address Translation (NAT) works within the Netopia R9100. The Netopia R9100 implements a powerful feature called Network Address Translation as specified in RFC 1631. NAT is used for IP address conservation and for security purposes since there will only be a single IP "presence" on the WAN. This appendix describes the NAT functionality within the Netopia R9100 and provides examples for setup and use.

Network configuration

Below is a diagram of the network referenced in this appendix.



Background

NAT is a mechanism employed within the Netopia R9100 to acquire a statically or dynamically assigned IP address on its WAN interface and proxy against locally assigned IP addresses on its LAN interface. The Netopia R9100 uses a one-to-many IP address mapping scheme; that is against a single IP address the Netopia R9100 acquires on its WAN interface, the Netopia R9100 can proxy 14, 30, or an unlimited number of IP hosts on the LAN interface.

In order to fully understand how NAT works, you must understand how a connection is established and IP addresses are negotiated.

When the Netopia R9100 establishes a connection over its WAN interface with another router it uses the Point-to-Point Protocol (PPP). Within PPP there is a Network Control Protocol (NCP) called Internet Protocol Control Protocol (IPCP), which handles the negotiation of IP addresses between the two routers, in this case the Netopia R9100 at the customer site above and the router at the Internet service provider (ISP).

If the Netopia R9100 calls the router at the ISP with NAT disabled, the Netopia negotiates its LAN interface address (as specified in IP Setup within the Netopia R9100's console) with the router at the ISP through IPCP and then sets up routing. From the diagram on the previous page you can see that the address for the Netopia R9100 is 192.168.5.1 and the address of the router at the ISP is 200.1.1.1. Assuming that the addresses negotiated by the routers are valid and unique for the Internet, the Netopia R9100 and the hosts on its LAN would be able to access the Internet.

If the Netopia R9100 calls the router at the ISP with NAT enabled, instead of negotiating the LAN interface address, the Netopia R9100 suggests the address 0.0.0.0 through IPCP. When the router at the ISP sees this all-zeros IPCP request, the router can either pull a free dynamic IP address from its pool and assign it to the Netopia R9100's WAN interface or, if configured to do so, it can match the Netopia R9100's incoming connection profile and assign a preconfigured static IP address to the Netopia R9100's WAN interface.

From the diagram, you can see that the IP address assigned to the Netopia R9100's WAN interface is 200.1.1.40, while the IP address assigned to the LAN interface remains the same. The LAN interface address 192.168.5.1 is thus hidden from the ISP and the Internet, and the Netopia R9100 only has a single valid IP presence on the Internet. The LAN interface IP address for the Netopia R9100 can be any IP address; however, it is recommended that you use the IANA-specified 192.168.X.X Class C address range, which is used for networks not attached to the Internet. This address range is described in RFC 1597.

The dynamic IP address acquisition on the WAN interface of the Netopia R9100 is one of several features of NAT. Another is the mapping of locally assigned IP addresses to the single globally unique IP address acquired by the Netopia R9100 on its WAN interface. NAT employs several things to accomplish this seamlessly. You must look at the formatting of an IP packet before IP address remapping can be explained.

Every IP packet that is transmitted across the Netopia R9100's LAN interface or across the WAN interface to the Internet contains several bits of information that indicate to any device where the packet is going and where it came from. In particular, you have the source and destination port and source and destination IP addresses.

A port is used within IP to define a particular type of service and could be either a Transmission Control Protocol (TCP) port or User Datagram Protocol (UDP) port. Both TCP and UDP are protocols that use IP as the underlying transport mechanism. The major difference between TCP and UDP is that TCP is a reliable delivery service, whereas UDP is a "best-effort" delivery service. A list of well-known TCP or UDP ports and services can be found in RFC 1700.

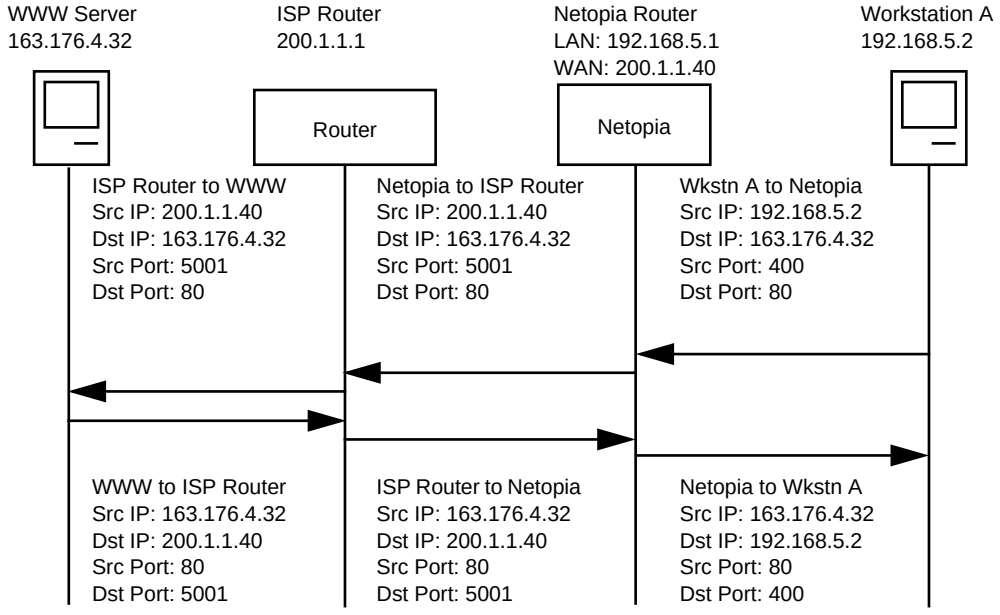
If Workstation A wants to communicate with a World Wide Web (WWW) server on the Internet and the Netopia R9100 does not have NAT enabled, Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32. The source port could be 400 while the destination port would be 80 (WWW server). The Netopia R9100 then looks at this IP packet, determines the best routing method and sends that packet on its way across the WAN interface to the WWW server on the Internet.

With NAT enabled, the Netopia R9100 does something different. For example, suppose that Workstation A again wants to communicate with the WWW server on the Internet. Workstation A forms an IP packet with the source IP address of 192.168.5.2 and destination IP address of 163.176.4.32, and source port could be 400 while the destination port would be 80 (WWW server).

When the Netopia R9100 receives this IP packet, it cannot simply forward it to the WAN interface and the Internet since the IP addresses on the LAN interface are not valid or globally unique for the Internet. Instead, the Netopia R9100 has to change the IP packet to reflect the IP address that was acquired on the WAN interface from the ISP.

The Netopia R9100 will first substitute the source IP address with the IP address that was acquired on the WAN interface, which in this case is 200.1.1.40. Next the Netopia R9100 will substitute the source TCP or UDP port with a TCP or UDP port from within a specified range maintained within the Netopia R9100. And finally the modified IP packet's checksum is recalculated (as specified in RFC 1631) and the packet is transmitted across the WAN interface to its destination, the WWW server on the Internet.

If the send and response IP packets were drawn out, this process would look like the following:

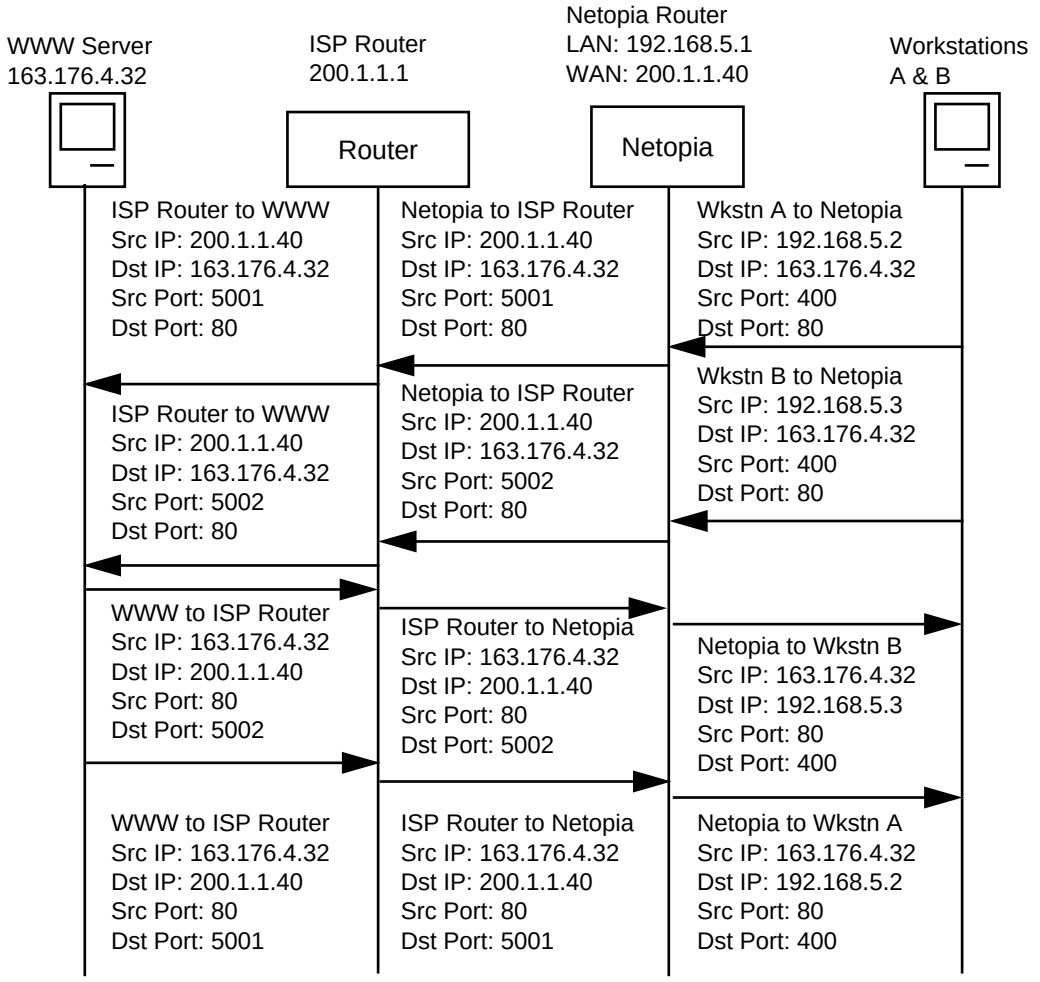


As you can see, the IP packet from Workstation A is sent to the Netopia R9100 and the source IP address is substituted with 200.1.1.40 and the source port is substituted with 5001, then the IP packet checksum is recalculated. When this modified packet reaches the WWW server on the Internet, the WWW server responds and sends the IP packet back to destination IP address 200.1.1.40 and destination port 5001.

When the Netopia R9100 receives this IP packet from the WWW server, the Netopia R9100 replaces the destination IP address with 192.168.5.2, the address for Workstation A. The port is changed back to 400, the IP packet checksum is recalculated, and the IP packet is sent to Workstation A on the Netopia R9100s LAN interface.

The reasons for the IP address changes are obvious from the preceding diagram, but what is not so obvious is why the TCP or UDP source ports need to be changed as well. These are changed and maintained in an internal table so the Netopia R9100 can determine which host on the local LAN interface sent the IP packet and what host the response from the WAN interface is going to go to on the LAN interface. This becomes especially important when two or more hosts on the LAN interface are accessing the same type of service on the Internet, like a WWW server (port 80), for example.

Now look at how two hosts on the LAN interface accessing the same WWW server on the Internet will work:



As you can see, when Workstation A and Workstation B transmit an IP packet to the WWW server on the Internet, they have unique source IP addresses on the LAN interface but potentially the same source ports, which in this case is 400. When the Netopia R9100 receives these packets, the source IP addresses are substituted with the single globally unique IP address that was acquired on the WAN interface, which is 200.1.1.40.

Now both IP packets have the exact same source IP address (200.1.1.40) and source ports (400). The Netopia R9100 is then able to distinguish between the two IP packets by changing the source TCP or UDP ports and keeping this information in an internal table. As seen above, the source port for Workstation A has been changed to 5001 and the source port for Workstation B has been changed to 5002.

If you were to look at the internal port mapping table that is maintained by the Netopia R9100, it would look similar to the following:

Source LAN IP	Source LAN Port	Remapped LAN Port
192.168.5.2	TCP 400	TCP 5001
192.168.5.3	TCP 400	TCP 5002

With this information the Netopia R9100 can determine the appropriate routing for an IP response from the Internet. In this case, when the WWW server responds with a destination port of 5001, the Netopia R9100 can see that this packet's destination on the local LAN interface is actually Workstation A at IP address 192.168.5.2. Likewise, with the response for port 5002, the Netopia R9100 can see that this packet's destination on the local LAN interface is actually Workstation B at IP address 192.168.5.3.

Exported services

Note that this “automatic” port remapping and IP address substitution only works in one direction – for IP packets that originated on the LAN interface destined to the WAN interface and the Internet. In order for port remapping and IP address substitution to work in the other direction – that is, hosts on the Internet that want to originate an IP packet destined to a host on the Netopia R9100s LAN interface – a manual redirection of TCP or UDP ports as well as destination IP addresses within the Netopia R9100 is required. This manual port remapping and IP address substitution is accomplished by setting up exported services.

Exported services are essentially user-defined pointers for a particular type of incoming TCP or UDP service from the WAN interface to a host on the local LAN interface. This is necessary since the Netopia R9100 and thus the attached local LAN has only one IP presence on the WAN interface and Internet. Exported services allows the user to redirect one type of service – for example Port 21 (FTP) – to a single host on the local LAN interface. This will then allow the Netopia R9100 to redirect any packets coming in from the Internet with the defined destination TCP or UDP port of port 21 (FTP) to be redirected to a host on the local LAN interface.

For example, suppose the WWW server on the Internet with the IP address of 163.176.4.32 wants to access Workstation B on the Netopia R9100s local LAN interface which is operating as an FTP server. The IP address for Workstation B is 192.168.5.3, which is not a valid IP address, and thus the WWW server on the Internet cannot use this IP address to access Workstation B.

The WWW server on the Internet would then have to use the single valid IP address that was acquired on the Netopia R9100's WAN interface to access any host on the Netopia R9100's local LAN interface, since this is the only valid address for the Internet. But if the WWW server on the Internet opens a connection to 200.1.1.40 via port 21 (FTP) and no exported services are defined on the Netopia R9100, the Netopia R9100 will discard the incoming packet since the Netopia R9100 itself does not perform the requested service.

You can see why exported services are necessary. In the example above, an Exported Service needs to be defined within the Netopia R9100 redirecting any incoming IP traffic with a destination port of 21 to the host on the local LAN interface with the IP address of 192.168.5.3.

If the WWW server on the Internet then tries to open a connection to the IP address of 200.1.1.40 with the appropriate Exported Service defined, the Netopia R9100 will look at the destination port and will find that it is destined for port 21 (FTP). The Netopia R9100 then looks at the internal user-defined exported services table and finds that any incoming IP traffic from the WAN port with a destination of port 21 (FTP) should be redirected to the IP address of 192.168.5.3 on the local LAN interface, which in this case is Workstation B.

Once the appropriate exported services are defined, there can be seamless communication between a host on the Internet and a host on the Netopia R9100's local LAN interface.

Important notes

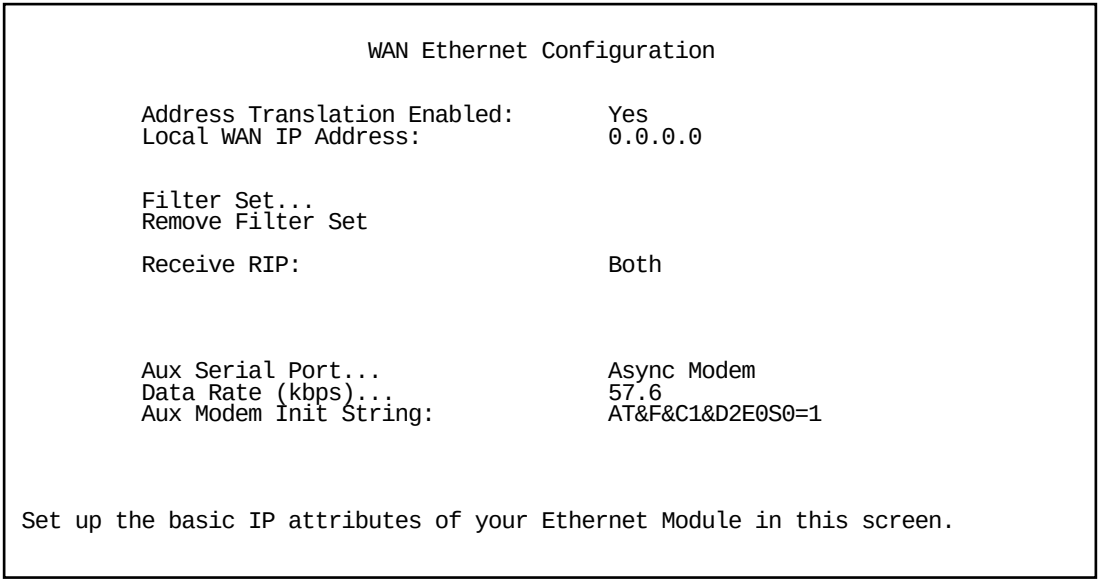
Even with the advantages of NAT, there are several things you should note carefully:

- There is no formally agreed-upon method among router vendors for handling an all-zeros IPCP request. The majority of router vendors use the all-zeros IPCP request to determine when a dial-in host wants to be assigned an IP address. Some vendors however attempt to negotiate and establish routing with an all-zeros IP address. The Netopia R9100 will not allow routing to be established with an all-zeros IP address and the call will be dropped with an error logged in the Device Event History.
- When using NAT it is most likely that the Netopia R9100 will be receiving an IP address from a "pool" of dynamic IP addresses at the ISP. This means that the Netopia R9100's IP presence on the Internet will change with each connection. This can potentially cause problems with devices on the Internet attempting to access services like WWW and FTP servers or AURP partners on the Netopia R9100's local LAN interface. In this case, if a dynamic IP address is assigned to the WAN interface of the Netopia R9100 each time, the administrator of the Netopia R9100 will have to notify clients who want to access services on the Netopia R9100's LAN interface of the new IP address after each connection.
- With NAT enabled, there cannot be two or more of the same types of service accessible from the Internet on the LAN interface of the Netopia R9100. For example, there cannot be multiple FTP servers (Port 23) on the Netopia R9100's LAN interface that can be accessible by workstations on the Internet. This is because there is no way within the Netopia R9100 and IP to distinguish between multiple servers using the same port, in this case port 23.
- Fictional IP addresses may be assigned on the Netopia R9100's LAN interface. It is strongly recommended that for the Netopia R9100's LAN interface, an IP address from the Class C address range of 192.168.X.X be used. This is because this range is defined by the IANA as an address space that will never be routed through the Internet and is to be used by private Intranets not attached to the Internet.

  If the address range of 192.168.X.X is not used and another range of addresses such as 100.1.1.X is used instead, this address space can potentially overlap an address space that is owned by a user attached to the Internet. Thus if a user on the Netopia R9100's LAN interface has an IP address of 100.1.1.2 while the Netopia R9100's LAN interface is 100.1.1.2 and the local host wants to access a host on the Internet with the address of 100.1.1.8, the Netopia R9100 has no way of knowing that the 200.1.1.8 address is actually on the Internet and not on its local LAN interface, since the local LAN interface is assigned the IP address range of 200.1.1.1 to 200.1.1.14.

Configuration

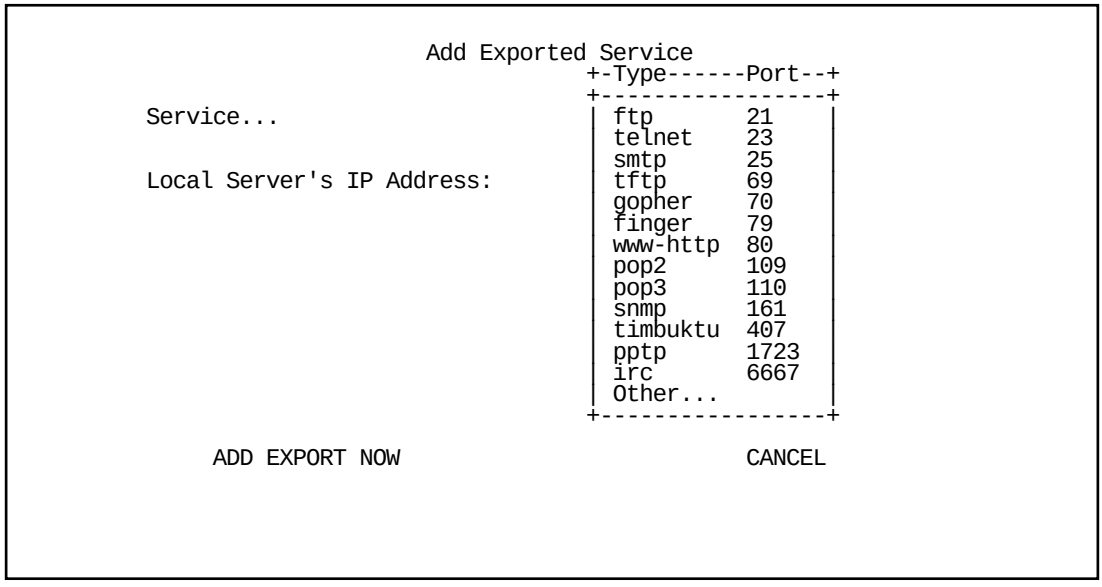
Network Address Translation is enabled by default with the SmartStart configuration utility. You can toggle **Address Translation Enabled** to No or Yes in the WAN Ethernet Configuration screen in WAN Configuration under the Main Menu. An example of enabling NAT is as follows:



Toggling Address Translation Enabled to Yes enables the Netopia R9100 to send out an all-zeros IPCP address that requests an IP to be assigned to the Netopia R9100's WAN interface. Note that the remote IP address is 127.0.0.2, which should also be the default gateway under IP Setup in System Configuration. This is done for profile matching purposes and because the IP address of the router the Netopia R9100 is dialing is not always known.

As mentioned earlier in this appendix, NAT works well for IP sessions originated on the Netopia R9100's LAN interface destined for the Internet without any additional configuration. For incoming IP connections from the Internet to a host on the Netopia R9100's LAN interface, exported services need to be used.

Exported services are configured under IP Setup in System Configuration. This is where a particular type of TCP or UDP service originating from the Internet is redirected to a host on the Netopia R9100's LAN interface. An example of this screen follows:



Within exported services is a pop-up list of well-known TCP and UDP services that can be redirected to a single host on the Netopia R9100's LAN interface. There is also an "Other..." option that allows for manual configuration of additional TCP or UDP ports. There can be a total of 32 exported services that can be defined.

When a particular type of service is redirected to an IP address, that service is removed from the pop-up list, since only one type of service can be redirected to a single host. However several different types of services can be redirected to a single or multiple hosts. For example, port 80 (WWW server) could be redirected to 192.168.5.3 on the Netopia R9100's LAN interface, and port 23 (Telnet) can be redirected to that same host.

Summary

NAT is a powerful feature of the Netopia R9100 and when used and set up properly can yield a secure network while only using one IP address on the WAN interface. Note that the addresses listed in this appendix are for demonstration purposes only. Do not use these addresses when configuring your local network.

Appendix D

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.

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
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

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
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 E

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.

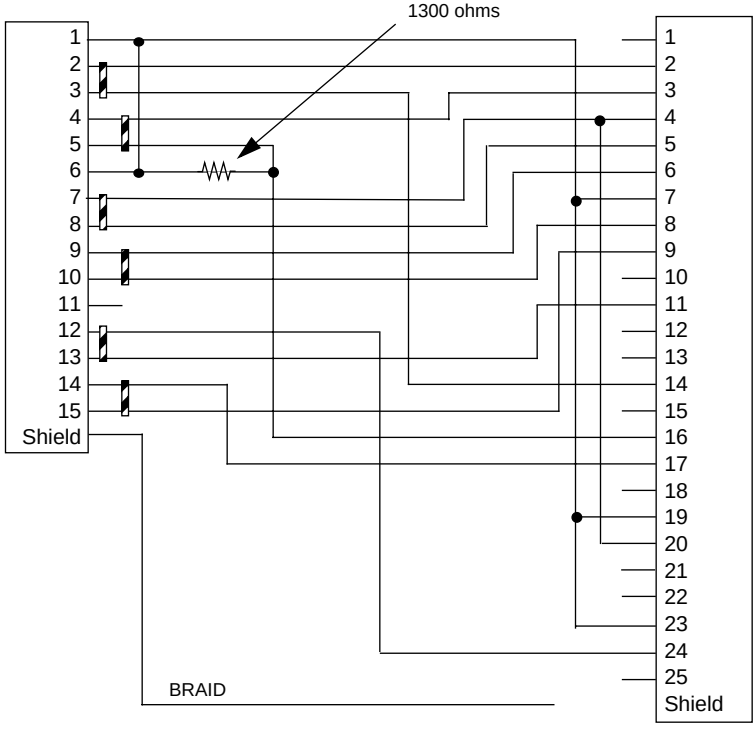
Tsuchiya, P. "Components of OSI: Routing (An Overview)." *ConneXions: The Interoperability Report*, Vol. 3, No. 8: August 1989.

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 F

Technical Specifications and Safety Information

Pinouts for Auxiliary port modem cable



HD-15		DB-25	
Pin 1	Ground	Pin 1	(not used)
Pin 2	TDA	Pin 2	TD
Pin 3	TDB	Pin 3	RD
Pin 4	RDA	Pin 4	RTS
Pin 5	RDB	Pin 5	CTS
Pin 6	(not used)	Pin 6	DCE Ready
Pin 7	DTR	Pin 7	Ground
Pin 8	CTS	Pin 8	RLSD

HD-15		DB-25	
Pin 9	DSR	Pin 9	-RSET (EIA-530)
Pin 10	DCD	Pin 10	(not used)
Pin 11	(not used)	Pin 11	-TSET (EIA-530)
Pin 12	TCA	Pin 12	(not used)
Pin 13	TCB	Pin 13	(not used)
Pin 14	RCA	Pin 14	-TD (EIA-530) STD (EIA-232)
Pin 15	RCB	Pin 15	(not used)
		Pin 16	-RD (EIA-530) SRD (EIA-232)
		Pin 17	RSET
		Pin 18	(not used)
		Pin 19	-RTS (EIA-530) SRTS (EIA-232)
		Pin 20	DTE Ready
		Pin 21	(not used)
		Pin 22	(not used)
		Pin 23	Ground
		Pin 24	TSET
		Pin 25	(not used)
Note: Certain RS-232 modems do not properly accept signals on pins 12/24, 13/11, 14/17, and 15/9. For these applications, these pins may need to be cut.			

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 R9100 Ethernet Router has an RJ-45 jack for Ethernet line 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: Ethernet

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 R9100 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 R9100 Ethernet Router has met the safety standards (per CSA-950) of the Canadian Standards Association for Canada.

The Netopia R9100 Ethernet Router 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 R9100'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. For more information on IP network address classes, see Appendix B, "Understanding IP Addressing."

client: An intelligent workstation that makes requests to other computers known as servers. PC computers on a LAN can be clients.

clustering: A feature that clusters remapped network numbers into a range of sequential network numbers.

CNA (Calling Number Authentication): A security feature that will reject an incoming call if it does not match the Calling Number field in one of the Netopia ISDN Router's connection profiles.

CND (Calling Number Delivery): Also known as caller ID, a feature that allows the called customer premises equipment (CPE) to receive a calling party's directory number during the call establishment phase.

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.

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).

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 R9100 Ethernet Router (the "Product") will be free from defects in materials and workmanship under normal use for a period of one (1) year from date of purchase. 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 MERCHANTABILITY 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. v.0300