Cyclades-PR4000
Installation Manual

Mid-range, Multi-protocol, Expandable Remote Access Server

Cyclades Corporation

Cyclades-PR4000 Installation Manual
Version 2.2 – May 2002
Copyright (C) Cyclades Corporation, 1998 - 2002

We believe the information in this manual is accurate and reliable. However, we assume no responsibility, financial or otherwise, for any consequences of the use of this Installation Manual.

This manual is published by Cyclades Corporation, which reserves the right to make improvements or changes in the products described in this manual as well as to revise this publication at any time and without notice to any person of such revision or change. The menu options described in this manual correspond to version 1.8.x of the CyROS operating system. This manual is printed horizontally in order to match the electronic (PDF) format of the Installation Manual, page per page.

All brand and product names mentioned in this publication are trademarks or registered trademarks of their respective holders.

FCC Warning Statement:
The Cyclades-PR4000 has been tested and found to comply with the limits for Class A digital devices, 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 Installation 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 is required to correct the problem at his or her own expense.

Canadian DOC Notice:
The Cyclades-PR4000 does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le Cyclades-**PR4000** n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectrique edicté par le Ministère des Communications du Canada.

Table of Contents

Cyclades-PR4000

CHAPTER 1 HOW TO USE THIS MANUAL

Three Cyclades manuals are related to the PR4000.

1 The Quick Installation Manual -- provided with the router,
2 The Installation Manual -- available electronically on the Cyclades web site,
3 The CyROS Reference Guide -- also available electronically on the Cyclades web site.

CyROS stands for the Cyclades Routing Operating System. It is the operating system for all Cyclades Power Routers (PR1000, PR2000, PR3000, and PR4000). The CyROS Reference Guide contains complete information about the features and configuration of all products in the PR line.

CyROS is constantly evolving, and the menus in this manual might be slightly different from the menus in the router. The latest version of all three manuals (and the latest version of CyROS) can be downloaded from Cyclades' web site. All manuals indicate on the second page the manual version and the corresponding version of CyROS.

The first three chapters of this manual should be read in the order written, with exceptions given in the text. The most appropriate example in Chapter 4 should then be read, with chapters 5 through 14 providing complementary information.

Chapter 2 - What is in the Box **-** explains how the router should be connected.

Chapter 3 -Using Menus **-** describes CyROS menu navigation.

Chapter 4 -Step-by-Step Instructions for Common Applications - guide to configuration with detailed examples.

Chapters 5 to 11- Basic router configuration information for applications that do not fit any of the examples in chapter 4.

Chapter 12 - CyROS - shows how to set router specific parameters and create lists of hosts and users.

Chapter 13 - Network Address Translation - describes CyROS' NAT implementation.

Chapter 14- Filters and Rules - demonstrates how to protect your router from undesired traffic.

Chapter 15 - IPX - presents the hidden menus available only in routers with IPX activated.

Chapter 16 - Virtual Private Network - describes CyROS' VPN implementation.

Appendix A - Troubleshooting - provides solutions and tests for typical problems.

Appendix B - Hardware Specifications.

Appendix C - Configuration Without a Console.

Appendix D - Modem Installation and Configuration

Installation Assumptions

This Installation Manual assumes that the reader understands networking basics and is familiar with the terms and concepts used in Local Area and Wide Area Networking.

Text Conventions

Common text conventions are used. A summary is presented below:

Convention	Description
CONFIG=>INTERFACE=>L	A combination of menu items, with the last being either a menu item, a parameter, or a command. In this example, L lists the interface configuration.
<INTERFACE>	A variable menu item that depends on hardware options or a choice of hardware or software options.
IP Address	A parameter or menu item referenced in text, without path prepended.
`Screen Text`	Screen Text
<ESC>, <Enter>	Simbols representing special keyboard keys.

Icons

Icons are used to draw attention to important text.

Icon	Meaning	Why
	What is Wrong?	When an error is common, text with this icon will mention the symptoms and how to resolve the problem.
	Where Can I Find More Information?	CyROS contains many features, and sometimes related material must be broken up into digestible pieces. Text with this icon will indicate the relevant section.
	Caution!	Not following instructions can result in damage to the hardware. Text with this icon will warn when damage is possible.
	Reminder.	Certain instructions must be followed in order. Text with this icon will explain the proper steps.

Cyclades Technical Support and Contact Information

All Cyclades products include limited free technical support, software upgrades and manual updates.

These updates and the latest product information are available at:

http://www.cyclades.com
ftp://ftp.cyclades.com/pub/cyclades

> ✓ Before contacting us for technical support on a configuration problem, please collect the information listed below.

- The Cyclades product name and model.
- Applicable hardware and software options and versions.
- Information about the environment (network, carrier, etc).
- The product configuration. Print out a copy of the listing obtained by selecting INFO=>SHOW CONFIGURATION=>ALL.
- A detailed description of the problem.
- The exact error or log messages printed by the router or by any other system.
- The Installation Guide for your product.
- Contact information in case we need to contact you at a later time.

In the United States and Canada, contact technical support by phone or e-mail:

Phone: (510) 770-9727 (9:00AM to 5:00PM PST)
Fax: (510) 770-0355
E-mail: support@cyclades.com

Outside North America, please contact us through e-mail or contact your local Cyclades distributor or representative.

The mailing address and general phone numbers for Cyclades Corporation are:

Cyclades Corporation

Phone: + 01 (510) 770-9727
Fax: + 01 (510) 770-0355

41829 Albrae Street
Fremont, CA 94538
USA

CHAPTER 2 WHAT IS IN THE BOX

The following are included with the PR4000:

- PR4000 Main Unit
- Power Cord
- Console Cable

- Quick Installation Manual and Documentation CD
- Mounting Kit with Handles
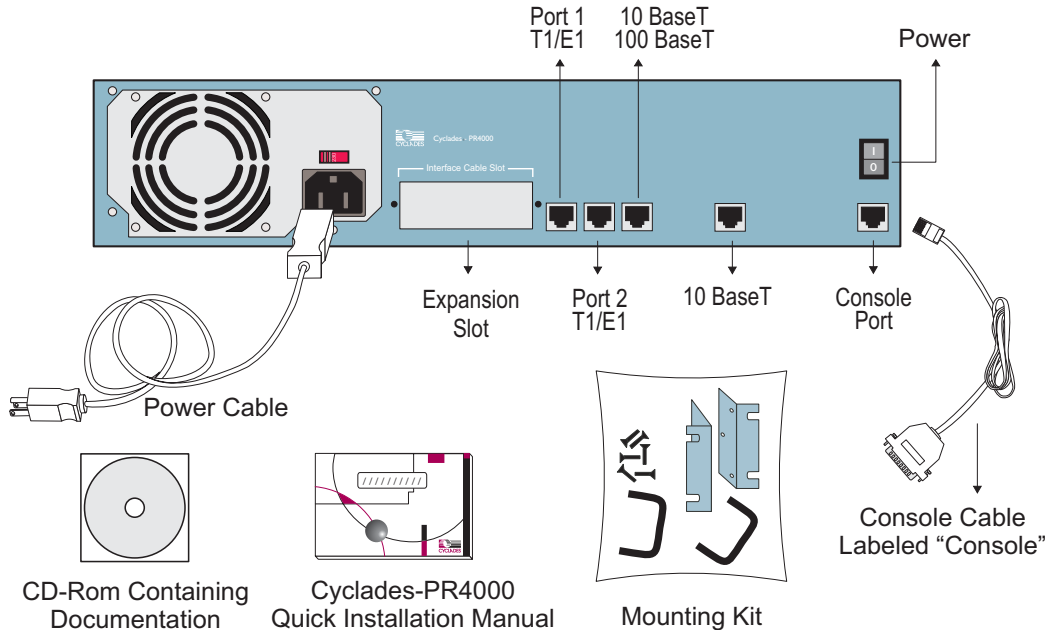
FIGURE 2.1 ITEMS INCLUDED WITH ALL PR4000 MODELS

SWAN Expansion Card

The PR4000 is often sold with a SWAN card in the expansion slot. The SWAN can be connected to a modem or DSU/CSU as shown in Figure 2.3. Cables are not included with the product.

Back Panel of PR4000

Slot with
SWAN RSV Card

or

DB-25
Male

DB-25
Male

Straight Cable

V.35 Cable Set

DB-25 Male

DB-25
Male

DB-25 Female/ M.34
Male Converter

RS-232 Modem
with DB-25
Interface

V.35 DSU/CSU
with M.34
Interface
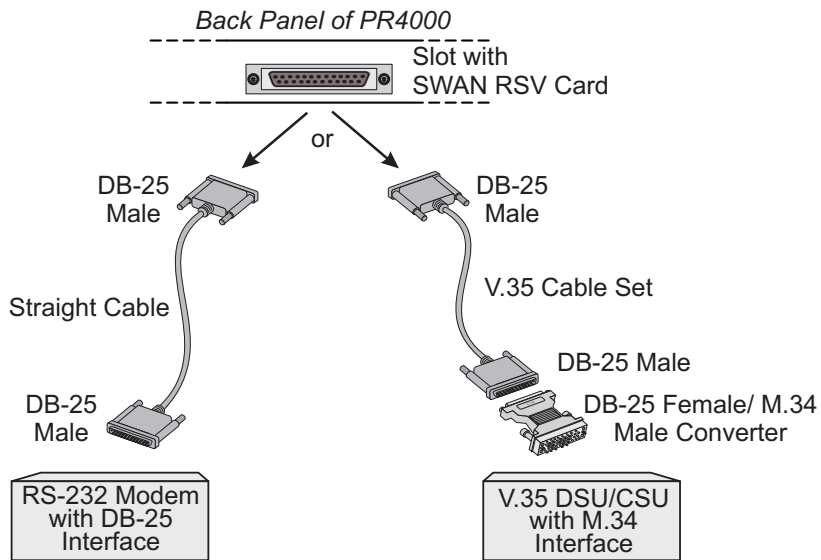
FIGURE 2.3 SWAN EXPANSION CARD SHOWING CABLE CONNECTIONS

Provisioning the T1/E1 Dialup Lines

This section provides information useful when provisioning the T1 or E1 dialup trunk lines for use with the Cyclades-PR4000 Remote Access Server. Line provisioning parameters vary widely depending on the switch being used at the central office and the service options offered by the carrier. In North America and Japan, a digital trunk uses a T1 speed of 1.5Mbps. In Europe and most other countries, a digital trunk runs at E1 speeds of 2Mbps. A digital trunk is a Time Division Multiplexed (TDM) line that carries information from several channels in digital form. In a given country, only E1 or T1 is offered.

Signaling: ISDN-PRI (CCS) or CAS

Phone lines carry signaling information used to establish and maintain connections. In a regular phone this information translates into dialing, ring, busy signal, dial tone, caller ID, etc. In an analog phone line, the signaling information shares the channel used to carry voice. In a T1 or E1 trunk, the signaling information for the trunk can be carried by a separate channel or can share the same channel used to carry data. There are three basic signaling protocols: ISDN-PRI (T1 or E1), CAS-BR (T1), or R2D/MFR2 (E1).

Newer systems use the ISDN-PRI signaling protocol, with channels dedicated to control. With this protocol, a T1 line carries 23 phone connections and an E1 line carries 30 phone connections.

In North America, older T1 systems use CAS (Channel Associated Signaling) protocols. These protocols "steal" some of the bandwidth from the data channels using a scheme called "bit robbing" (BR) and allow a T1 line to carry 24 phone connections. In other countries, older E1 systems use R2D/MFR2 signaling with a dedicated channel, leaving 30 phone connections. Lines with CAS or R2D/MFR2 signaling are sometimes referred as "Channelized T1/E1" or "DS-1".

ISDN-PRI provides more control over connections than the older CAS or R2Ds. Given a choice between ISDN-PRI and CAS/R2D, select ISDN-PRI.

Number of Phone Lines

In most applications, the maximum number of phone lines (for the protocol used) are purchased. However, it is also possible to request fewer lines. When using fewer lines, make sure to disable the remaining channels using the menu CONFIG =>INTERFACE =>E1/T1 =><CHANNEL> =>ENCAPSULATION =>INACTIVATE.

ISDN Switch Type (ISDN-PRI only)

Different switch vendors have different signaling protocol implementations. If you are in the US and are given a choice of ISDN switch types, select National ISDN 2, which is intended to be the US standard switch type. Other common and acceptable options are Custom AT&T 5ESS and Northern Telecom DMS-100. In Europe, Euro ISDN (ETSI) is the standard ISDN switch type, but there are still some variations in use. Examples are TR6 in Germany and VN6 in France. Australia, Japan and Korea each have their own standard switch type. Other countries usually adopt the European standards.

Data/Voice Support

From the phone system standpoint, analog modem connections (V.34, V.90, K56 flex) are "voice" while "data" refers to digital connections using ISDN-BRI or V.110. Lines with CAS signaling support only voice calls. Most ISDN-PRI lines support both data and voice channels, but some lines are configured to support only voice or only data. If given a choice, both voice and data support is preferable. If only one may be chosen, voice should be chosen to support modem (V.34, V.90) clients and data should be chosen to support clients using ISDN-BRI or V.110. The Cyclades-PR4000 supports both digital and analog calls and can terminate both at the same time in the same trunk.

Phone Numbers, Hunting Groups, and Hunting Sequence

Each T1/E1 channel can have a different phone number or be organized into hunting groups with the same phone number. In the second case, the client gets the first available line within the hunting group. The line allocation can be done in a linear (the first available line gets a new call, from the first line to the last or vice-versa) or round-robin fashion. ISPs usually group all lines into one hunting group so that all customers call the same phone number. Breaking the trunk into more than one hunting group can be used to reserve a certain number of lines for different classes of customers.

One-Way or Two-Way Service

A line can only receive calls (dial-in) or receive and generate calls (dial-out). An ISP usually only needs to receive calls and one-way service is the recommended configuration unless you plan to support services that require dial-out (fax servers, call back, etc.).

Signaling Method and Dialing Method (T1 CAS-BR only)

T1 with CAS signaling may require additional parameters. For Signaling Method, the selection may be MFR1, DTMF or no signaling. For Dialing Method, the selection may be wink-start or loop-start. The suggested choice is wink-start.

Line Coding

This refers to the way the digital data is encoded in the line. For T1 lines, the options are usually Bipolar with 8 Zeroes Substitution (B8ZS) or Alternate Mark Inversion (AMI). B8ZS is better suited to digital transmissions, so it should be the choice if available. For E1 lines, the options are usually High Density Bipolar of Order 3 (HDB3) and Alternate Mark Inversion (AMI). HDB3 is the more modern of the two and better suited to digital transmissions.

Framing

This refers to how the data bits are framed in the TDM bus. For T1 lines, the possibilities are D4 Super Frame (D4) or Extended Super Frame (ESF). ESF provides error checking and should be the choice if available. For E1 lines, the choices are usually Frame Alignment Signal with or without CRC4 (4-bit Cyclic Redundancy Check). If given a choice, select a line with CRC4, which will provide error checking.

Termination at the Customer Premises

The Cyclades-PR4000 supports T1 on a standard 100-Ohm RJ-48C connector and E1 on a standard 120-Ohm RJ-48C connector. In some countries, especially those using E1 lines, the termination may be provided on a Coax G703 connector (75 Ohms). An external interface converter (balum) is necessary in this case.

Chapter 3 Using CyROS Menus

This chapter explains CyROS menu navigation and special keys. There are four ways to interact with CyROS:

- Traditional menu interface using a console or Telnet session,
- CyROS Management Utility based on interactive HTML pages,
- Front-panel display,
- SNMP (explained in the CyROS Reference Manual).

Connection Using the Console Cable and a Computer or Terminal

The first step is to connect a computer or terminal to the router using the console cable. If using a computer, HyperTerminal can be used in the Windows operating system or kermit in the Unix operating system. The terminal parameters should be set as follows:

- Serial Speed: 9600 bps
- Data Length: 8 bits
- Parity: None
- Stop Bits: 1 stop bit
- Flow Control: Hardware flow control *or* none

Once the console connection is correctly established, a Cyclades banner and login prompt should appear on the terminal screen. If nothing appears, see the first section of the troubleshooting appendix for help. The second step is to log in. The preset super-user user ID is "super" and the corresponding preset password is "surt". The password should be changed as soon as possible, as described in chapter 13 of the installation manual and at the end of every example in chapter 4. The login prompt and main menu are shown in Figure 3.1.

Cyclades-PR4000

```
[PR4000] login : super
[PR4000] Password : ****


Cyclades Router (Router Name) – Main Menu

1 – Config       2 – Applications   3 – Logout
4 – Debug        5 – Info           6 – Admin

Select Option ==>
```

FIGURE 3.1 LOGIN PROMPT AND MAIN MENU

All menus have the following elements:

- Title – In the example in Figure 3.1: "Main Menu".
- Prompt – The text: "Select Option ==>" (this text can be changed by the super user.)
- Options –The menu options, which are selected by number.
- Router Name – The default is the name of the product. Each router can be renamed by the super user for easier identification.

Menus can also be navigated using a short-cut method. This method must be activated first by choosing a shortcut chraacter ("+" in the example that follows) in the CONFIG =>SYSTEM =>ROUTER DESCRIPTION menu. Typing 4+1+1 at the main-menu prompt, for example, is equivalent to choosing option 4 in the main menu (Debug), then choosing option 1 in the debug menu (Trace), then choosing option 1 in the trace menu (Driver Trace). In addition to menus, some screens have questions with letter choices. In the line below, several elements may be identified:

```
lmi-type((A)NSI, (G)roup of four, (N)one )[A]:
```

- Parameter description – The name of the parameter to be configured, in this case "lmi-type".
- Options – Legal choices. The letter in parentheses is the letter that selects the corresponding option.
- Current value – The option in square brackets is the current value.

Pressing <Enter> without typing a new value leaves the item unchanged.

Special Keys

<Enter> or <Ctrl+M>	These keys are used to end the input of a value.
<ESC> or <Ctrl+I>	These keys are used to cancel a selection or return to the previous menu. In some isolated cases, this key jumps to the next menu in a series of menus at the same level.
<Backspace> or <Ctrl+H>	These keys have the expected effect of erasing previously typed characters.
L	When available, this option displays the current configuration. For example, in the Ethernet Interface Menu, "L" displays the Ethernet configuration.
<Ctrl+L>	This key combination works like a toggle switch to allow display of one page of information at a time or display the entire configuration without page breaks.
<Ctrl+C>	This key combination disables any traces activated in the Debug Menu.

On leaving a menu where a change in configuration was made, CyROS will ask whether or not the change is to be saved:

```
    (D)iscard, save to (F)lash, or save to (R)un configuration:
```

Selecting *Discard* will eliminate all changes made since the last time the question was asked. Saving to *Flash* memory makes all changes permanent. The changes are immediately effective and are saved to the configuration vector in flash memory. In this case, the configuration is maintained even after a router reboot. Saving only to the *Run* configuration makes all changes effective immediately, but nothing is saved permanently until explicitly saved to flash (which can be done with the option ADMIN =>WRITE CONFIGURATION=>TO FLASH).

The menus and parameter lists are represented in this manual by tables. The first column contains the menu item or the parameter, and the second column contains its description.

This menu interface is also available via Telnet if one of the interfaces has been connected and configured. The

menu interface is the same as that described earlier in this section. Using Telnet instead of a console for the initial Ethernet configuration is discussed in Appendix C of the Installation Manual.

The CyROS Management Utility

After one of the interfaces has been connected and configured, there is another way to interact with CyROS. Type the IP address in the location field in an HTML browser of a PC connected locally or remotely through the configured interface. A super-user ID and password will be requested (these are the same ID and password used with the line-terminal interface). A clickable image of the router back panel will apear, as shown in Figure 3.2.
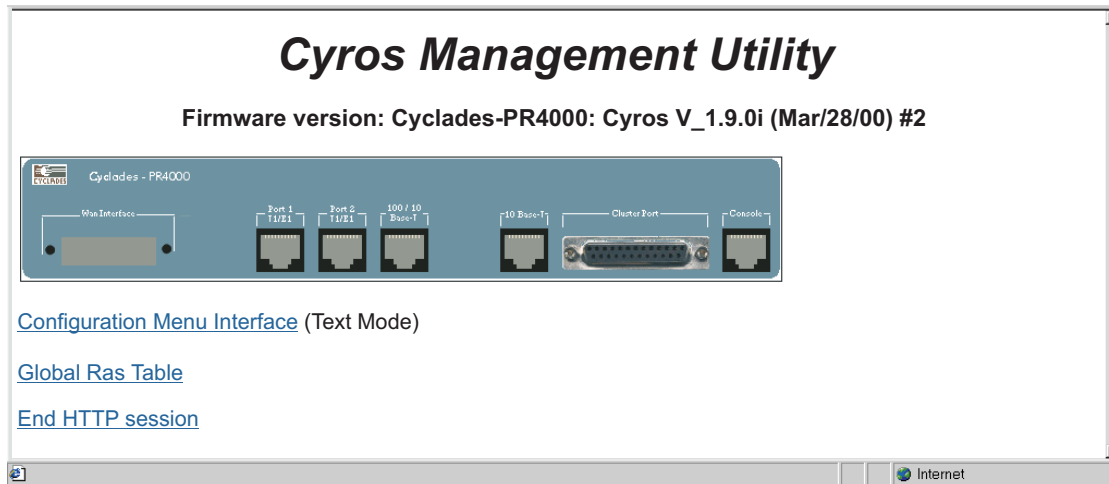
FIGURE 3.2 CYROS MANAGEMENT UTILITY HOME PAGE

The link *Configuration Menu Interface* will present an HTML version of the CyROS Main Menu, described previously. Clicking on an interface will show its current status and some additional information. The link *Global RAS Table* will show a table similar to that shown in Figure 3.3. Clicking on *End HTTP Session* will terminate the connection.

Cyclades-PR4000

CyROS Management Utility

	Global Remote Access Table Port Status					
Seq#	Slot #2 Port#1	User Name	Start Session Time	Elapsed Time	Connect String	Caller ID
1	Slot #2 Port#3	Arlt	Apr/18 18:11	0:04:46	Md=23 V34 28800 26400 LAPM/V42Bis	1115553000
2	Slot #2 Port#6	Marquez	Apr/18 18:05	0:10:46	Md=12 V90 28800 42666 LAPM/V42Bis	1115551268
3	Slot #2 Port#7	Neruda	Apr/18 18:31	0:05:09	Md=21 V34 28800 24000 LAPM/V42Bis	1115554811
4	Slot #2 Port#10	Cervantes	Apr/18 16:05	2:10:56	Md=13 V34 28800 16800 LAPM/V42Bis	1115550000
5	Slot #2 Port#11	Casares	Apr/18 18:08	0:07:47	Md=17 V90 24000 28000 LAPM/V42Bis	1115559743
6	Slot #2 Port#15	Allende	Apr/18 17:41	0:35:27	Md=19 V34 31200 33600 LAPM/V42Bis	1115557553
7	Slot #2 Port#17	Skarmeta	Apr/18 18:10	0:05:58	Md=20 V34 28800 31200 LAPM/V42Bis	1115551174
8	Slot #2 Port#	Rozenmacher	Apr/18 18:09	0:06:34	Md=18 V32 1440	1115559800

FIGURE 3.3 GLOBAL RAS TABLE

Cyclades-PR4000

Clicking on one of the links in the Global RAS Table will provide more detailed information about the connection and the user. An example is shown in Figure 3.4. The user can be disconnected with the hangup button and the interface can be temporarily disabled by clicking on the administrative down button.

```
                           Slot #2 Port #26 Status

Username: cas
Start Session Time: Apr/18/00 18:01:29
Elapsed Time: 0:11:01
Inactivity Timeout: None
Caller ID: 5554321
modem Id 9 V32B Initial Rate 14400/14400 Current Rate 14400/14400 LAPM/V42Bis

Number of transmitted Frames: 237670
Number of transmitted bytes: 106541777
Number of transmission errors: 2368
Number of received frames: 245235
Number of received bytes: 34399893
Number of reception errors: 96


PPP LCP state = OPENED
    PPP PAP state = OPENED
    PPP NCP (IPCP) state = OPENED Local IPaddr (200.200.200.200) Remote IPaddr (200.200.200.100)
```

Hangup Connection

Current Administrative Status is UP. Change it to **Admin. DOWN**

Go Back

Concluído   Internet

FIGURE 3.4 CHANNEL DETAILS

Returning to the CyROS Management Utility Home Page, clicking on a T1 or E1 port on the figure will display the channel details. There is a toggle button in the upper-right-hand corner which toggles between name and speed. When set to name, as shown in Figure 3.5, passing the mouse over a channel displays the username. When set to speed, it displays the carrier and speed of the connection. The ports are color-coded with the current status.
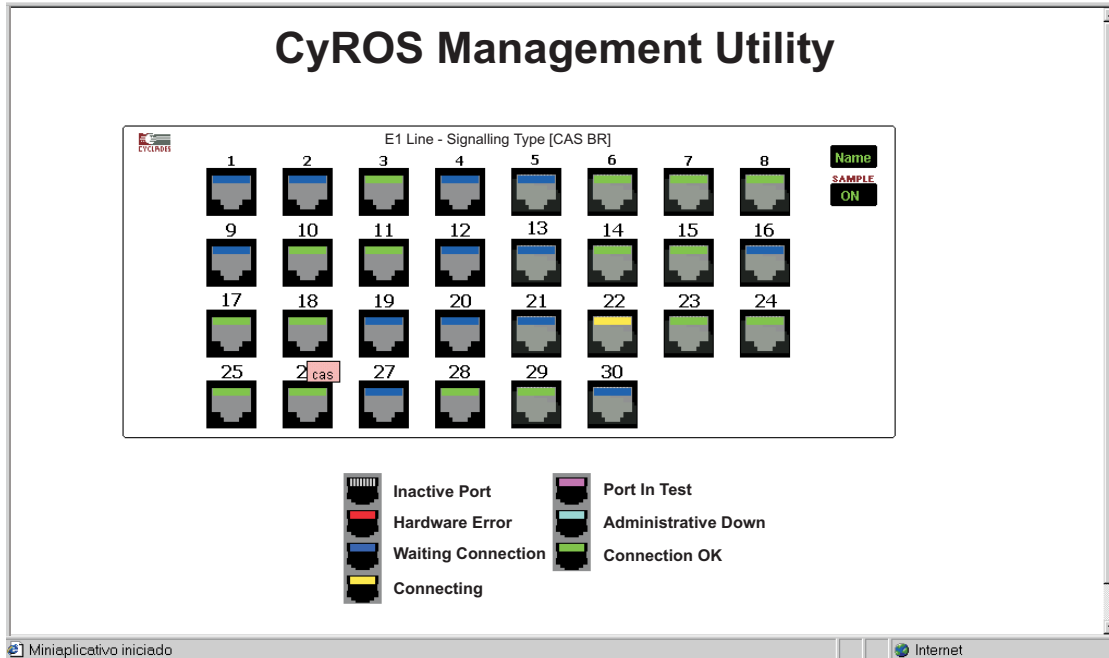
FIGURE 3.5 CHANNEL SUMMARY WITH TOGGLE SET TO NAME

Operating the Front-Panel Display

The Cyclades logo appears on the front-panel display (shown in Figure 3.6) after a sucessful boot.
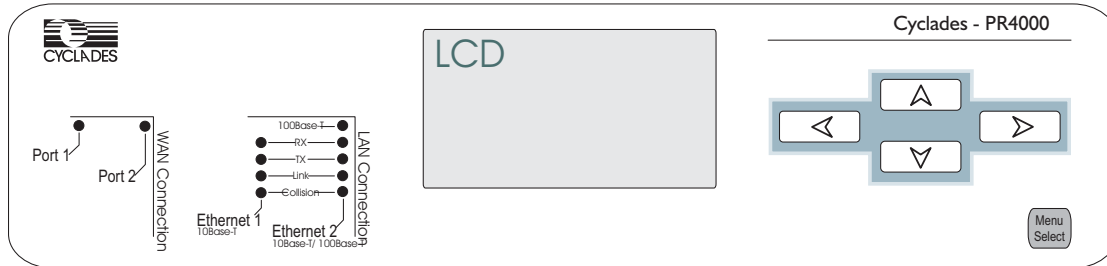
FIGURE 3.6 FRONT-PANEL DISPLAY

There are 5 push buttons: 4 arrows and one menu selection button. Pressing the menu selection button displays the main menu, which contains the following options:

- Modem Overview
- Interface Overview
- IP Traffic
- Syslog Messages
- System Info
- Reboot (If configured to appear using the menu item CONFIG =>SYSTEM =>HARDWARE)
- Quit

Modem Overview

The status of each connection can be displayed by modem or by interface.

Modem Order

This menu item presents a screen with one box for each modem. Each row corresponds to a Modem board. When 64 modems are present, the screen will appear as in Figure 3.7. The box on the upper left is the first modem, the upper right is the eight modem, and so forth for as many modems as are installed.
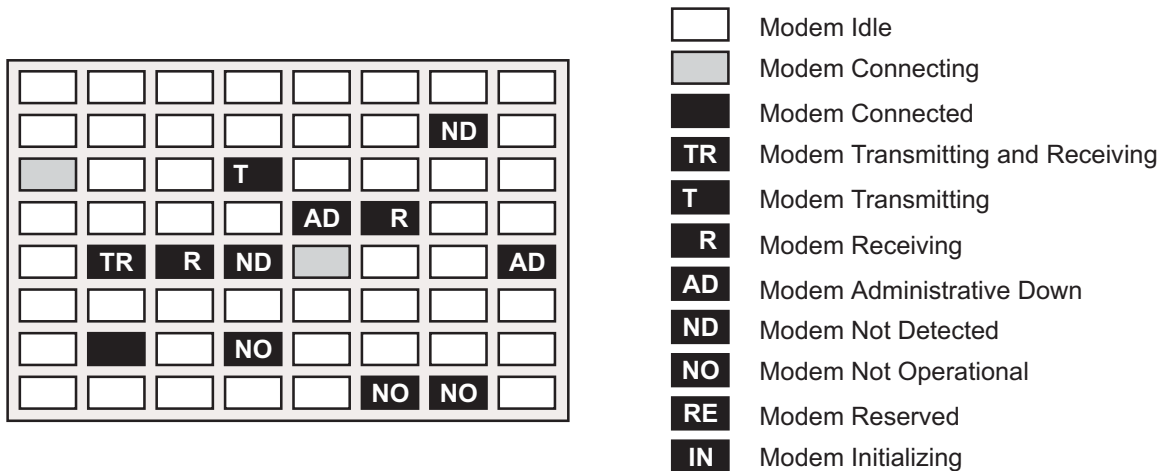
FIGURE 3.7 MODEM ORDER SCREEN

Slot/Link Order

This menu item presents a screen with one box per T1/E1 channel. Figure 3.8 shows two lines with 30 channels each. The box on the upper left is the first channel, the upper right is the eighth channel, and so forth for as many channels as are configured.
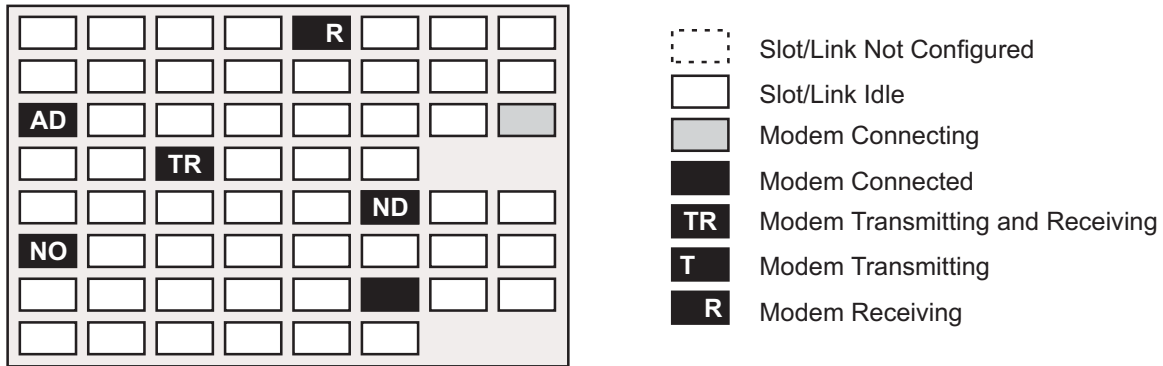
FIGURE 3.8 SLOT/LINK ORDER SCREEN

Interface Overview

This screen presents the status of each E1/T1 interface and indicates which modem has been allocated to each channel. The ordering of the channels is the same as for the previous screen
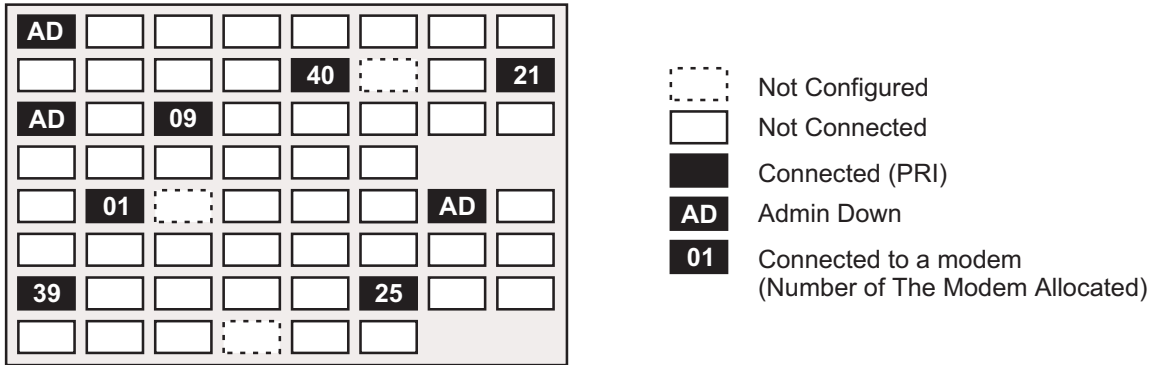
FIGURE 3.9 INTERFACE OVERVIEW SCREEN

IP Traffic

After choosing the interface desired, a bar graph showing bytes per second or packets per second is displayed. It is a snapshot of the last 10 minutes of IP traffic through the interface (TX for transmitted and RX for received), with a refresh every minute. The arrow keys toggle the display between bytes and packets per second. Pressing <menu select> returns to the main menu.

Syslog Messages

Selecting this menu item leads to another menu that allows changes in the display of syslog messages. Syslog messages are administrative and debug events. The following options are available:

- Display - Exibits the last syslog message generated by CyROS. Arrow keys may be used to see the syslog history.
- Stop - New syslog messages are discarded. The syslog history remains unchanged.
- Start - New syslog messages are stored in the syslog history and are displayed.
- Clear - Clears the syslog history.
- Quit - Returns to the main menu.

System Info

This menu item presents a sequence of four screens: Hardware Information, Board Information, Modem Information, and Boot Information. Any arrow key switches between screens. The menu select key returns to the main menu.

CHAPTER 4 STEP-BY-STEP INSTRUCTIONS FOR COMMON APPLICATIONS

This chapter provides detailed examples that can be used as models for similar applications. Turn to the example that is closest to your application, read the explanations, and fill in the blank spaces with parameters appropriate to your system. At the end of the section, you should have listed all the parameters needed to configure the router. At that point, read chapter 3 if you have not already, and configure your router with help from later chapters of the Installation Guide, when needed.

> ✓ Please read the entire example and follow the instructions before turning the router on. The router is programmed to log the super user off after 10 minutes of inactivity. All data not explicitly saved to memory is then lost. Collecting the data *while* configuring the router will likely cause delays and frustration.

Example 1 Using the PR4000 as a Remote Access Server

This example explains the configuration of an E1 or T1 line with signaling, the most common option when the PR4000 is used as a RAS. When the incoming call is made by a computer using a modem, the internal digital modems are used to convert analog signals to digital signals. Either CAS or CCS signaling can be used in this case. When the incoming call is made by an ISDN-BRI line subscriber (and the E1/T1 line is configured for CCS), the digital modems are bypassed.

This section will guide you through a complete RAS configuration. Figure 4.1 shows the example system used in this section. Spaces have been provided next to the parameters needed for the configuration so you can fill in the parameters for your system. Do this now before continuing.
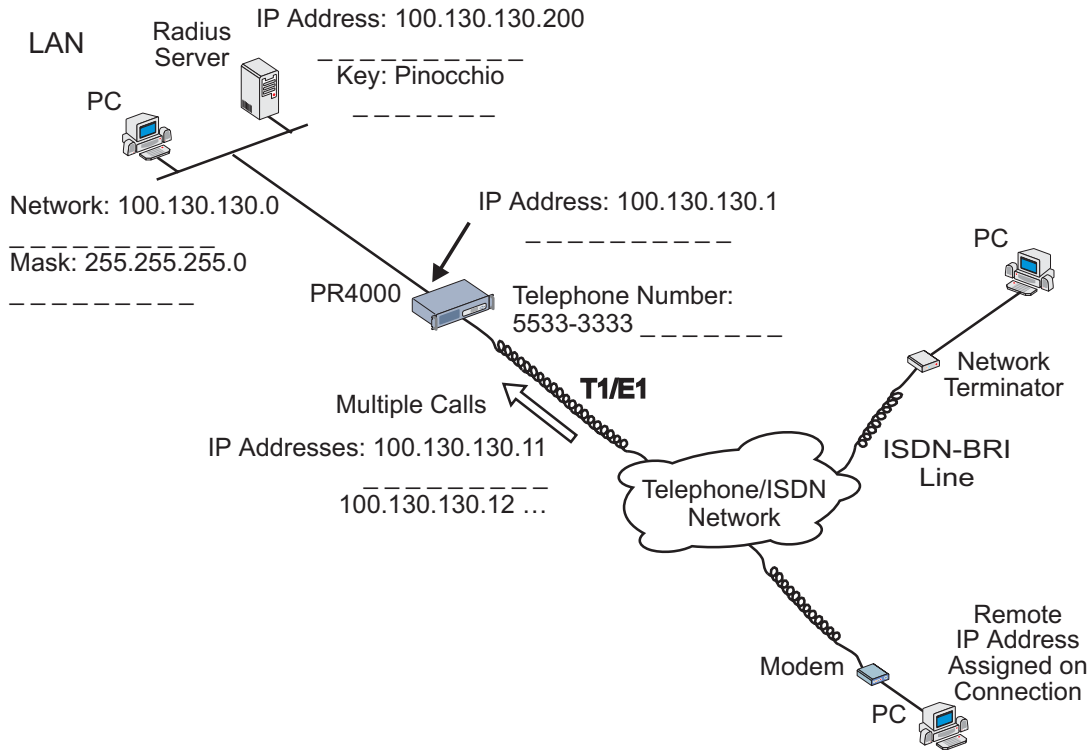
FIGURE 4.1 RAS EXAMPLE SHOWING DIAL-IN USERS

STEP ONE

The first step is to determine the parameters needed to configure the Fast Ethernet interface (ETH0). The parameters in the Network Protocol Menu (IP) are shown in Figure 4.2. Fill in the blanks for your application in the right-most column. These parameters will be entered into the PR4000 later, after all parameters have been determined. Each parameter in this menu is explained in more detail in chapter 5 of the Installation Guide.

Menu CONFIG=>INTERFACE=>FAST ETHERNET=>NETWORK PROTOCOL=>IP		
Parameter	**Example**	**Your Application**
Active or Inactive	Active enables IP communication (IPX and Transparent Bridge are not used in this example).	
Interface Unnumbered	Numbered	
Primary IP Address	100.130.130.1	
Subnet Mask	255.255.255.0	
Secondary IP Address	0.0.0.0 for none.	
Enable Dynamic Local IP Address	No	
IP MTU	Use the preset value, 1500. This determines whether or not a given IP datagram is fragmented.	
NAT	Global, because NAT is not being used in this example.	
ICMP Port	Inactive	
Incoming Rule List	None, filters and traffic control are not included in this example.	
Outgoing Rule List Name	None, filters and traffic control are not included in this example.	
Proxy ARP	Inactive	
IP Bridge	Inactive	

FIGURE 4.2 ETHERNET NETWORK PROTOCOL MENU PARAMETERS

STEP TWO

No more parameters are necessary for the Ethernet interface. The next step is the configuration of the E1 or T1

Chapter 4 - Step-By-Step Instructions for Common Applications 32

line using the controller. Both CAS and CCS signaling are explained. Which one is used will depend on the services offered by the telephone system.

Menu CONFIG=>CONTROLLER=>T1/E1		
Parameter	**Example**	**Your Application**
Frame Mode	This value is provided by the T1/E1 line provider. For T1, *ESF* (Extended Super Frame, the most common) and *D4* are the options. For E1, *CRC4* (the most common) and *Non-CRC4* are the options.	
Line Code	This value is provided by the T1/E1 line provider. For T1, *B8ZS* (Bipolar 8 Zero Substitution, the most common) and *AMI* (Alternate Mark Inversion) are used. For E1, the choices are *HDB3* (High-Density Bipolar) and *AMI*.	
Signaling Mode	*CCS* for ISDN-PRI (digital or analog remote access). *CAS* for analog, modem-based remote access (usually used with telephone networks that do not support ISDN).	
Clock Mode (CAS only)	Slave	
Line Build Out	Applies only to T1. The T1 service provider should supply this parameter.	
Receiver Sensitivity	Short Haul	
Companding Mode	This value is provided by the T1/E1 line provider. *A-law* is usually used for E1 lines and *u-law* is usually used for T1 lines.	
Signaling Type (CAS only)	Wink Start or Loop Start for T1 and R2 Digital ITU-T for E1 are the options	
Tone Signaling	CAS Only. This value is provided by the T1/E1 line provider. DTMF is the most common for T1 and MFR2 Compelled is the most common for E1.	
Country Signaling	Type ? to the options available for each country. This value is provided by the T1/E1 line provider.	

FIGURE 4.3 E1/T1 CONTROLLER MENU PARAMETERS

STEP THREE

It is likely that not just anyone should have access to your LAN. A Radius or Tacacs server can be used to authenticate the username and password of the incoming connection request. A Radius server is used in this example. More than one Radius server can be configured. Fill in the data for your Radius Server in the table below.

Menu CONFIG=>SECURITY=>RADIUS=>RADIUS STATUS=>ADD		
Parameter	**Example**	**Your Application**
Radius Server IP Address	100.130.130.200	
Radius Server Type	*Both* Authentication and Accounting.	
Radius Server Retries	5	
Radius Server Timeout	5	
Radius Server Encryption Key	pinocchio	
Radius Server Authentication Port	1812. Older standards used 1645.	
Radius Server Send Start accounting	Yes	

FIGURE 4.4 RADIUS SERVER PARAMETERS

STEP FOUR

The RAS Wizard can be used to set up a PPP Remote Access Server using modems or DSU/CSUs and dial-up lines. The wizard can be used for one port or a range of ports. If the Wizard is used for a range or all ports, the ports will be numbered consecutively.

Menu CONFIG=>INTERFACE=>T1/E1(ISDN-PRI)=><CHANNEL>=>WIZARDS=>RAS PROFILE		
Parameter	**Example**	**Your Application**
Remote IP Address	100.130.130.11	
Phone Number (CAS Only)	This number is only used for callback (in the outgoing connection request).	
Digital Modem Profile ID (CAS Only)	1	

FIGURE 4.5 RAS WIZARD PARAMETERS

STEP FIVE

Now that the parameters have been defined, enter into each menu described above, in the order presented (read chapter 3, Using Menus, if you have not done so already). Set the parameters in each menu according to the values you wrote in the figures above. Save the configuration to flash memory at each step when requested — configurations saved in run memory are erased when the router is turned off. If you saved part of the configuration to run memory for some reason, save to flash memory now using the menu option ADMIN =>WRITE CONFIGURATION =>TO FLASH. Be sure to change the superuser password using the menu option CONFIG =>SECURITY =>USERS =>MODIFY. The user ID, super, can remain the same, but the password must be changed to avoid unauthorized access.

If the Radius Server does not appear to be working, try switching the UDP port setting. This often resolves Radius problems. The menu item INFO =>AUTH. SERVERS STATUS =>RADIUS SERVERS STATUS also provides information about the status of the Radius Server. Any status other than OK means that either the RAS configuration is incorrect or the Radius Server configuration is incorrect. It may be necessary to reboot the router after performing the configuration described in step three, for the changes to take effect.

Cyclades-PR4000

At this point, you should create a back-up of the configuration file (in binary) and print out a listing of the configuration.

Instructions for creating a back-up of the configuration file:
Use the menu option ADMIN =>WRITE CONFIGURATION =>TO FTP SERVER. Fill in the IP address of the computer where the configuration file should be saved, the file name, the directory name, and the user account information. This configuration file can later be downloaded with the ADMIN =>LOAD CONFIGURATION =>FTP SERVER option.

Instructions for listing the configuration:
The menu option INFO =>SHOW CONFIGURATION =>ALL will list to the terminal screen the configuration of the router. This can be saved as a text file and/or printed on a printer.

Example 2 Connection to an Internet Access Provider via Modem

This section will guide you through a complete router installation for the connection of a LAN to an Internet access provider via PPP. The configuration of NAT (Network Address Translation) will also be shown. Figure 4.6 shows the example system used in this section. Spaces have been provided next to the parameters needed for the configuration where you can fill in the parameters for your system. Do this now before continuing.
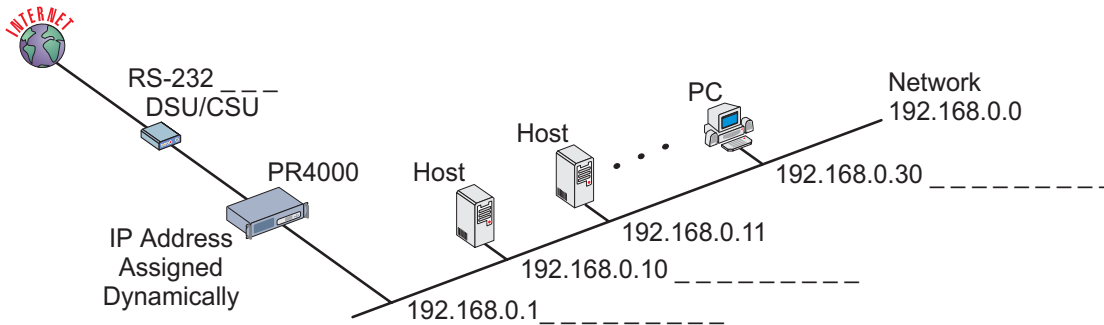
FIGURE 4.6 CONNECTION TO ACCESS PROVIDER USING A SWAN INTERFACE AND A MODEM

Please read the entire example and follow the instructions before turning the router on. The router is programmed to log the super user off after 10 minutes of inactivity. All data not explicitly saved to memory is then lost. Collecting the data *while* configuring the router will likely cause delays and frustration.

STEP ONE

The first step is to determine the parameters needed to configure the Ethernet interface (ETH0). The parameters in the Network Protocol Menu (IP) are shown in Figure 4.7. Fill in the blanks for your application in the right-most column. These parameters will be entered into the router later, after all parameters have been chosen. Each parameter in this menu is explained in more detail in chapter 5 of the Installation Guide.

Menu CONFIG=>INTERFACE=>ETHERNET=>NETWORK PROTOCOL=>IP		
Parameter	**Example**	**Your Application**
Active or Inactive	Active enables IP communication (IPX and Transparent Bridge are not used in this example).	
Interface Numbered /Unnumbered	Numbered	
Primary IP Address	192.168.0.1	
Subnet Mask	255.255.255.0	
Secondary IP Address	0.0.0.0 for none	
IP MTU	Use the preset value, 1500. This determines whether or not a given IP datagram is fragmented.	
NAT	Local	
ICMP Port	Inactive	
Incoming Rule List	None, filters and traffic control are not included in this example.	
Outgoing Rule List Name	None, filters and traffic control are not included in this example.	
Proxy ARP	Inactive	
IP Bridge	Inactive	

FIGURE 4.7 ETHERNET NETWORK PROTOCOL MENU PARAMETERS

STEP TWO
No more parameters are necessary for the Ethernet interface. The other interface to be configured is the SWAN in slot 1. The SWAN physical media parameters are shown in Figure 4.8. Fill in the values for your application. The SWAN configuration is described in more detail in chapter 6 of the Installation Guide.

Menu CONFIG=>INTERFACE=>SWAN=>PHYSICAL		
Parameter	**Example**	**Your Application**
Mode	Asynchronous	
Speed	115.2k	

FIGURE 4.8 SWAN PHYSICAL MENU PARAMETERS

STEP THREE
The network protocol parameters, shown in Figure 4.9, are similar to those for the Ethernet interface. Fill in the parameters for your network in the right-most column. For an example using NAT where the Primary IP Address is not dynamically assigned, see the chapter dedicated to NAT in the Installation Manual.

Menu CONFIG=>INTERFACE=>SWAN=>NETWORK PROTOCOL=>IP		
Parameter	**Example**	**Your Application**
Active or Inactive	Active enables IP communication (IPX and Transparent Bridge are not used in this example).	
Interface Unnumbered/ Numbered	Numbered	
Primary IP Address	0.0.0.0 (This number will be assigned by the Access Provider dynamically.)	
Subnet Mask	255.0.0.0	

FIGURE 4.9 SWAN NETWORK PROTOCOL (IP) MENU PARAMETERS

Parameter	Example	Your Application
Secondary IP Address	0.0.0.0 for none	
Enable Dynamic Local IP Address	Yes, because the IP address of the SWAN interface will be assigned dynamically.	
Remote IP Address Type	Any	
Remote IP Address	0.0.0.0	
IP MTU	Use the preset value, 1500. This determines whether or not a given IP datagram is fragmented.	
NAT	*Global Assigned* because the IP address of the SWAN interface will be assigned dynamically.	
ICMP Port	Inactive	
Incoming Rule List	None, filters and traffic control are not included in this example.	
Outgoing Rule List Name	None, filters and traffic control are not included in this example.	
Routing of Broadcast Messages	Inactive	

FIGURE 4.9 CONTINUED -- SWAN NETWORK PROTOCOL (IP) MENU PARAMETERS

STEP FOUR

The Encapsulation parameters for PPP are less straight-forward. Many of them are based on decisions that cannot be shown in a diagram. Fortunately, the choices made here will mostly affect the performance of the link, rather than whether it works or not. Fill in the parameters appropriate for your system, consulting chapter 11 of the Installation Guide for more information if necessary.

Menu CONFIG=>INTERFACE=>SWAN=>ENCAPSULATION=>PPP		
Parameter	**Example**	**Your Application**
MLPPP	*No*	
PPP Inactivity Timeout	*None* so that the connection is never broken.	
Enable Van Jacobson IP Header Compression	No	
Disable LCP Echo Requests	No	
Edit ACCM	No Value. This will depend on the modem used.	
Time Interval to Send Config Requests	Use the preset value, one.	
Enable Predictor Compression	No	

FIGURE 4.10 PPP ENCAPSULATION MENU PARAMETERS

STEP FIVE

A static route must be added to tell the router that all traffic not intended for the local LAN should be sent to the Access Provider. Chapter 12 of the Installation Guide explains static routes and other routing methods available in CyROS. Fill in the spaces in Figure 4.11 with the values for your application.

Menu CONFIG=>STATIC ROUTES=>IP=>ADD ROUTE		
Parameter	**Example**	**Your Application**
Destination IP Address	Type in the word "DEFAULT".	
Gateway or Interface	*Interface*, because the IP addresses are not known at configuration time.	
Interface	*Link 1* in the example.	
Is This a Backup Route?	No	
OSPF Advertises This Static Route	No	

FIGURE 4.11 STATIC ROUTE MENU PARAMETERS

STEP SIX

NAT must now be activated. There are two varieties of NAT: Normal and Expanded. This example uses the Normal NAT Mode. The other mode is explained in the chapter on NAT in the Installation Manual.

Menu CONFIG =>SECURITY =>NAT =>GENERAL		
Parameter	**Example**	**Your Application**
Nat Status	Enabled	
Nat Mode	Normal	
Disable Port Translation	No	

FIGURE 4.12 GENERAL NAT PARAMETERS

STEP SEVEN

NAT parameters will now be determined for routing outside of the local LAN. Network Address Translation maps the local IP addresses, registered in the local address range menu below, to the one global IP address assigned by the access provider. Local IP addresses not indicated in this menu will not be translated.

Menu CONFIG =>SECURITY =>NAT =>LOCAL ADDRESS =>ADD RANGE		
Parameter	**Example**	**Your Application**
First IP Address of New Range	192.168.0.10	
Number of IP Addresses in the Range	21	

FIGURE 4.13 NAT LOCAL ADDRESS RANGE MENU PARAMETERS

The factory preset values for all other NAT parameters are appropriate for this example.

STEP EIGHT

Now that the parameters have been defined, enter into each menu described above, in the order presented (read chapter 3, Using Menus, if you have not done so already). Set the parameters in each menu according to the values you wrote in the figures above. Save the configuration to flash memory at each step when requested — configurations saved in run memory are erased when the router is turned off. If you saved part of the configuration to run memory for some reason, save to flash memory now using the menu option ADMIN =>WRITE CONFIGURATION =>TO FLASH.

STEP NINE

The Ethernet interface can be tested as described in the troubleshooting appendix. The SWAN interface can be tested in a similar manner. At this point, you should create a back-up of the configuration file (in binary) and print out a listing of the configuration.

Instructions for creating a back-up of the configuration file.
Use the menu option ADMIN =>WRITE CONFIGURATION =>TO FTP SERVER. Fill in the IP address of the computer where the configuration file should be saved, the file name, the directory name, and the user account information. This configuration file can later be downloaded with the ADMIN =>LOAD CONFIGURATION =>FTP SERVER option.

Instructions for listing the configuration.
The menu option INFO =>SHOW CONFIGURATION =>ALL will list to the terminal screen the configuration of the router. This can be saved as a text file and/or printed on a printer.

CHAPTER 5 CONFIGURATION OF THE ETHERNET INTERFACE

The PR4000 has one Ethernet 10/100Base-T interface, provided in a standard RJ-45 modular jack, which should be connected to an Ethernet hub or switch. Use a standard 10/100Base-T straight-through cable (not included). When the Ethernet link is correctly connected, the link LED will be lit. The menus for the Ethernet Interface are independent of the speed of the link.

If your network uses 10Base2 (thin coaxial cable) or 10Base5 (thick coaxial cable), you will need a transceiver to convert between the different Ethernet media. A crossover cable is required for direct connection to a computer (an RJ-45 Ethernet pinout is provided in appendix B). Note: While Cyclades Power Routers work with most standard RJ-45 cable/connectors, shielded Ethernet cables should be used to avoid interference with other equipment .

The parameters in the encapsulation menu are preset at the factory and it is usually not necessary to change them. The first step in the Ethernet configuration is to choose which network protocol to use and assign values to the relevant parameters. Either IP, Transparent Bridge, or IPX (optional) must be activated. In this chapter, IP Bridges are also described. Use the information provided below to set the parameters for the Ethernet interface.

The IP Network Protocol

Some parameters are explained in detail in later chapters. At this point, the preset values provided by the operating system can be accepted and the interface will work at a basic level.

Network Protocol Menu CONFIG =>INTERFACE =>ETHERNET =>NETWORK PROTOCOL =>IP

Parameter	Description
Active or Inactive	Activates this interface.
Interface Unnumbered	Unnumbered interfaces are used for point-to-point connections.
Assign IP From Interface	Applies to *Unnumbered* interfaces. Applies the IP address of another router interface to this one.
Primary IP Address	Applies to *Numbered* interfaces. Address assigned to this interface.
Subnet Mask	Applies to *Numbered* interfaces. Subnet mask of the network.
This table is continued.	

Network Protocol Menu (Continued)

Parameter	Description
Secondary IP Address	Applies to *Numbered* interfaces. Indicates a second (or third, etc. up to eight) IP address that can be used to refer to this interface. This parameter and the next are repeated until no value is entered.
Subnet Mask	Applies to *Numbered* interfaces. Subnet mask of *Secondary IP Address*.
IP MTU	Assigns the size of the Maximum Transmission Unit for the interface. This determines whether or not a given IP datagram is fragmented.
NAT	Determines the type of IP address if NAT is being used. Use *Global* otherwise. See chapter 13 or the examples in chapter 2 for details on how to configure NAT.
ICMP Port	*Active* causes the router to send ICMP Port Unreachable messages when it receives UDP or TCP messages for ports that are not recognized. This type of message is used by some traceroute applications, and if disabled, the router might not be identified in the traceroute output. However, there are security and performance reasons to leave this option *Inactive*.
Incoming Rule List	Filter rule list for incoming packets. See chapter 14 for instructions on how this parameter should be set.
Detailed Incoming IP Accounting	Applies when a list is selected in the previous parameter. See explanation of IP Accounting in chapter 12. IP Accounting for a rule requires that the parameter CONFIG =>RULES LIST=>IP=>CONFIGURE RULES=>ADD RULE=>ALLOW ACCOUNT PROCESS also be *Yes*.
Outgoing Rule List Name	Filter rule list for outgoing packets. See chapter 14 for instructions on how this parameter should be set.
Detailed Outgoing IP Accounting	Applies when a list is selected in the previous parameter. See explanation of *Detailed Incoming IP Accounting*.
Routing of Broadcast Messages	Activating this parameter causes the router to route broadcast messages from the LAN to the WAN and vice-versa. An individual interface can be excluded by setting this parameter to *Inactive*, without effecting the broadcast of messages on the other interfaces.
Proxy ARP	Causes the router to answer ARP requests with its own MAC address for IP addresses reachable on another interface.

IP Bridge

An IP Bridge is used to divide a network without subnetting. Whenever a subnetwork is created, two IP numbers are lost — one describing the network and the other reserved for broadcast. This does not occur with an IP Bridge.
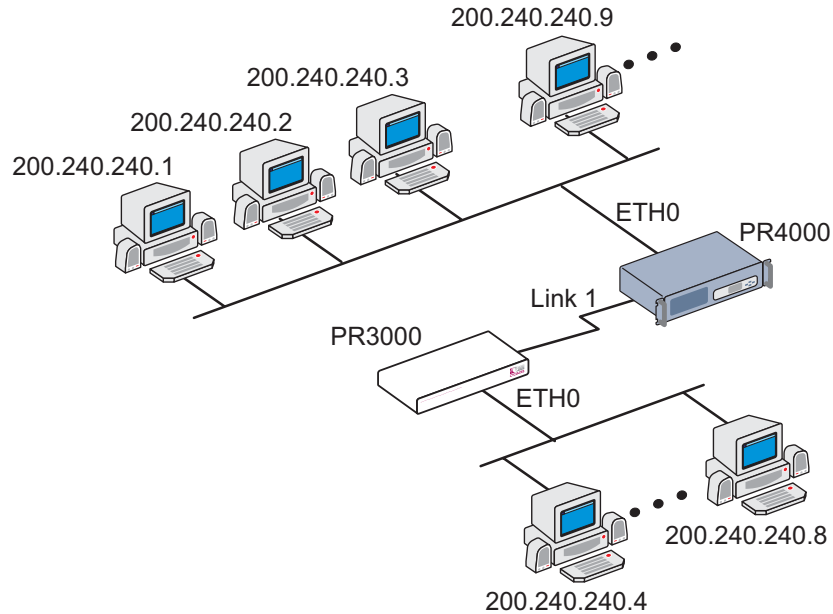
FIGURE 5.1 IP BRIDGE EXAMPLE

In Figure 5.1, an example of the use of an IP Bridge is given. From the available IP addresses, the range 200.240.240.4 to 200.240.240.8 is bridged to another physical location. The following parameters apply only for IP Bridge.

Network Protocol Menu (Continued) -- (IP Bridge)

Parameter	Description
IP Bridge	Activates the IP Bridge functionality.
The following parameters apply only if IP Bridge is *Active*.	
Initial IP Address to be Bridged	Indicates the start of the range of IP addresses to be transferred to another physical location. This and the next three parameters are repeated in case the bridge is to be broken up into various sections. Up to 8 sections can be defined. In the example, this value is 200.240.240.4.
Ending IP Address to be Bridged	Indicates the end of the range of IP addresses to be transferred to another physical location. In the example, this value is 200.240.240.8.
Broadcast Over the Link	Allows propagation of broadcast IP packets over this bridge.
Bridge Over Link	Indicates which link forms the other half of the bridge. In the example, link 1 is used.

Other Parameters

Transparent Bridge is covered in chapter 7 and IPX is covered in chapter 15. The parameters defined in the Routing Protocol and Traffic Control Menus should be set after reading chapters 11 and 14, respectively. It is probably best to complete the basic configuration of all router interfaces, then return to the routing protocol and traffic control menus after general routing and traffic control strategies have been defined.

CHAPTER 6 THE SWAN INTERFACE

This chapter describes how to configure a SWAN interface. The physical link should be set up as shown in chapter 2, according to the type of modem or device at the other end of the connection and the type of SWAN port.

STEP ONE
The first step in the SWAN interface configuration is to define its physical characteristics. These parameters are presented in the Physical Menu Table.

Physical Menu   CONFIG=>INTERFACE=>SWAN=>PHYSICAL

Parameter	Description
Mode	Asynchronous or Synchronous. This parameter is determined by the mode of the device at the other end of the connection.
Clock Source	Applies for *Synchronous Mode*. Whether this interface provides clock for the device at the other end of the cable or vice-versa. When the interface is connected to a modem, the *Clock Source* is always *External*.
Receive Clock	Applies for *Internal Clock Source*. When this interface provides clock, it can either compare incoming messages with the clock it is generating (*Internal*) or with the clock it receives from the sender along with the message (*External*). *External* is recommended.
Speed	Applies for *Internal Clock Source*. Determines at which speed the data will be sent across the line.
Media for SWAN Cable	Type of cable -- RS-232, V.35 or X.21. Usually the type is cable is detected by the router.

STEP TWO
The second step is to choose a data-link protocol in the Encapsulation menu. There are many encapsulation options on this interface.

For synchronous communication:
- Frame Relay: the Frame Relay Protocol is based on frame switching and constructs a permanent virtual circuit (PVC) between two or more points.
- X.25: The X.25 Protocol is generally used to connect to a public network. The router can act either as a DTE or a DCE.
- HDLC: A proprietary alternative to PPP.

For synchronous or asynchronous communication:
- PPP: The PPP (Point-to-Point) protocol is used for leased, dial-up, and ISDN lines. Multilink PPP is also provided.

Information on how to determine the values of the parameters for each data-link protocol is provided in chapter 8.

STEP THREE
The third step is to set the Network Protocol parameters. Information for this step is provided in chapter 7.

STEP FOUR
If PPP Encapsulation is being used, a type of authentication should be chosen. This is done in the authentication menu.

Authentication Menu   CONFIG=>INTERFACE=>SWAN=>AUTHENTICATION

Parameter	Description
Authentication Type	*Local* uses the list of users defined in CONFIG=> SECURITY=>USERS=>ADD. *Server* uses either Radius or Tacacs to authenticate the user. *Remote* is when this interface is considered to be the user and the **other** end of the connection performs the authentication
Username	Applies when Authentication Type is Remote. The username the remote device expects to receive.
Password	Applies when Authentication Type is Remote. The password the remote device expects to receive.
Authentication Server	Applies when *Authentication Type* is *Server*. Indicates that either a Radius or Tacacs server is used for validation. The location and other parameters of the server must be configured in CONFIG=> SECURITY. See section 4.3 of the CyROS Reference Guide.
Authentication Protocol	Applies when *Authentication Type* is *Local* or *Server*. Either PAP or CHAP or both can be used for authentication.

STEP FIVE
The parameters defined in the Routing Protocol and Traffic Control Menus should be set after reading chapters 9 and 12, respectively. It is probably best to complete the basic configuration of all router interfaces, then return to the routing protocol and traffic control menus after general routing and traffic control strategies have been defined.

CHAPTER 7 THE E1 AND T1 INTERFACES, WITHOUT SIGNALING

The menus relating to configuration of the E1 and T1 interfaces without signaling are given in this chapter. T1 is a standard used in the United States, Canada, and Japan. It has a clock speed of 1.5MHz and has 24 channels of 64K each. One of the channels is reserved for signaling when ISDN/PRI is used. E1 is a standard used in Europe and many other countries. It has a clock speed of 2MHz and has 32 channels with two reserved for signaling. Aside from this, there are few differences between the two standards in terms of configuration.

The Controller menu tree for the PR4000 (for Signaling Mode = None) is shown in figure 7.1
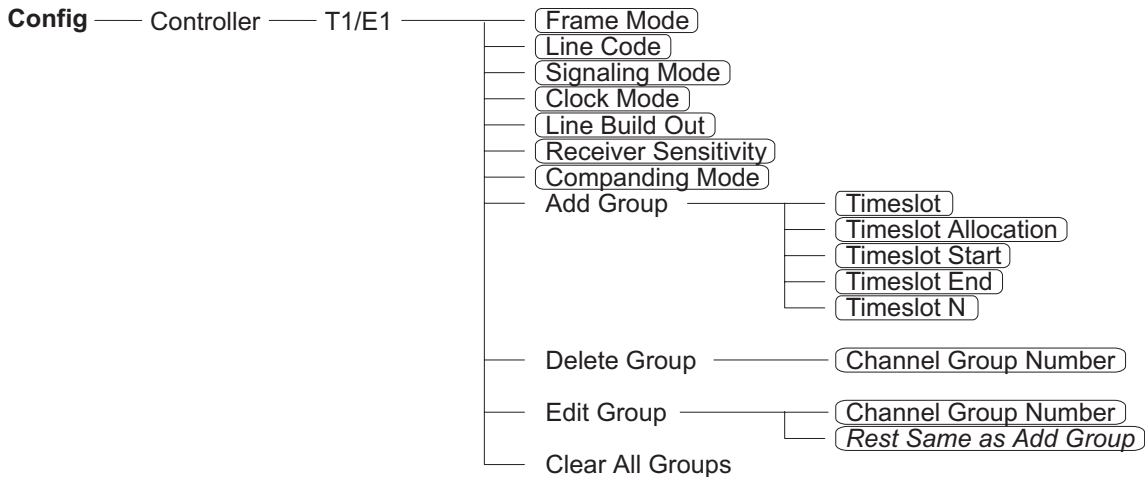
FIGURE 7.1 PR4000 CONTROLLER MENU TREE

Cyclades-PR4000

The controller parameters are explained in the table that follows.

Controller Menu   CONFIG=>CONTROLLER=>T1/E1

Parameter	Description
Frame Mode	**T1**: *ESF* (Extended Super Frame, the most common) and *D4* are the options. **E1**: *CRC4* (the most common) and *Non-CRC4* are the options.
Line Code	**T1**: *B8ZS* (Bipolar 8 Zero Substitution, the most common) and *AMI* (Alternate Mark Inversion). **E1**: *HDB3* (High-Density Bipolar) and *AMI*.
Signaling Mode	Only appears for the PR4000. *None* for channelized lines without signaling, **otherwise, see chapter 8.**
Clock Mode	Selects the clock mode: *Master* or *Slave*.
Line Build Out	Applies only to T1. Sets the attenuation on the TX line. The T1 service provider should supply this parameter.
Receiver Sensitivity	*Short haul* is usually used. *Long haul* is necessary if attenuation prevents reception of data, usually when the router is installed more than 2000 feet from the cable termination.

For the CCS Signaling Mode (ISDN-PRI) and the CAS Signaling Mode, read chapter 8 **INSTEAD** of this chapter.

The T1/E1 interface can be broken up into channels, defined by timeslots. Each timeslot is a slice of time allotted to throughput from a particular source. The configuration can be done in three ways:

1 Full T1/E1: Only one channel group is defined and no others are allowed. All timeslots are allocated automatically to this channel.
2 Fractional T1/E1: Only one channel group is defined. One or more timeslots are allocated to this channel. The number of timeslots can be increased at a later time.
3 Channelized T1/E1: Many channels are defined, with one or more timeslots allocated to each channel.

STEP ONE
The first step in the T1/E1 configuration is the assigning of channel groups, performed in the channel groups menu shown in Figure 8.1. A brief description of the add group menu parameters is given in the table.

Add Channel Group Menu CONFIG =>CONTROLLER =>T1/E1 =>CHANNEL GROUPS =>ADD GROUP

Parameter	Description
Timeslot	*Full* is used for Full T1/E1 as described above. *Fractional* is for Fractional or Channelized T1/E1 as described above.
Timeslot Allocation	*Contiguous* allows configuration of a range of timeslots while *Manual* presents each available timeslot one by one.
Timeslot Start	Applies for *Contiguous Timeslot Allocation*. Defines the beginning of the range.
Timeslot End	Applies for *Contiguous Timeslot Allocation*. Defines the end of the range.
Timeslot N	Applies for *Manual Timeslot Allocation*. Allows inclusion of this timeslot in the channel.

STEP TWO
The parameters for each E1/T1 channel are configured in the CONFIG =>INTERFACE =>T1/E1 =>*<CHANNEL>* menu.   A summary menu tree is given in Figure 7.2.
A brief description of each principal item appears in the following table.

E1/T1 Interface Menu CONFIG=>INTERFACE=>T1/E1=>*<CHANNEL>*

Menu Item	Description
Encapsulation	Determines the data-link layer protocol to be used for this communication link.
Network Protocol	Provides menus for the IP and Transparent Bridge parameters, including rules to be applied to this interface.
Routing Protocol	Submenus for RIP and OSPF configuration.
Traffic Control	Sets the bandwidth of the connection for use with traffic control rules and associates a traffic control rule list to this interface. See chapter 14 for more information on traffic control rules.
Authentication	Determines the method used for authentication for connections on this line.

Config

```
Interface ── T1/E1 ── Channel ──── Encapsulation ── Frame Relay [menu shown in a later figure]
                     (if Channelized)                PPP [menu shown in a later figure]
                                                     X.25 [menu shown in a later figure]

                                                     HDLC ──────────── [Keep Alive Interval]

                                                     Inactive

                                    Network Protocol [menu shown in a later figure]
                                    Routing Protocol [menu shown in a later figure]

                                    Traffic Control ── General ──── [Bandwidth]
                                                                    [IP Traffic Control List]

                                    Authentication ── [Authentication Type]
                                                      [Username]
                                                      [Password]
                                                      [Authentication Server]
                                                      [Authentication Protocol]
```
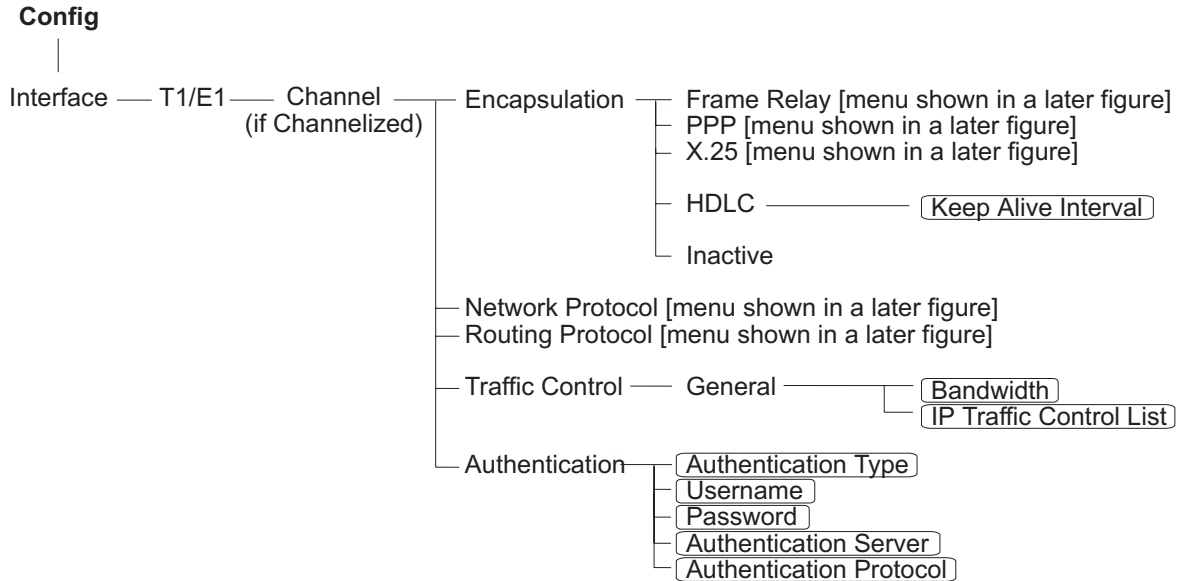
FIGURE 7.2 E1/T1 INTERFACE CONFIGURATION MENU TREE

STEP THREE
There are many encapsulation options on this interface.
For full T1/E1:
- Frame Relay,
- PPP,
- X.25, and
- HDLC.

For channelized T1/E1:
- PPP and HDLC.

The Encapsulation options are described in chapter 10.

STEP FOUR

The Network Protocol Menu parameters must be set next. A description of these parameters appears in chapter 9. The remaining menus in Figure 7.2 are described in later chapters. Routing Protocols is the subject of chapter 11, and Traffic Control is discussed in chapter 14. The Authentication Menu is only relevant when PPP Encapsulation is used.

Authentication Menu CONFIG =>INTERFACE =>T1/E1 =>*CHANNEL* =>AUTHENTICATION

Parameter	Description
Authentication Type	*Local* uses the list of users defined in CONFIG =>SECURITY =>USERS =>ADD. *Server* uses either Radius or Tacacs to authenticate the user. *Remote* is when this interface is considered to be the user and the **other** end of the connection performs the authentication
Username	Applies when Authentication Type is Remote. The username the remote device expects to receive.
Password	Applies when Authentication Type is Remote. The password the remote device expects to receive.
Authentication Server	Applies when *Authentication Type* is *Server*. Indicates that either a Radius or Tacacs server is used for validation. The location and other parameters of the server must be configured in CONFIG=>SECURITY. See section 4.3 of the CyROS Reference Guide.
Authentication Protocol	Applies when *Authentication Type* is *Local* or *Server*. Either PAP or CHAP or both can be used for authentication.

CHAPTER 8 THE E1 AND T1 INTERFACES, WITH SIGNALING

Two varieties of signaling are available. The older mode, called CAS, and the newer mode, called CCS (which is used for ISDN-PRI). The first step in the configuration process is to configure the channels using the Controller menu. The Controller Menu tree is shown in Figure 8.1. The parameters are described in the table that follows.

```
Config ——— Controller ——— E1/T1 ——┬— Frame Mode
                                    ├— Line Code
                                    ├— Signaling Mode
                                    ├— Clock Mode
                                    ├— Receiver Sensitivity
                                    ├— Companding Mode
                                    ├— Signaling Type
                                    ├— Tone Signaling
                                    ├— Contry Signaling
                                    └— Switch Type
```
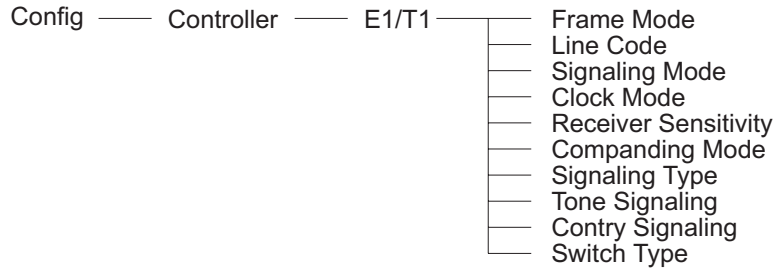
FIGURE 8.1 THE CONTROLLER MENU TREE

Controller Menu   CONFIG=>CONTROLLER=>T1/E1

Parameter	Description
Frame Mode	**T1**: *ESF* (Extended Super Frame, the most common) and *D4* are the options. **E1**: *CRC4* (the most common) and *Non-CRC4* are the options.
Line Code	**T1**: *B8ZS* (Bipolar 8 Zero Substitution, the most common) and *AMI* (Alternate Mark Inversion). **E1**: *HDB3* (High-Density Bipolar) and *AMI*.
Signaling Mode	*None* for channelized lines without signaling (see chapter 7), *CCS* for ISDN-PRI and *CAS* for analog, modem-based remote access (usually used with telephone networks that do not support ISDN).
Clock Mode	Selects the clock mode: *Master* or *Slave*.
Line Build Out	Applies only to T1. Sets the attenuation on the TX line. The T1 service provider should supply this parameter.
Receiver Sensitivity	*Short haul* is usually used. *Long haul* is necessary if attenuation prevents reception of data, usually when the router is installed more than 2000 feet from the cable termination.
Companding Mode	Defines the compression mode to be used. Depends on the telephone exchange and the E1/T1 provider should supply this parameter. *A-law* is usually used for E1 lines and *u-law* is usually used for T1 lines.
Signaling Type	Applies when *Signaling Mode* is *CAS*. Selects the signaling type. This should be supplied by the service provider. The options are R2-Digital, ITU-T, and R2-Analog.
Tone Signaling	Applies when *Signaling Mode* is *CAS*. Will depend on what is expected by the line provider. DTMF is the most common tone signaling for T1 and MFR2 Compelled is the most common for E1.
Country Signaling	Applies when *Signaling Mode* is *CAS*. Determines country-dependent signaling parameters.
Switch Type	Applies when *Signaling Mode* is *CCS*. Selects the signaling protocol. This should be supplied by the service provider.

The CCS Signaling Mode (ISDN-PRI)

ISDN, the Integrated Services Digital Network, was intended to be a digital upgrade to the current analog telephone system. The ISDN discussed in this chapter is N-ISDN, where the N is for Narrow Band. A Broad Band ISDN also exists. There are two ISDN interfaces:

- BRI — Basic Rate Interface — used for residential or small-business access.
- PRI — Primary Rate Interface — used to provide access or used by large businesses for access.

Two PRI interfaces are provided on the PR4000 via E1 or T1 ports with CCS Signaling. These connections can be digital or analog (via a modem). The data layer protocols CHAR, PPPCHAR and Slip are used with a modem connection.

A typical application in an Internet Service Provider is shown in Figure 8.2.
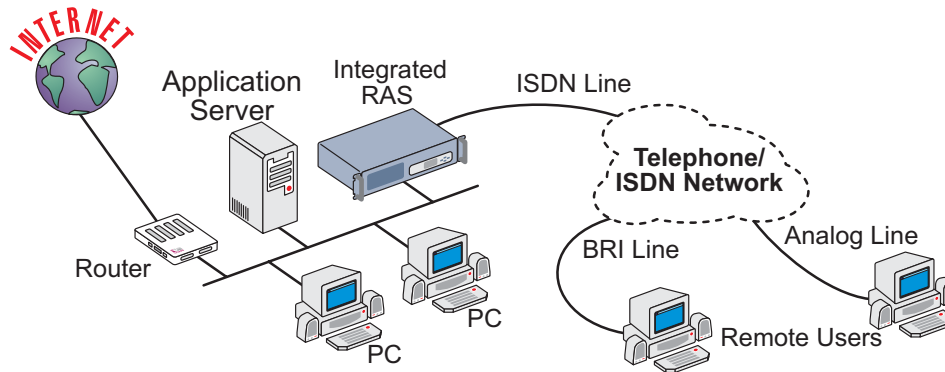
FIGURE 8.2 ISDN-PRI APPLICATION EXAMPLE

After the channel groups are defined, the ISDN line and channels must be configured. The ISDN-PRI Interface Configuration Menu tree is shown in Figure 8.3.

Config —— Interface —— T1/E1 (ISDN-PRI) —— ISDN —— Main Phone
      Idle Timeout
      T200
      N200
      T203
      Add Entry —— Destination IP Address / DestinationPhone # / Slot N Channel #
      Delete Entry
      Edit Entry —— *Same as Add Entry*
      Clear All Entries

One Channel —— Encapsulation / Network Protocol / Routing Protocol / ISDN / Traffic Control —— Bandwidth / IP Traffic Control List
      Authentication —— Authenticarion Type / Username / Passaword / Authentication Server / Authenticarion Protocol
      Wizards

Range —— *Same Parameters as One Channel*

All Channels —— *Same Parameters as One Channel*

FIGURE 8.3 ISDN-PRI INTERFACE CONFIGURATION MENU TREE

The general ISDN options are explained first.

ISDN General Menu CONFIG=>INTERFACE=>T1/E1(ISDN-PRI)=>ISDN

Parameter	Description
Main Phone #	Principal phone number assigned to the ISDN trunk line. Leave this parameter blank if this number should not be confirmed by the router. This is recommended when the provider does not send the trunk line number in the incoming call message.
Idle Timeout	Time, in minutes, for the connection to time out if there is no traffic. For this to work, any status messages, like PPP's LCP Echo Requests, must be disabled. The value 0 disables the timeout function.
T200	Data-layer timer. When the router sends a command, this timer determines how long it should wait for a response.
N200	Data-layer number of re-tries. When the T200 period passes without a response, the command is re-sent up to N200 times.
T203	When no messages are received for T203 seconds, an enquiry (RR or RNR) is sent.

At the end of this parameter list appears the menu for the dial-out table. It can also be reached by using the <ESC> key at any time during the parameter list.

Each entry is an association between a channel and the IP Address and Phone number at the other end of the connection. The router uses the IP information stored here in its routing table. When a packet arrives at the router, and the IP is listed in the dial-out table, the router will attempt a connection on the slot indicated using the associated phone number. The parameters for each entry are given next.

Add Entry Menu CONFIG =>INTERFACE =>T1/E1(ISDN-PRI)= >ISDN =><ESC> =>ADD ENTRY

Parameter	Description
Destination IP Address	IP Address assigned to the remote connection.
Destination Phone #	Phone number assigned to the remote connection
Slot N Channel #	Channel used to reach this destination.

The CAS Signaling Mode

A typical application that uses CAS Signaling is shown in Figure 8.4.
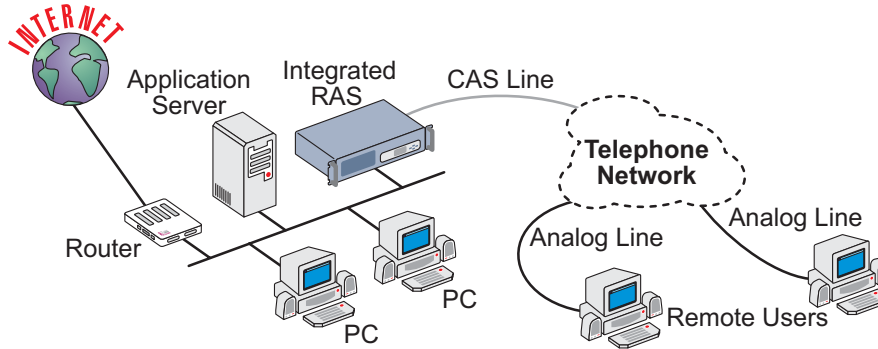
FIGURE 8.4 CAS APPLICATION EXAMPLE

The CAS Signaling Mode does not have a menu equivalent to the CONFIG =>INTERFACE =>T1/E1(ISDN-PRI) =>ISDN menu described above. Both signaling modes have a mode-specific menu at the channel level, with different names, but basically the same function. This menu, CONFIG =>INTERFACE =>T1/E1 =>*<CHANNEL>* =>SIGNALING, will be described in the next section. The Interface Configuration tree for E1/T1 with CAS Signaling is shown in Figure 8.5
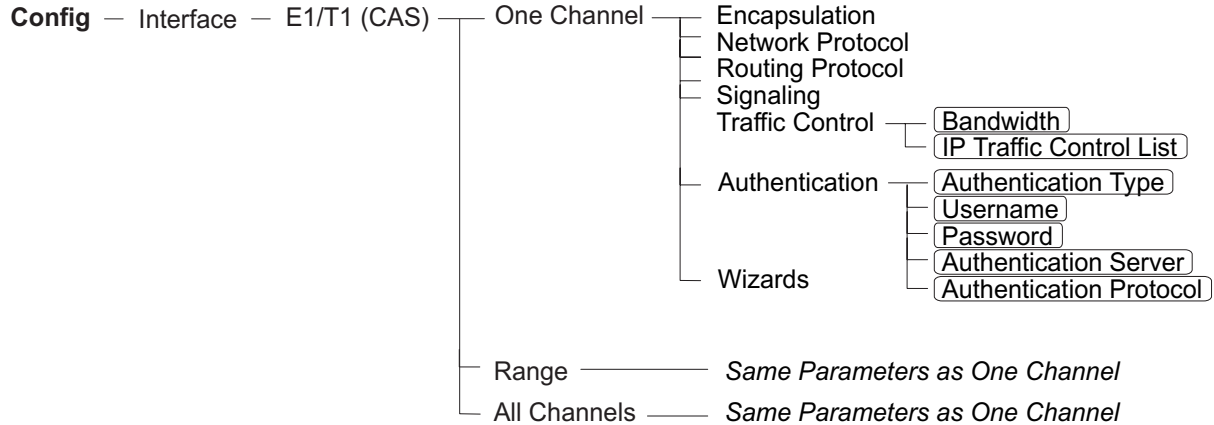
FIGURE 8.5 CAS INTERFACE CONFIGURATION MENU TREE

Parameters Independent of Signaling Mode

The channel specific parameters can be set for each channel individually, for a range of channels, or for all channels. Wizards are available to automatically configure the channels for typical applications. Details appear at the end of this chapter. The notation *<CHANNEL>* will be used to represent *One Channel*, *Range*, or *All Channels* where appropriate. The following menu options are available for each channel:

Channel Menu   CONFIG=>INTERFACE=>T1/E1=>*<CHANNEL>*

Menu Option	Description
Encapsulation	Determines the data-link layer protocol to be used for this communication link.
Network Protocol	Provides menus for the IP and Transparent Bridge parameters, including rules to be applied to this interface.
Routing Protocol	Configures RIP parameters.
ISDN(CCS) / Signaling (CAS)	Sets parameters particular to the signaling mode, and determines the phone number and modem profile.
Traffic Control	Sets the *Bandwidth* of the connection for use with traffic control rules and associates a *Traffic Control Rule List* to this interface. See section 4.7 for more information on traffic control rules.
Authentication	Determines the method used for authentication for connections on this line.
Wizards	Tools that aid in the configuration of the interface for common applications.

The encapsulation options, PPP, PPPCHAR, CHAR, Slip, and SlipChar are discussed in chapter 10.

Multilink Options

There are three ways to make two or more physical links perform as one logical link:

 1 Multichassis, Multilink PPP,
 2 Multilink PPP,
 3 CyROS Multilink (at the network-protocol level).

Multichassis PPP is a feature that allows two or more connections to different PR4000s on the same LAN act as one logical connection. The Cyclades Multichassis PPP implementation is compatible with the Lucent Portmaster 3 (either PR4000s/PR3000s or Portmaster 3s can be used to form the multichassis circuit). The multichassis PPP functionality is demonstrated in Figures 8.6 and 8.7.

Figure 8.6 shows a RAS bank in an Internet Service Provider. The RAS that receives the first connection becomes the master and the connection becomes the primary link. The information sent on link 1 passes through the RAS and continues on to its destination (in this example, a server on the LAN). At the same time, the RAS (IP 200.200.200.1 in the example) sends a broadcast message to all other RASs in the same group letting them know that it has the primary link for this PPP connection.
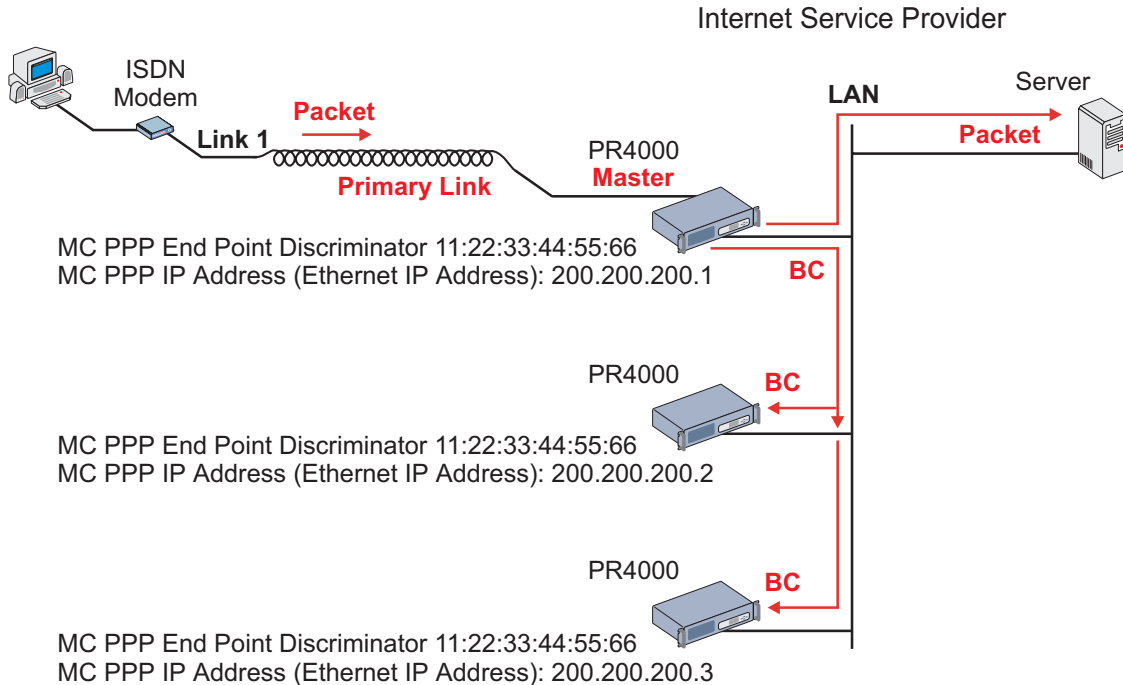
FIGURE 8.6 FIRST INCOMING CONNECTION OF A MULTICHASSIS PPP CIRCUIT

The RAS that receives the second connection from the same ISDN modem (shown in Figure 8.7), has already been informed by the broadcast message that the first RAS has the primary link. The connection is set up as a secondary link with this RAS (IP 200.200.200.3 in the example) as the slave. The information is not sent directly to its final destination. Rather, the packets are sent to the master RAS where they are joined with packets sent through other physical links before being forwarded to their final destination.

Cyclades-PR4000

The info menu items INFO=> SHOW MCPPP LINKS and INFO=> SHOW MCPPP NEIGHBORS provide information about the PPP connections and the other RASs forming the circuit. The tool DEBUG=> MESSAGE TRACE=> MCPPP may be useful in discovering MCPPP problems. Another tool exists which must be used in the RAS containing the primary link for a given PPP connection. The menu option ADMIN=> KILL VIRTUAL SESSION will show all active secondary links. Selecting one of them will cause the master RAS to send a message to the slave RAS holding that secondary link, ordering it to drop its connection.
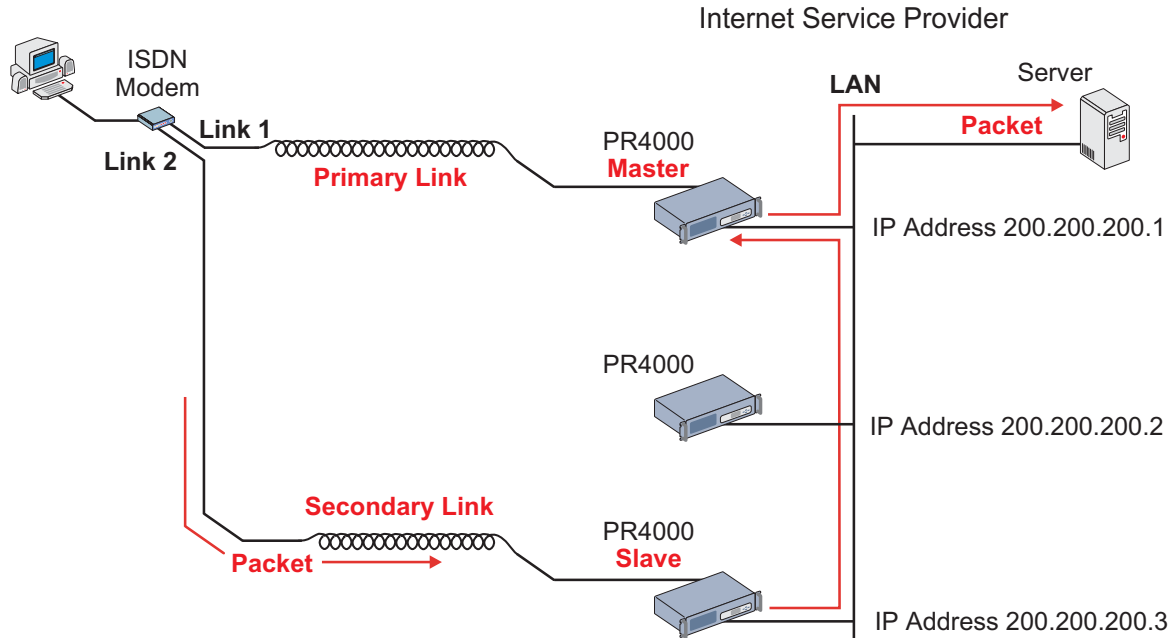
FIGURE 8.7 SECOND INCOMING CONNECTION OF A MULTICHASSIS PPP CIRCUIT

Multilink PPP (MLPPP) is similar in functionality to the Multichassis feature. The primary difference is that all physical links reside in the same RAS/Router. It is similar to the CyROS Multilink capability described in section 4.4 of the CyROS Refrence Guide, but it is implemented at the data-link level instead of the network-protocol level. When compared to Multilink, MLPPP is slightly more efficient and less generic (because it applies only to PPP encapsulation).
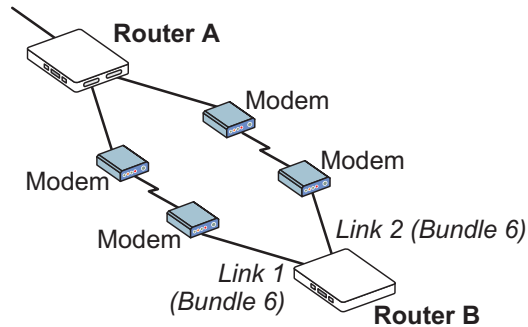
FIGURE 8.8 MULTILINK PPP EXAMPLE

In Figure 8.8, Router B connects to Router A via two modem connections to achieve a larger bandwidth. Router A accepts the two physical connections, but treats them as one logical connection (one "bundle"). MLPPP must be enabled on all interfaces that will form this bundle, (and on both sides of the connection), with the same bundle identifier specified for each.

Configuration of Multilink PPP (with an extension to Multichassis Multilink PPP) includes the following steps:

STEP ONE
The first four parameters in the PPP Menu must be defined. The PPP Menu can be reached by following the path: CONFIG =>INTERFACE =>*<INTERFACE or LINK>* =>ENCAPSULATION =>PPP. The first parameter enables MLPPP. The second parameter determines the type of connection (leased line, dial-in, etc.). The third parameter is the number assigned to the bundle, as described above (except for dial-in lines, where the bundle is defined dynamically). The number itself is not important, but must be consistently used by the routers on both ends of the connection. The fourth parameter determines the maximum number of links included in the multilink PPP circuit.

STEP TWO (only for Multichassis Multilink PPP)
The menu CONFIG =>IP =>MCPPP contains the only two parameters necessary to enable MCPPP. The first is the MCPPP End Point Discriminator, which must be the same for all RASs that will participate in the Multichassis Multilink PPP Circuit. The value of the number is immaterial, but it must have the form of a MAC number, as shown in the example. The other parameter is the MCPPP IP Address, which must be the same as the Ethernet IP address for the LAN where the other RASs are located. The MCPPP parameters must be set for all the RASs that will participate in the circuit.

The Network Protocol Menu tree is explained in chapter 9. The only routing protocol available is RIP. RIP is described in chapter 11. For each channel, certain signaling parameters must be configured. This menu tree is shown in Figure 8.9.

FIGURE 8.9 CHANNEL ISDN (OR SIGNALING) MENU TREE

Cyclades-PR4000

Channel ISDN Menu CONFIG=>INTERFACE=>T1/E1(ISDN-PRI)=><*CHANNEL*> =>ISDN
or
Channel Signaling Menu CONFIG=>INTERFACE=>T1/E1(CAS)=><*CHANNEL*> =>SIGNALING

Parameter	Description
Connection Type	Applies only for ISDN. Whether the line will be used to receive (dial-in) or send (dial-out) messages, or both.
Phone # for this Channel	Applies for Dial-in, or Both. If a specific phone number is assigned to each channel, enter it here. Usually this does not happen.
Increment By	Applies only for CAS, when configuring a range or all channels. Increment by zero assigns all channels in the range the same phone number (set in the previous item). Increment by one assigns consecutive phone numbers to all channels in the selected range.
Digital Modem Profile ID	Applies for Dial-in, or Both. The modem profiles are defined in CONFIG =>SYSTEM =>MODEMS =>DIGITAL MODEM.
Automatic Dial Out	Applies only for ISDN and Dial-out. If *Yes*, the router will try to connect with the first destination listed in the dial-out table as soon as the ISDN line is up and synchronized. If *No*, the connection will occur only on demand.
Use DSP to Dial Out	Applies only for ISDN and Dial-out or Both. If *Yes*, the connection will be analog (modem). If *No*, digital.

The Authentication Menu Tree, which appears only for PPP and PPPCHAR encapsulation, is shown in Figure 8.3.

Authentication Menu CONFIG =>INTERFACE =>T1/E1=>*<CHANNEL>* =>AUTHENTICATION

Parameter	Description
Authentication Type	*Local* uses the list of users defined in CONFIG=> SECURITY=>USERS=>ADD. *Server* uses either Radius or Tacacs to authenticate the user. *Remote* is when this interface is considered to be the user and the **other** end of the connection performs the authentication
Username	Applies when Authentication Type is Remote. The username the remote device expects to receive.
Password	Applies when Authentication Type is Remote. The password the remote device expects to receive.
Authentication Server	Applies when *Authentication Type* is *Server*. Indicates that either a Radius or Tacacs server is used for validation. The location and other parameters of the server must be configured in CONFIG=> SECURITY. See section 4.3.
Authentication Protocol	Applies when *Authentication Type* is *Local* or *Server*. Either PAP or CHAP or both can be used for authentication.

Wizards were created to simplify the E1/T1 configuration for common applications. The Wizards Menu tree is shown in Figure 8.10, and its parameters are explained in the next table. The parameters set automatically are given in the tables that follow.

Cyclades-PR4000

Config

```
Interface ── T1/E1 ── <Channel> ── Wizards ──┬── TS Profile ──────────────┬── [Username]
                                             │                            ├── [Phone #]
                                             │                            └── [Digital Modem Profile ID]
                                             │
                                             ├── RAS Profile ─────────────┬── [Remote IP Address]
                                             │                            ├── [Phone #]
                                             │                            └── [Digital Modem Profile ID]
                                             │
                                             ├── LAN-to-LAN Profile ──────┬── [Primary IP Address]
                                             │                            ├── [Subnet Mask]
                                             │                            ├── [Secondary IP Address]
                                             │                            ├── [Subnet Mask]
                                             │                            ├── [Remote IP Address Type]
                                             │                            ├── [Remote IP Address]
                                             │                            ├── [Phone #]
                                             │                            └── [Digital Modem Profile ID]
                                             │
                                             └── Copy From Channel ─────── [Channel]
```
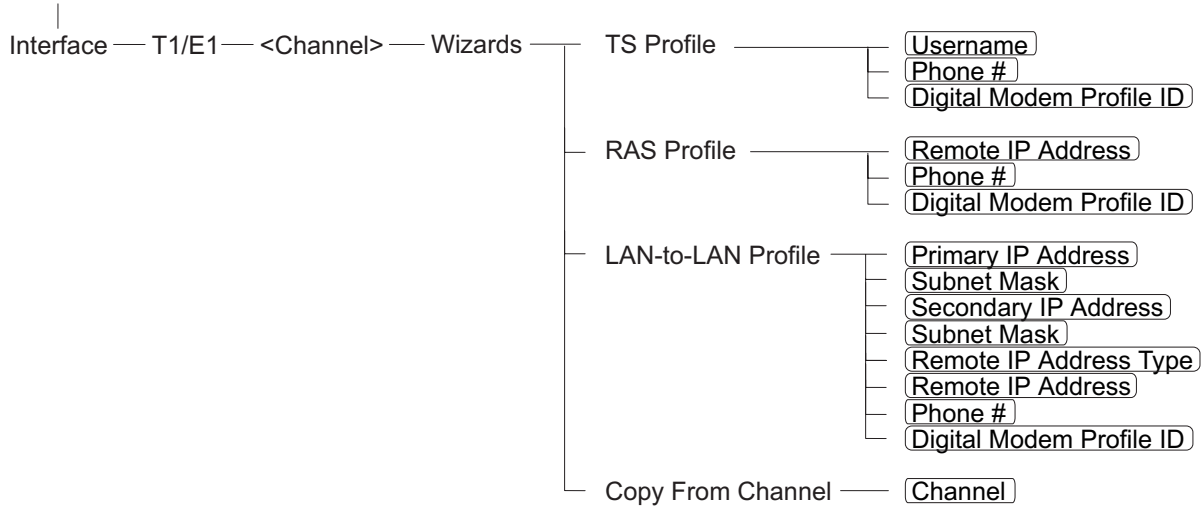
FIGURE 8.10 WIZARDS MENU TREE

Wizards Menu CONFIG =>INTERFACE =>T1/E1 =>*<CHANNEL>* =>WIZARDS

Menu Items	Description
TS Profile	Used to create a local host Terminal Server. For CCS, the only parameter is the Username. For CAS, the parameters are the Username, the Phone Number for the channel, and the Digital Modem Profile ID.
RAS Profile	Used to set up a PPP Remote Access Server using modems and dial-up lines. The *Remote IP Address* of the first port is the only parameter, for CCS. For CAS, the parameters are *Remote IP Address*, the *Phone Number* for the channel, and the *Digital Modem Profile ID*. If the Wizard is used for a range or all ports, the following ports will be the numbered consecutively.
Lan-to-Lan Profile	Used to connect two LANs. The only parameters are the *Primary IP Address*, the *Subnet Mask*, any *Secondary IP Addresses* and *Subnet Masks*, the *Remote IP Address Type* and the *Address*. For CAS, the parameters *Phone Number* and *Digital Modem Profile ID* are also requested.
Copy From Channel	Used to copy an entire configuration from one channel to another, while changing the IP address so that the ports are numbered consecutively.

The parameters automatically configured by the terminal server wizard are shown in Figure 8.11.

Encapsulation	CHAR
Device Type	Terminal
TCP KeepAlive	Inactive
Terminal Type	ANSI
Escape Session Character Code	1
Switch Session Character Code	11
Direct Login User	***
Dial-Out	Non-Automatic (CCS only)
Phone #	*** for CAS
Digital Modem Profile ID #	*** for CAS

FIGURE 8.11 PARAMETERS SET BY THE TS WIZARD

Cyclades-PR4000

The parameters automatically configured by the RAS wizard are shown in Figure 8.12.

Encapsulation	PPPCHAR
IP Protocol	Active
Interface	Unnumbered
Primary IP Address	***
Subnet Mask	*Depends on the IP
Remote IP Address Type	Fixed
Remote IP Address	***
IP MTU	1500
NAT - Address Scope	Global
ICMP Port	Inactive
Incoming Filter List	None
Outgoing Filter List None	None
Interface Transparent Bridge	Inactive
Bandwidth	0
IP Traffic Control List	None
Van Jacobson IP Header Compression	Disabled
LCP ECHO Requests	Enabled
Time Interval to Send Config Requests:	1
ACCM for Reception:	000A0000
Escape Session Character Code	1
Switch Session Character Code	11
Predictor Compression	Disabled
Inactivity Timeout	None
Link Authentication Method	PAP/CHAP Local Authenticator
Connection	Dial-In
Phone #	*** for CAS
Digital Modem Profile ID #	*** for CAS

FIGURE 8.12 PARAMETERS SET BY THE RAS WIZARD

Cyclades-PR4000

The parameters automatically set by the Lan-to-Lan wizard are shown in Figure 8.13.

Encapsulation	PPP
IP Protocol	Active
Interface	Numbered
Primary IP Address	***
Subnet Mask	***
Secondary IP Address	***
Secondary Subnet Mask	***
Remote IP Address Type	***
Remote IP Address	***
IP MTU	1500
NAT - Address Scope	Global
ICMP Port	Inactive
Incoming Filter List	None
Outgoing Filter List None	None
Interface Transparent Bridge	Inactive
Bandwidth	0
IP Traffic Control List	None
Van Jacobson IP Header Compression	Disabled
LCP ECHO Requests	Enabled
Time Interval to Send Config Requests:	1
ACCM for Reception:	00000000
Predictor Compression	Disabled
Inactivity Timeout	None
Link Authentication Method	None
Connection	Dial-In
Phone #	*** for CAS
Digital Modem Profile ID #	*** for CAS

FIGURE 8.13 PARAMETERS SET BY THE LAN-TO-LAN WIZARD

CHAPTER 9 NETWORK PROTOCOLS

The second step in most interface configurations is to choose which network protocol to use and assign values to the relevant parameters. At least one of IP, Transparent Bridge, or IPX (optional, and discussed in chapter 15) must be activated. Use the information provided below to set the parameters for each interface. The Ethernet network protocol menu includes IP bridging and is explained in chapter 5. The SWAN Network Protocol Menu is given in figure 7.1. Note that this menu varies slightly for each interface. Specific information on the options for each interface is provided in the CyROS Reference Guide in the chapter for the interface.

Config

Interface — SWAN — Network Protocol — IP

- Active
- Interface Unnumbered/Numbered
- Assign IP from Interface
- Primary IP address
- Subnet Mask
- Secondary IP Address
- Subnet Mask
- IP MTU
- NAT
- ICMP Port
- Incoming Rule List Name
- Detailed Incoming IP Accounting
- Outgoing Rule List Name
- Detailed Outgoing IP Accounting
- Routing of Broadcast Messages

Transparent Bridge

- Status
- Port Priority
- Incoming Rule List Name
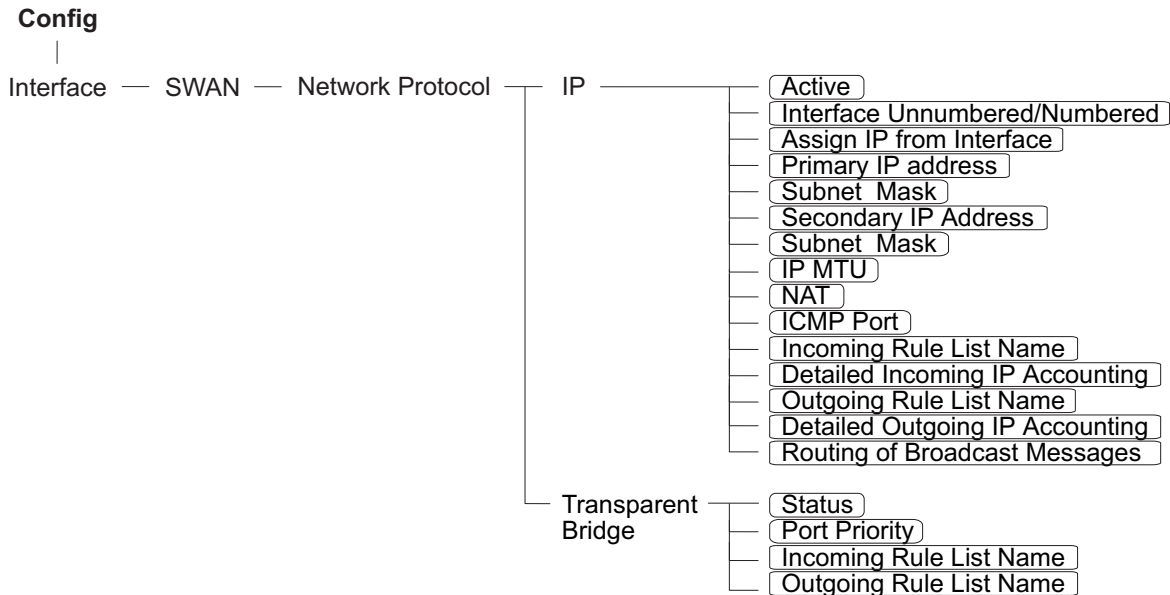- Outgoing Rule List Name

FIGURE 7.1 NETWORK PROTOCOL MENU TREE FOR THE SWAN INTERFACE

The IP Protocol

If the preset values provided by the operating system are accepted, the interface will work at a basic level. The most common options are explained in the following table.

Network Protocol (IP) Menu CONFIG=>INTERFACE=><LINK>=>NETWORK PROTOCOL=>IP

Parameter	Description
Active or Inactive	Activates this interface.
Interface Unnumbered	Unnumbered interfaces can be used for point-to-point connections.
Assign IP From Interface	Applies to *Unnumbered* interfaces. Applies the IP address of another router interface to this one.
Primary IP Address	Applies to *Numbered* interfaces. Address assigned to this interface.
Subnet Mask	Applies to *Numbered* interfaces. Subnet mask of the network.
Secondary IP Address	Applies to *Numbered* interfaces. Indicates a second (or third, etc. up to eight) IP address that can be used to refer to this interface. This parameter and the next are repeated until no value is entered.
Subnet Mask	Applies to *Numbered* interfaces. Subnet mask of *Secondary IP Address*.
Enable Dynamic Local IP Address	The terminal connected through PAD assigns an IP address to the router for purposes of their connection.
Remote IP Address Type	The computer connected through PAD or PPP sends its IP address in the negotiation package. *Fixed*: The IP address sent must match the number set in the next parameter. *Same Net*: The IP address sent must be an address in the network set in the next parameter. *Any*: The IP address can be any number that does not conflict with any local IP address. *None*: Any IP address is accepted. This is not recommended.
Remote IP Address.	If *Remote IP Address Type* not *None*. Used in conjunction with the previous parameter.
this table is continued	

Network Protocol (IP) Menu (Continued)

Parameter	Description
IP MTU	Assigns the size of the Maximum Transmission Unit for the interface. This determines whether or not a given IP datagram is fragmented.
NAT	Determines the type of IP address if NAT is being used. Use *Global* otherwise. See chapter 11 or the examples in chapter 4 for details on how to configure NAT.
ICMP Port	*Active* causes the router to send ICMP Port Unreachable messages when it receives UDP or TCP messages for ports that are not recognized. This type of message is used by some traceroute applications, and if disabled, the router might not be identified in the traceroute output. However, there are security and performance reasons to leave this option *Inactive*.
Incoming Rule List	Filter rule list for incoming packets. See chapter 12 for instructions on how this parameter should be set.
Detailed Incoming IP Accounting	Applies when a list is selected in the previous parameter. See explanation of IP Accounting later in this chapter. IP Accounting for a rule requires that the parameter CONFIG =>RULES LIST=>IP=>CONFIGURE RULES=>ADD RULE =>ALLOW ACCOUNT PROCESS also be *Yes*.
Outgoing Rule List Name	Filter rule list for outgoing packets. See chapter 12 for instructions on how this parameter should be set.
Detailed Outgoing IP Accounting	Applies when a list is selected in the previous parameter. See explanation of *Detailed Incoming IP Accounting*.
Routing of Broadcast Messages	Activating this parameter causes the router to route broadcast messages from the LAN to the WAN and vice-versa. An individual interface can be excluded by setting this parameter to *Inactive*, without effecting the broadcast of messages on the other interfaces.

The Transparent Bridge Protocol

The Transparent Bridge Protocol can be used in conjunction with either IP or IPX. A detailed explanation of its use appears in section 4.6 of the CyROS Reference Guide.

Transparent Bridge Menu CONFIG=>INTERFACE=>SWAN=>NETWORK PROTOCOL=>TRANSPARENT BRIDGE

Parameter	Description
Status	Activates the Transparent Bridge on this interface.
Port Priority	For the Spanning Tree Algorithm, a priority is given to each link in the router and to each router in the network. See CONFIG=>TRANSPARENT BRIDGE =>SPANNING TREE in the CyROS Reference Guide for more information.
Incoming Rule List Name	Transparent Bridge rule list name for incoming packets. Note: Rule lists for Transparent Bridge and IP are created separately. See section 4.7 in the CyROS Reference Guide for instructions on how this rule list is created.
Outgoing Rule List Name	Filter rule list name for outgoing packets. See section 4.7 in the CyROS Reference Guide for instructions on how this rule list is created.

CHAPTER 10 DATA-LINK PROTOCOLS (ENCAPSULATION)

Each encapsulation option is presented in a separate section in this chapter. Not all data-link protocols are available for all interfaces.

PPP (The Point-to-Point Protocol)

PPP is the only encapsulation option than can be either synchronous or asynchronous. It is important to choose between them in CONFIG =>INTERFACE =><LINK> =>PHYSICAL before entering the Encapsulation menu. The menu options depend on this choice. (Note: not all interfaces support both the synchronous and asynchronous modes. In this case, there is no physical menu.)

The configuration of the PPP data-link protocol is confined to one menu, CONFIG =>INTERFACE =><LINK> =>ENCAPSULATION =>PPP. Information about all the parameters appearing in this menu is provided in the table below. Not all parameters will appear for all interfaces.

PPP Menu CONFIG =>INTERFACE =><LINK> =>ENCAPSULATION =>PPP

Parameter	Description
MLPPP	Enables Multilink PPP on this interface. MLPPP is described in the CyROS Reference Guide for each interface that supports it.
Leased, Dial-in, etc.	Applies for *MLPPP = Yes*. Type of line used on this link.
Identification for This Bundle	Applies for *MLPPP = Yes* and *Dial-out* or *Leased*. An integer value.
Total Number of lines for This Bundle	Applies for *MLPPP = Yes*. Maximum number of links allowed in the bundle.
PPP Inactivity Timeout	Applies to asynchronous connections only. The connection is closed when data does not pass through the line for this period of time.
Enable Van Jacobson IP Header Compression	Allows the link to receive compressed packets. This type of compression is useful for low-speed links and/or small packets. It is not recommended for fast links, as it requires CPU time.
Transmit Compressed Packets	Applies when *Enable Van Jacobson IP Header Compression* is *Yes*. This parameter causes the link to send compressed packets.

PPP Menu (Continued)

Parameter	Description
Disable LCP Echo Requests	LCP (Link Control Protocol) messages are normally exchanged to monitor the status of the link. Disabling these messages reduces traffic, but the link then has no way of knowing if the other end is still connected.
Time Interval to Send Config Requests	Config Request messages are used to negotiate the parameters at the start of a PPP connection. For a slow line, this time should be increased to allow the reply to return to the sender. If not, the sender will assume it was lost and send another.
Edit ACCM	Applies to asynchronous connections only. Permits control character mapping negotiation on asynchronous links. This is useful when you need to send a control character as data (e.g. XON/XOFF, Crtl A, etc.) over an asynchronous link and do not want it interpreted by the modem or other device in the middle. The map is built up with the following commands. *Clear* – Resets the ACCM table toggle; *Toggle XON/XOFF* – Add XON/XOFF control characters to the ACCM table; *Toggle Char* – Add other control characters to the ACCM table, using their ASCII value. Typing the option once (for example, X), includes it in the table. Typing it again excludes it from the table. More details are given in the CyROS Reference Guide.
Enable Predictor Compression	Enables data compression using the Predictor algorithm. This feature should be enabled only if Cyclades' equipment is being used on both ends of the connection because there is no established standard for data compression interoperability. Data compression is very CPU-intensive, making this feature effective only for links running at speeds under 1Mbps. At higher speeds, the time necessary to compress data offsets the gains in throughput achieved by data compression.
Number of Bits for Compression	Applies when *Predictor Compression Enabled*. Sixteen is fastest, but 10 must be used if the router on the other end is a PathRouter, for compatibility.
Connection Type	Applies to asynchronous connections only. *NT-Serial Cable* is a direct connection to a Windows NT computer. This is necessary because NT requires a negotiation before the beginning of the PPP negotiation. *Direct* is used for other connections using cables or leased lines.

CHAR

The configuration of the CHAR data-link protocol is confined to one menu, CONFIG =>INTERFACE =><LINK> =>ENCAPSULATION =>CHAR. Information about all the parameters appearing in this menu is provided in the table below. Not all parameters will appear for all interfaces.

CHAR Encapsulation Menu   CONFIG=>INTERFACE =><LINK>=>ENCAPSULATION =>CHAR

Parameter	Description
Device Type	Determines whether a *Terminal*, *Printer*, or *Socket* device will be connected to this port.
TCP Keep Alive Timer	The delay between Keep Alive messages sent by TCP.
Terminal Type	For a *terminal*, *ANSI* is generally used. For a *printer*, *dumblp* is generally used.
Switch Session Character Code	Applies for *Terminal Device*. Control character used to switch sessions. 1 is Ctrl-A, 2 is Ctrl-B, etc. The value 254 disables this option.
Escape Session Character Code	Applies for *Terminal Device*. Control character used while in a telnet session, to return to the router menu without closing the session.
Username	Applies for a *Terminal Device*. Must be entered into the local user table first. See chapter 10. If this parameter is left blank, the user will have to enter a username
Wait for or Start a Connection	Applies for *Socket Device*. *Wait* is used when the remote application will start the communication. When *Start* is used, a connection is attempted as soon as the line is considered operational.
Destination Hostname	Applies for *Socket Device*. The remote hostname to which the socket will be connected, if the previous parameter was start. This name must have been defined in the host table. See chapter 10.
Filter Null Char after CR Char	Applies for *Socket Device*. Interprets a CR NULL sequence, received on a TCP connection, as CR (only).
Idle Timeout in Minutes	Applies for *Socket Device*. The connection is broken if no traffic passes in this time.
DTR ON Only if Socket Connection Established	Applies for *Socket Device*. If *False*, the Data Terminal Ready line is switched on when the router is booted.
Device Attached to This Port Will Send ECHO	Applies for *Socket Device*. *Yes* if the device attached to the socket will echo the chacters sent to it.

PPPCHAR

The configuration of the PPPCHAR protocol is contained in the menu CONFIG =>INTERFACE =><LINK> =>ENCAPSULATION =>PPPCHAR. The parameters for PPPCHAR are a combination of those for PPP and CHAR. See the tables describing the PPP and CHAR options for guidance in configuring this protocol.

HDLC

This data-link protocol is a proprietary alternative to PPP. It has only one parameter, the *HDLC Keepalive Interval*. This is the time interval between transmission of Keepalive messages. The receiver of these messages must send keepalive messages with the same frequency or will be considered inoperative.

Frame Relay

FR supports multiple connections over a single link. Each data link connection (DLC) has a unique DLCI (data link connection identifier). This allows multiple logical connections to be multiplexed over a single channel. These are called Permanent Virtual Circuits (PVCs). The DLCI has only local significance and each end of the logical connection assigns its own DLCI from the available local numbers.

Traffic Control based on Data Link Connection
Traffic Control as described in chapter 14 can also be performed on a Frame Relay interface for each permanent virtual connection. The parameters in the *Add DLCI* menu are used in the same manner as those described in chapter 14. More details are available in the CyROS Reference Guide.

STEP ONE

The first step is to set the general Frame Relay parameters, those applying to all DLCs. This is done in the Frame Relay Menu. The parameters are shown in the table below. Most of these depend on the standards used by the Frame Relay Network Provider.

The Local Management Interface (LMI) Protocol provides services not available in simple Frame Relay. It is used for controlling the connection between the user and the network. It monitors this link, maintains the list of DLCs, and sends status messages about the PVCs. A separate virtual circuit is created to pass this information (DLCI 0).

Frame Relay Menu CONFIG=>INTERFACE=><LINK>=>ENCAPSULATION =>FRAME RELAY

Parameter	Description
SNAP IP	Indicates that the Sub-Network Access Protocol should be used. The router on the sending end must be using the same header type (NLPID or SNAP) as the router on the receiving end. See the CyROS Reference Guide for more information.
LMI	Selects the Local Management Interface specification to be used. *ANSI*, *Group of Four* (defined by the vendors that first implemented Frame Relay), *Q933a* (defined by ITU-T), and *None* (used for a dedicated FR connection without a network).
T391	Interval between the LMI Status Enquiry messages.
N391	Full Status Polling Counter. Full Status Enquiry messages are sent every N391-th LMI Status Enquiry message.
N392	Error Threshold. The network counts how many events occur within a given period and considers an interface inactive when the number of events exceeds a threshold. *N393* is the number of events to be considered and N392 the number of errors within this period. If *N392* of the last *N393* events are errors, the interface is deemed inactive. A successful event is the receipt of a valid Status Enquiry message
N393	Monitored Events Count. See the description of *N392*. This value must be larger than N392.
CIR	Committed Information Rate, in percentage of total bandwidth (bandwidth defined in CONFIG=>INTERFACE=>SWAN =>TRAFFIC CONTROL =>GENERAL =>BANDWIDTH). Traffic above this rate may be discarded if the network is congested.
Bandwidth Reservation	Enables traffic control per DLCI. Traffic control options appear in the Add DLCI Menu.
FRF-12	When set, indicates the size of the FRF012 fragment in bytes (range: 40-1600).

STEP TWO

After configuring the general parameters, each DLC must be defined. An example will be used to demonstrate the procedure.

A public Frame Relay network connecting offices in São Paulo, Rio de Janeiro, Salvador, and Recife is shown in Figure 11.1. Each router will have a routing table pairing destination network with router interface and gateway. A Frame Relay Address Map is also created (either statically or dynamically) to associate each DLCI with the destination router IP.

For the router in Salvador, the Frame Relay address map will look like this:

DLCI	IP
11	200.1.1.1
21	200.1.1.4
81	200.1.1.3

Data link connections are defined in the *Add DLCI* menu, which appears at the end of the Frame Relay parameter list. It can be reached by passing through all parameters or by using the <ESC> key at any point in the parameter list.
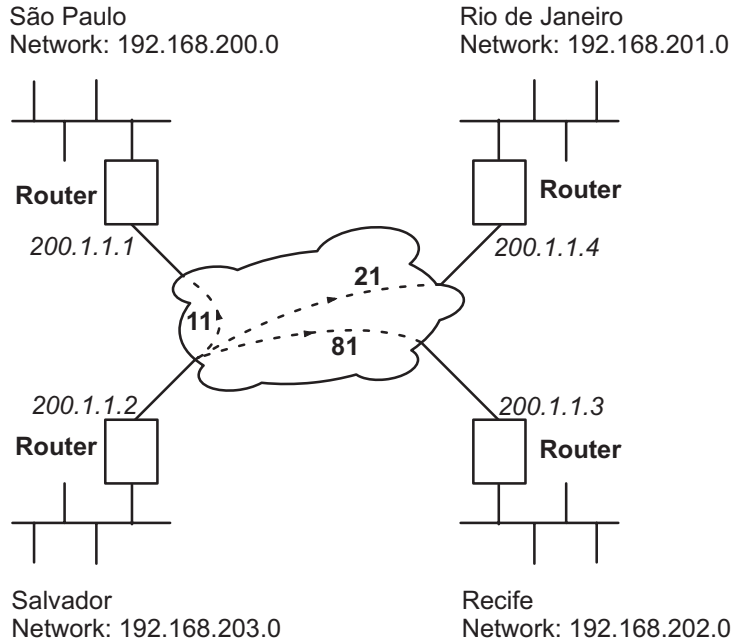
FIGURE 8.1 PERMANENT VIRTUAL CIRCUITS BETWEEN OFFICES

Add DLCI Menu CONFIG=>INTERFACE =><LINK> =>ENCAPS =>FRAME RELAY =><*ESC*> =>ADD DLCI

Parameter	Description
DLCI Number	Used to identify the DLC. This number is supplied by the Public Frame Relay network provider. The DLCIs are stored in a table which can be seen with the *L* command.
Frame Relay Address Map	Determines the method used for mapping the remote IP address to the Permanent Virtual Circuit. *Static* maps one IP address to this DLCI. *Inverse ARP* maps the IP address dynamically, in a manner similar to the ARP table.
IP Address	Applies when *Frame Relay Address Map* is *Static*. Provides the IP address to be used for static address mapping.
Enable Predictor Compression	Enables data compression using the Predictor algorithm. This feature should be enabled only if Cyclades' equipment is being used on both ends of the connection because there is no established standard for data compression interoperability. Data compression is very CPU-intensive, making this feature effective only for links running at speeds under 1Mbps. At higher speeds, the time necessary to compress data offsets the gains in throughput achieved by data compression.
Number of Bits for Compression	Applies when *Predictor Compression Enabled.* Sixteen is fastest, but 10 must be used if the router on the other end is a PathRouter, for compatibility.
DLCI Priority Level	This is the equivalent of CONFIG=>RULES LIST=>IP =>CONFIGURE RULES=>ADD RULE=>FLOW PRIORITY LEVEL. See the section on traffic control in chapter 12.
Reserved Bandwidth	This is the equivalent of CONFIG=>RULES LIST=>IP =>CONFIGURE RULES=>ADD RULE=>RESERVED BANDWIDTH. Defines what percentage of the CIR (Committed Information Rate) for an interface will be set aside for this DLC. See the section on traffic control in chapter 12.
Bandwidth Priority Level	This is the equivalent of CONFIG=>RULES LIST=>IP =>CONFIGURE RULES=>ADD RULE=>BANDWIDTH PRIORITY LEVEL. See the section on traffic control in chapter 12.

To edit the DLCI table, use the list command (CONFIG=>INTERFACE=><LINK>=>ENCAPSULATION =>FRAME RELAY=>L) to discover the number CyROS has assigned to each table entry. It will not be the same as the DLCI.
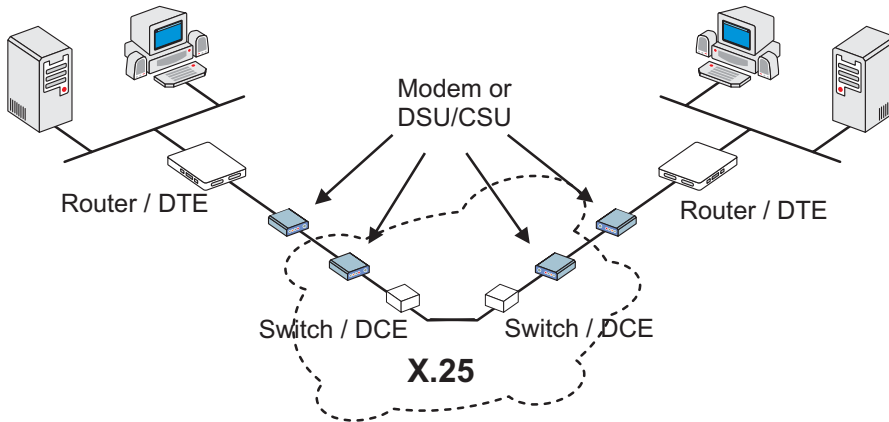
FIGURE 8.2 PUBLIC X.25 NETWORK EXAMPLE

X.25

A Cyclades Router can act either as a DTE (Data-terminal Equipment) connected to a public X.25 network or as a DTE or DCE (Data circuit-terminating Equipment) as part of a private X.25 network. The first case is discussed in this chapter. The second case is described in the CyROS Reference Guide. Both Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs) can be defined. A PVC requires that two DTEs be permanently connected.

STEP ONE
First, the general X.25 protocol parameters are set in the X.25 Menu. A detailed description of the X.25 parameters and their values for the example is provided in the table below.

X.25 Menu   CONFIG=>INTERFACE=><LINK>=>ENCAPSULATION =>X.25

Parameter	Description
X.121 (Local DTE) Address	Address assigned to this interface (provided by the public X.25 Network Provider). Can be up to 15 digits.
Switch Mode Active	Causes the Router to act as a switch.
Incoming Calls Received Over the Other X.25 Links With Unknown Destination DTE Can be Forwarded Through This Link	Applies when Switch Mode is *Active*.
Suppress Calling Address	**Public X.25 Network:** This parameter must be chosen according to the guidelines given by the Public X.25 Network provider. When activated, the sender's Local DTE address is not included in the Call Request Message.
Inactivity Timeout	Time until connection is automatically terminated by the router if there is no traffic.
Configure as DTE or DCE	As mentioned above, the router can act either as the recipient of information (*DTE*), or as the passer-on of information (*DCE*). **Public X.25 Network:** Both routers are DTEs.
Number of Virtual Circuits	Indicates the maximum number of virtual circuits (total of PVCs and SVCs) allowed on this interface. The maximum is 64.
Number of Permanent Virtual Circuits	Indicates the number of permanent virtual circuits that will be connected through this interface. This maximum is also 64.
this table continued	

X.25 Menu (Continued)

Parameter	Description
Layer 3 Window Size	The layer 3 (packet) level window represents the number of sequentially numbered packets that can be sent before an acknowledgement must be received. This number may be negotiated if the Window Size Facility is utilized (see last parameter in this table).
Layer 2 Window Size	The layer 2 (frame) level window represents the number of sequentially numbered frames that can be sent before an acknowledgement must be received. The frame numbers are independent of the packet numbers.
Packet Size	The packet size to be sent across the interface. This number may be negotiated if the Packet Size Facility is utilized (see last parameter in this table).
Number of Retries N2	Number of times an information frame can be resent, without response, before the link is considered down.
TL	Time the frame level waits for an acknowledgement for a given frame before re-sending it.
T2	Time that can elapse, after receiving a frame, until the router must send an acknowledgement.
T21	Call Request response Timer. After this time has elapsed, the DTE sends a Clear message.
T23	Clear Request response Timer. After this time has elapsed, the DTE retransmits the Clear message.
Negotiable Facilities	Initiates facility negotiation during virtual circuit creation.
Send Facility	Determines which facilities are negotiated during virtual circuit creation: *Packet size* is part of the flow control parameters negotiation, *Throughput* is part of the throughput class negotiation, and *N3 Window* (Level 3 Window Size, above) is part of the flow control parameters negotiation.

STEP TWO

The next step is to create a static routing table associating each remote X.121 address with an IP address or a TCP Socket location. This is done in the Add DTE menu, which appears at the end of the X.25 parameter list. It can be reached by passing through all X.25 parameters or by using the <ESC> key at any point in the parameter list.

X.25 Add DTE Menu   CONFIG=>INTERFACE=><LINK>=>ENCAPSULATION =>X.25=>***<ESC>=>***Add DTE

Parameter	Description
Type of Logical Address	IP Address or TCP Socket. Users that intend to use the TCP Socket option should see the CyROS Reference Guide.
IP Address	Applies for *IP Address Type*. IP Address of remote DTE device.
X.121(DTE) Address	Address of remote DTE device.
VC Number	Number assigned to this circuit, if it is a PVC. For SVCs, the value should be zero.
Enable Predictor Compression	Applies for *IP Address Type*. Enables data compression using the Predictor algorithm. This feature should be enabled only if Cyclades' equipment is being used on both ends of the connection because there is no established standard for data compression interoperability. Data compression is very CPU-intensive, making this feature effective only for links running at speeds under 1Mbps. At higher speeds, the time necessary to compress data offsets the gains in throughput achieved by data compression.
Number of Bits for Compression	Applies when *Predictor Compression Enabled*. Sixteen is fastest, but 10 must be used if the router on the other end is a Cyclades PathRouter, for compatibility.

X.25 with PAD (Packet Assembler/Disassembler)

PAD acts as a protocol converter, allowing a user to access the packet-switched network via a serial terminal. This asynchronous connection is then converted into synchronous communication with the router and the network beyond (using the telnet application available in the router). Please see the CyROS Reference Guide for information about this Encapsulation option.

CHAPTER 11 ROUTING PROTOCOLS

Routing Strategies

Routing can be done either statically or dynamically.

Static Routing

Static routing is recommended when the network contains a small number of routers and other equipment. When a system is simple and without redundant links, static routing is the simplest option. Even with some redundant links, a multilink circuit can be created for semi-dynamic routing behavior. Multilink circuits are described in section 4.4 of the CyROS Reference Guide.

Dynamic Routing

Dynamic routing is recommended when the network contains a large number or routers with redundant links between them. RIP and OSPF are currently available in the Power Router line.   RIP is simpler to configure and is appropriate for systems that are stable (links do not go down often). OSPF is more complicated to configure, requires much more CPU, and is not necessarily available in all equipment in a network. A mixture of RIP, OSPF, and static routes is often used.

BGP-4 is a dynamic routing protocol used to route packets on the Internet. It is used in addition to the protocols RIP and OSPF or static routing.

Static Routes

Routers used in very small or simple networks may use static routes as the primary routing method. When RIP or OSPF are used, some static routes may still be needed. Configuration of static routes will be explained using two examples.
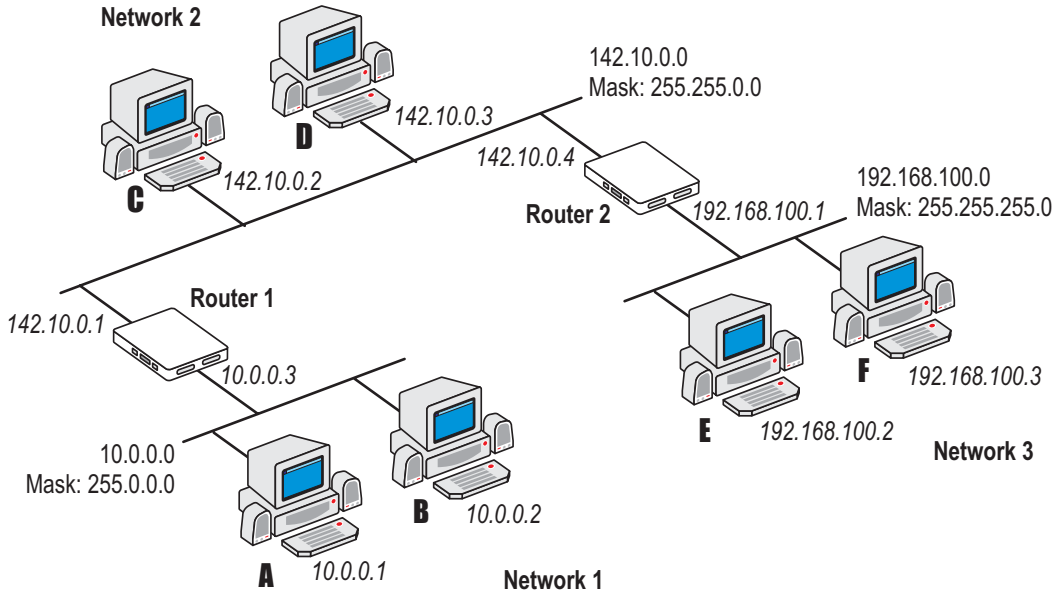
FIGURE 12.1 STATIC ROUTING EXAMPLE 1

In the first example, three networks are connected by 2 routers. The routing table for router 1 will automatically include servers A,B,C, and D, as they are direct links. A static route must be created for access to Network 3. This type of route, a *Gateway* route, tells the router that any message not intended for hosts A, B, C or D should be sent to Router 2. Details are given in the parameter table that follows.
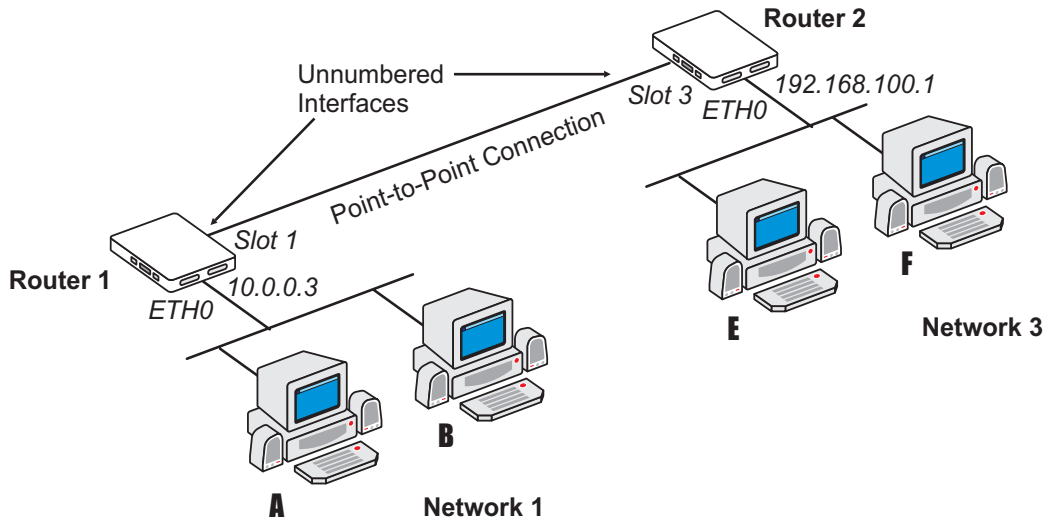
FIGURE 12.2 STATIC ROUTING EXAMPLE 2

Figure 12.2 shows another static routing example to explain the *Gateway* or *Interface* parameter. Between the two routers is a point-to-point connection. Another network could be created, but is not necessary. Both routers can be assigned unnumbered interfaces, because everything that leaves one router is sent to the other.

To define static routes, enter the menu CONFIG =>STATIC ROUTES =>IP =>ADD ROUTE. A description of the parameters in this menu, with the configuration for Router 1 in the examples above, is given in the table that follows.

Add Static Route Menu CONFIG =>STATIC ROUTES =>IP =>ADD ROUTE

Parameter	Description
Destination IP Address	Address that route will lead to. To configure a default route, type "default" for this parameter, otherwise enter 0.0.0.0 in both this and the next parameter. **Both Examples** -- for the static route between Router 1 and Network 3, the IP address is 192.168.100.0.
Subnet Mask	**Both Examples** -- To access all hosts in Network 3, its mask, 255.255.255.0, is used.
Gateway or Interface	**Example 1** -- the route is to a gateway. **Example 2** -- the route is to an interface since unnumbered interfaces are being used.
Gateway IP Address	Applies only when previous parameter is *Gateway*. It must be an address visible to the router. In **Example 1**, it is 142.10.0.4.
Interface	Applies only when previous parameter is *Interface*. Select the port (Ethernet or slot N) that will be unnumbered. In **Example 2**, it is Slot 1.
Metric	Relative cost of this link. Generally measured in number of routers between two IP addresses. **Both Examples** -- 1.
Is This a Backup Route?	Indicates that this route is used as a backup in a multilink circuit. See section 4.4 for more information about multilink circuits.
OSPF Advertises This Static Route	Static routes defined in the router can be advertised by OSPF. Both this parameter and the parameter CONFIG=>IP=>OSPF=>GLOBAL=>ADVERTISE STATIC ROUTES must be set to *Yes* for the route to be advertised.
External Metric	Applies when *OSPF Advertises This Static Route* is set to *Yes*. Defines the metric that will be advertised by OSPF.
External Metric-Type	Applies when *OSPF Advertises This Static Route* is set to Yes. For *Type 1*, the total metric of this route is composed of the internal metric (inside the autonomous system) and the external metric (provided in the previous parameter). For *Type 2*, the total metric of this route is the value provided in the previous parameter.

RIP Configuration

CyROS supports three basic types of RIP:

1 RIP1 [RFC 1058]
2 RIP2 with broadcast (compatible with RIP1) [RFC 1723]
3 RIP2 with multicast [RFC 1723]

The primary difference between RIP1 and RIP2 is that only RIP2 advertises subnet masks and next hops. If the network contains equipment that understands only RIP1 packets, then RIP1 or RIP2 with broadcast should be used. See RFC 1723, item 3.3 for more details. If only RIP2 is used, RIP2 with multicast is recommended.

Unlike static routes RIP is configured on each interface rather than in a global menu. The menu is the same for all interfaces and its parameters are presented in the table below.

RIP Menu CONFIG =>INTERFACE =>*<LINK>* =>ROUTING PROTOCOL =>RIP

Parameter	Description
Send RIP	Causes the router to transmit RIP messages.
Listen RIP	Causes the router to accept RIP messages.
RIP2 Authentication	Applies if *RIP2* was chosen in the first two options. Activates RIP message authentication with a password.
RIP2 Authentication Password	Applies if *RIP2 Authentication* is *Active*. Password used for both received and transmitted RIP messages.

OSPF

The OSPF (Open Shortest Path First) routing protocol is significantly more complicated than RIP. The determination of which protocol is better suited to a given network is beyond the scope of this manual. An example network using OSPF is given in Figure 12.3.
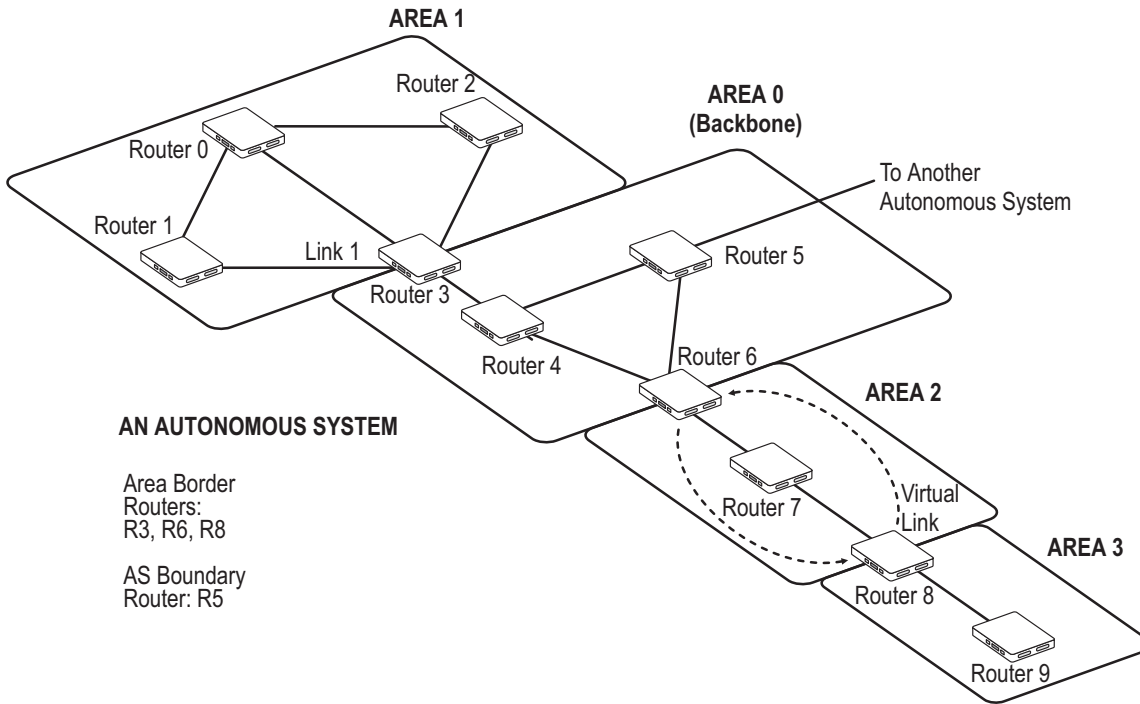

FIGURE 12.3 OSPF EXAMPLE

First, some definitions:

- An **Autonomous System (AS)** is a portion of the network that will use a single routing strategy. It is made up of a backbone area and optionally of non-backbone areas.
- **OSPF Areas** are sub-systems that have identical routing databases. An area generally has no knowledge of the routing databases of other areas.
- The **Backbone** connects areas and contains any routers not contained in another area.
- An **Area Border Router** connects areas and contains a separate database for each area it is contained in.
- An **Autonomous System Boundary Router (ASBR)** connects Autonomous Systems. The other Autonomous System does not necessarily need to use OSPF.

STEP ONE
If using OSPF for the first time, sketch the network and determine which routers will make up the backbone and each area. Determine if each router is an area border router or an autonomous system boundary router.

OSPF Configuration on the Interface

STEP TWO
Contrary to most other protocols in CyROS, OSPF must first be configured on each interface, then configured in the CONFIG =>IP =>OSPF menu. Enter into each interface and set the parameters listed in the table.

OSPF Menu CONFIG =>INTERFACE =>*<LINK>* =>ROUTING PROTOCOL =>OSPF

Parameter	Description
OSPF on This Interface	Activates OSPF. *Enable Inactive* is used to temporarily disable the OSPF protocol without erasing the parameters set below. This is useful when OSPF is first configured, as the general parameters must be set afterwards in CONFIG=>IP =>OSPF and OSPF cannot function without them.
Parameters that apply only when *OSPF on This Interface* is *Disabled*.	
Advertise This Non-OSPF Interface	Causes the router to include this interface in its advertisements through other interfaces (as an external route).
This table is continued.	

OSPF Menu (continued)

External Metric	Defines the metric that will be advertised by OSPF.
External Metric Type	For *Type 1*, the total metric of this route is composed of the internal metric (inside the autonomous system) and the external metric (provided in the previous parameter). For *Type 2*, the total metric of this route is the value provided in the previous parameter.
Parameters that apply only when *OSPF on This Interface* is *Enable* or *Enable Inactive*.	
Area ID	Identifies the area to which the interface belongs. Areas are created here, then later defined in CONFIG=>IP=>OSPF =>AREA. Has the format of an IP address, but is not linked to any IP address in the system. Small OSPF networks will typically have only one area (the backbone area represented by 0.0.0.0).
Router Priority	Priority used by OSPF in multicast networks to elect the designated router. A priority of 1 will make this router the most likely to be chosen. A priority of 2 will make it second most likely. Set it to 0 (zero) if this router should never be the designated router.
Transit Delay in Seconds	Estimated transit time in seconds to route a packet through this interface. Use the preset value (1) or increase the number for slow links
Retransmit Interval *	Time in seconds between link-state advertisement retransmissions for adjacencies belonging to this interface.
Hello Interval *	Time in seconds between the hello packets on this interface.
Dead Interval *	Inactivity time (seconds) before a neighbor router is considered down.
Poll Interval *	Time in seconds between the hello packets sent to an inactive, non-broadcast, multi-access neighbor.
Password *	String of up to 8 characters used to authenticate OSPF packages. The use of this password is enabled in CONFIG=>IP=>OSPF=>AREA=>AUTHENTICATION TYPE
Metric	Defines the cost for normal service. For consistent routing, this parameter should be determined in the same manner for all routers in the OSPF Area. Normally, metric cost is defined as an inverse function of interface throughput (e.g. 1 for 100Mbps, 10 for 10Mbps, 65 for T1, 1785 for 56kbps, etc.).
Advertise Secondary IP Address	Causes the router to advertise additional addresses assigned to this interface. These are configured in CONFIG => INTERFACE =><LINK> =>NETWORK PROTOCOL =>IP.

* Inside a given area, these 4 parameters should be the same for all routers.

OSPF Global Configurations

STEP THREE

After completing the OSPF interface configuration for all interfaces (even those that will not use OSPF), navigate to the OSPF Menu, CONFIG=>IP=>OSPF. Enter into the OSPF Global Commands menu and set the parameters as indicated in the table below.

OSPF Global Commands Menu CONFIG =>IP =>OSPF =>GLOBAL

Parameter	Description
OSPF Protocol	Enables OSPF on all interfaces.
Router ID	Assigns a unique ID to the router for use by the OSPF protocol. It must be one of the router's IP addresses.
AS Boundary Router	An Autonomous System Boundary Router (ASBR) can convert external routes into OSPF routes. Which external routes is determined through the following parameters. In the figure, only Router 5 is an ASBR.
The following parameters apply only to *Autonomous System Boundary Routers*.	
Originate Default Gateway Advertisement	Router will advertise itself as the Default Gateway (DG).
Default Gateway External Metric	Applies when *Originate Default Gateway Advertisement* is set to *Yes*. Defines the metric that will be advertised by OSPF.
Default Gateway External Metric-Type	Applies when *Originate Default Gateway Advertisement* is set to Yes. For *Type 1*, the total metric of this route is composed of the internal metric (inside the autonomous system) and the external metric (provided in the previous parameter). For *Type 2*, the total metric of this route is the value provided in the previous parameter.
Advertise RIP Routes	Routes learned through the RIP protocol will be converted to OSPF as external routes.
RIP External Metric	Applies when *Advertise RIP routes* is set to *Yes*. Defines the metric that will be advertised by OSPF.
This table is continued.	

OSPF Global Commands (Continued)

Parameter	Description
RIP External Metric-Type	Applies when *Advertise RIP routes* is set to *Yes*. For *Type 1*, the total metric of this route is composed of the internal metric (inside the autonomous system) and the external metric (provided in the previous parameter). For *Type 2*, the total metric of this route is the value provided in the previous parameter.
Advertise Non-OSPF interfaces	A router can have both OSPF and non-OSPF interfaces. This option causes the router to advertise when these non-OSPF interfaces are up or down. When OSPF is disabled on an interface, the parameter CONFIG=>INTERFACE =><*LINK*> =>ROUTING PROTOCOL =>OSPF =>ADVERTISE THIS NON-OSPF INTERFACE must also be set to *Yes* for the interface to be advertised.
Advertise Static Routes	Static routes defined in the router will be converted to OSPF. Note that static routes can be configured individually as advertised or not in the parameter CONFIG=>STATIC ROUTES=>IP=>ADD ROUTE=>OSPF ADVERTISES THIS STATIC ROUTE. Both parameters must be *Yes* for the route to be advertised.

STEP FOUR
The next step is to define the areas created in step two. This is done in the OSPF Area Menu.

Area Menu CONFIG =>IP =>OSPF =>AREA

Parameter	Description
Area ID	Has the format of an IP address, but is not linked to any IP address in the system. Use the CONFIG=>IP=>OSPF=>L option to see which areas have been defined, and use the area ID here.
Authentication Type	Simple password authentication can be used in OSPF. The authentication type should be the same for all routers in an OSPF Area. If used, the password for each interface is set in CONFIG=>INTERFACE=><*INTERFACE*>=>ROUTING PROTOCOL =>OSPF =>PASSWORD.
This table is continued.	

Area Menu (continued)

Area Range N Status	An Area Border Router (ABR) advertises link states for all networks within the area. The number of such advertisements can potentially be reduced by condensing different IP networks into a single range.
Area Range N Net Address	Applies when *Area Range N Status* is *Active*. Sets the network IP address for the range.
Area Range N Mask	Applies when *Area Range N Status* is *Active*. Sets the network IP mask for the range.

STEP FIVE

The CONFIG =>IP =>OSPF =>NEIGHBORS menu is required if the router uses OSPF over non-broadcast multi-access interfaces such as X.25 and Frame Relay. If this is the case, set the parameters described in the following table.

Neighbors Menu CONFIG=>IP =>OSPF =>NEIGHBORS

Parameter	Description
Interface	Link for which neighbors will be defined. In the OSPF example, consider link 1 of Router 3.
Neighbor's IP	The router ID of the neighboring router. For Router 3, link 1, use the router ID of router 1.
Neighbor's Status	*Enable* includes link in OSPF database. *Enable Inactive* leaves link in OSPF database, but router at end of link (Router 1 in this case) no longer passes OSPF information. *Disable* deactivates neighbor link and erases *Neighbor's IP*.
Neighbor's Priority	Priority used by OSPF in multicast networks to elect the designated router. A priority of 1 will make this router the most likely to be chosen. A priority of 2 will make it second most likely. Set it to 0 (zero) if this router should never be the designated router. An example can be seen in Area 1 in the figure -- Router 1 should never be the Designated Router because it does not have a direct link to Router 2. Either Router 0 or Router 3 should be chosen.

STEP SIX

It is not always possible to connect all areas directly to the backbone. When an area is connected to the backbone only through another area, two virtual links must be created. One from the backbone to the unattached area and one from the unattached area to the backbone. If this occurs in the network containing the router, enter the Virtual Links Menu to configure this link. In the table listing the parameters, the link between Area 3 (router 8) and the backbone is used as an example.

Virtual Links Menu CONFIG =>IP =>OSPF =>VIRTUAL LINKS

Parameter	Description
Transit Area ID	ID of the OSPF Area sandwiched between this router and the backbone. In the figure, area 2 is the area used to link Router 8 with the Backbone. This ID has the form of an IP address.
Neighbor's ID	Router ID of router at end of virtual link. In the example, this will be Router 6.
Virtual Link Status	Activates the virtual link.
Parameters available only when *Virtual Link Status* is *Active*.	
Transit Delay in Seconds	Estimated transit time in seconds to route a packet from Router 8 to Router 6. Use the preset value (1) or increase the number for slow links.
Retransmit Interval in Seconds*	Time in seconds between link-state advertisement retransmissions for adjacencies belonging to this interface.
Hello Interval in Seconds*	Time in seconds between the hello packets on this interface.
Dead interval in Seconds*	Inactivity time (seconds) before a neighbor router is considered down.
Password*	String of up to 8 characters used to authenticate OSPF packages. The use of this password is enabled in CONFIG =>IP=>OSPF=>AREA=>AUTHENTICATION TYPE.

* Inside a given area, these 4 parameters should be the same for all routers. In the example virtual link, they should be the same as those used for the backbone.

BGP-4 Configuration

The BGP-4 routing protocol is used for routing on the Internet, performed between Autonomous Systems (ASs). An autonomous system is defined as:

· A set of routers and networks under the same administration.
· An interconnected network, where no router is reachable solely through a path exterior to the AS

Each AS is identified by a 16-bit AS number. This number is supplied by the service provider.

Steps
1. Complete the Global Parameters
2. Register the neighbors of the autonomous system, the routers with which it this router exchanges information.

At this point, the BGP-4 protocol is up and running. All remaining steps are fine tuning to improve performance and reduce the size of the routing table.

If some routes that might be received are undesired, they can be filtered as they enter (or leave) so that they are not placed in the routing table (or are not propagated to other autonomous systems).

This requires the following three steps:
3. Create an Access List
4. Add rules to the Access List
5. Return to the Neighbor configuration and match each list to the neighbor it should be applied to.

In some cases, a route should be accepted, but with changes determined by policies defined by the system administrator. In this case, a route map should be created indicating which of the path attributes of the incoming (or outgoing) message should be changed. This route map can be associated with a filter so that only specific rules will be altered. The steps are the following:
6. Create a route map/sequence pair
7. Edit the neighbor definition to link it to the new route map

The last option is to aggregate the addresses contained in the local autonomous system in order to present an aggregated route to the outside world. This is done in the last step.

   8. Aggregate the addresses contained in the AS.

The steps defined above will now be clarified.

STEP ONE
The global parameters apply to the router's AS. Classless Inter-Domain Routing (CIDR) Address notation is used instead of the normal IP Address and Subnet mask notation. Both are shown in Figure 12.4.
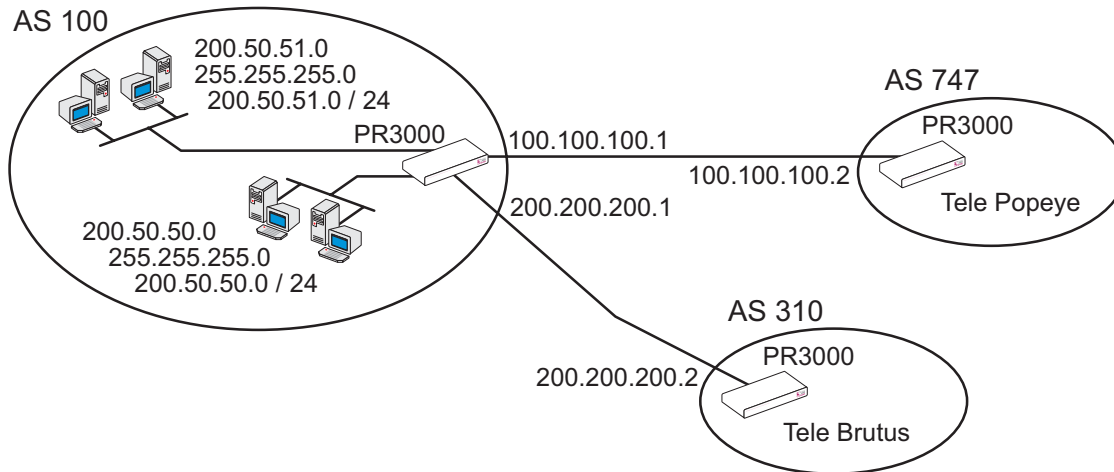
FIGURE 12.4 EXAMPLE SYSTEM WITH PR3000 IN AS 100 BEING CONFIGURED

CONFIG=>IP=>BGP4=>GLOBAL

Parameter	Description
BGP4 Protocol	Activates the protocol.
Local AS Number	This number is assigned by the service provider.
Router Identifier	Usually the same as the Router ID, one of the interface IP addresses
Cluster Identifier	Only used when this router is used as a router reflector.
Default Local Preference	Value of the attribute "local pref" used by IBGP.
Accept Connections From All Peers	Allows BGP connections from neighbors that have not been specified in the Neighbors Menu.
Advertise Direct Routes	Allows the removal of the interface routes from the list of routes to be advertised. In the example these would be 100.100.100.1, 200.200.200.1 and the LAN interface IP address.
Advertise Static Routes	Allows the removal of static routes from the list of routes to be advertised.
Advertise RIP Routes	Allows the removal of routes learned via RIP from the list of routes to be advertised.
Advertise OSPF Routes	Allows the removal of routes learned via OSPF from the list of routes to be advertised.

The BGP network menu allows registration of the IP Addresses contained in the AS. This will mark these routes as IGP instead of EGP or incomplete in the path origin attribute.

CONFIG=>IP=>BGP4=>BGP NETWORK=>ADD

Parameter	Description
Network Address	Network IP address of network to be added.
Network Mask (bitlen)	Mask in CIDR format.

STEP TWO

The neighbor menu identifies the routers inside and outside the AS that will communicate with the router via BGP-4. Each update message exchanged between routers contains path attributes. How these path attributes are manipulated by the router when routes are received or sent to each neighbor is determined here.

CONFIG=>IP=>BGP4=>NEIGHBOR=>ADD

Parameter	Description
Name	A string to facilitate identification of the Neighbor. In the example above, the names Popeye and Brutus could be used.
IP Address	The IP address at the other end of the connection. For AS 747, the value is 100.100.100.2.
Description	Another string to identify the Neighbor.
AS Number	The AS number assigned to the neighbor.
Maximum routes	When set, indicates the maximum number of routes accepted from this neighbor.
Source IP Address	When this number is set, the protocol accepts TCP/BGP connections only when the destination IP is this value. For Popeye, the value would be 100.100.100.1.
Passive	Causes the router to not initiate BGP connections with this neighbor.
Transparent-AS	*Yes* causes the router to NOT include its own AS number in the "AS Path" path attribute for update messages sent to this neighbor.
Transparent-NextHop	*Yes* causes the router to NOT alter the "NextHop" path attribute for update messages sent to this neighbor.
NextHop Self	*Yes* causes the router to change the NextHop path attribute for update messages sent to this neighbor. The value is replaced by the Source IP Address set above.
Route Reflector Client	Indicates that this router is a route reflector and the neighbor is a route reflector client.
Weight	Indicates the relative importance of the routes received from this neighbor. Routes with greater weights are chosen over routes with lesser weights.
Maximum-Prefix	When set, indicates the maximum number of routes that the router will accept in a single update message from this router.
Holdtime	When a message is not received from this neighbor for the holdtime, the neighbor is considered inactive.
This table is continued.	

CONFIG=>IP=>BGP4=>NEIGHBOR=>ADD (continued)

Keepalive	Interval between keepalive messages sent to this neighbor.
Connection Retry Time	When a connection with this neighbor is broken, the router try to reconnect with frequency 1 divided by the Connection Retry Time.
Start Time	Time delay before router tries to connect
Incoming Distribution Access List Name	Applies a distribution access list to update messages received from this neighbor.
Outgoing Distribute Access List Name	Applies a distribution access list to update messages sent to this neighbor.
Incoming Filter Access List Name	Applies a filter access list to update messages received from this neighbor.
Outgoing Filter Access List Name	Applies a filter access list to update messages sent to this neighbor.
Incoming Community Access List Name	Applies a filter access list to update messages received from this neighbor.
Outgoing Community Access List Name	Applies a filter access list to update messages sent to this neighbor.
Incoming Route Map Number	Applies a route map to update messages received from this neighbor.
Outgoing Route Map Number	Applies a route map to update messages sent to this neighbor.
Neighbor Alias Address	Additional address used by the other router.

STEP THREE

Figure 12.5 shows an example of a route that could be filtered out. The preferred route from 5 to 1 is through 4, with 6 serving as a reliable backup. Any route received from neighbor 2 which includes 5 will probably be a duplicate of the equivalent route received from 4. In order to reduce the size of the routing table, all routes received from 2 than contain 5 can be filtered out of incoming update messages.
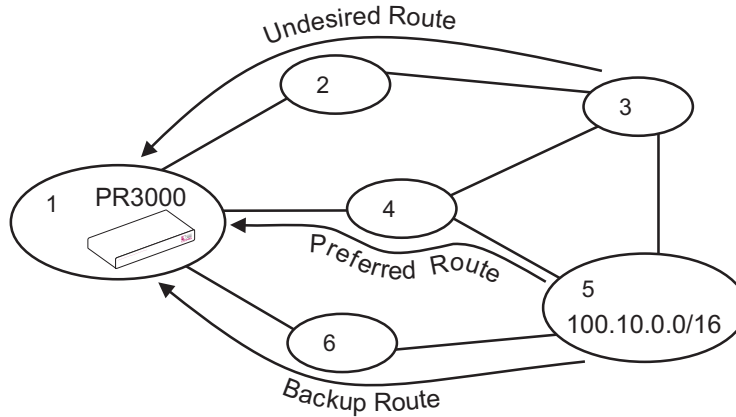
FIGURE 12.5 MULTIPLE ROUTES CONTAINING AS 5

CONFIG=>IP=>BGP4=>ACCESS LIST=>ADD

Parameter	Description
Access List Name	Name assigned to list, to indicate which interface and direction it applies to. A typical name for the example is from_two_p.
Access List Type	The AS Path type allows filtering by AS number; the Dist BGP type allows filtering by IP address and the Community BGP type allows filtering by community. In the figure, the filtering can be done based either on AS 5 or the address 100.10.0.0/16
Rule Status	Enables the rule.
Default Scope	If the default of the list is permit, the default of each rule must be deny and the corresponding rule must define which routes must be discarded. If the default of the list is deny, the default of each rule must be permit and the corresponding rule must define which routes will be accepted (with all others being discarded).

STEP FOUR

An access list needs at least one rule. The example in Figure 12.6 shows three access lists, each one with several rules. Each neighbor can be assigned up to 6 access lists, as seen in step 2.
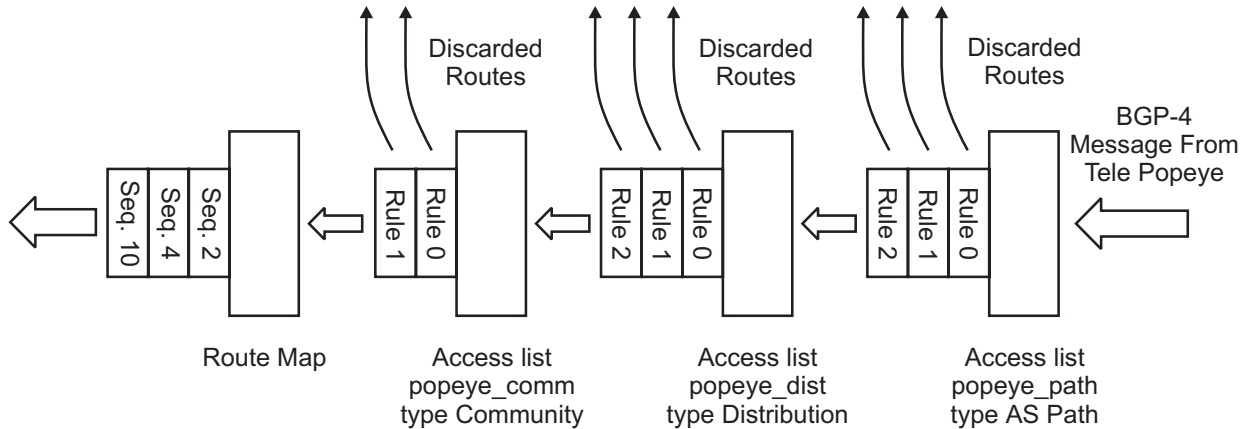
FIGURE 12.6 UPDATE MESSAGE ARRIVING FROM TELE POPEYE PASSING THROUGH 3 FILTERS AND A ROUTE MAP

An update message arriving from the neighbor called Popeye in step 2 will pass through the filters assigned to it in the Neighbor Menu. The figure shows the case where the scope of the list is permit and that of the rules is deny. Each rule causes routes to be discarded until finally the shortened message arrives at the route map (if one has been configured for this neighbor).

CONFIG=>IP=>BGP4=>ACCESS LIST=>CONFIGURE RULES=><ACCESS LIST NAME>=>*ADD*

Parameter	Description
Rule Status	Enables the rule.
Scope	See explanation of this parameter in step 3.
Rule AS Position	Applies only for *Access List Type* equal to AS Path. Limits the search on AS number to a particular position in the route. For the example in Figure 12.5, Any would be the correct choice because AS 5 will appear in the middle or the beginning of the route.
Rule AS Number	Applies only for *Access List Type* equal to AS Path. Applies the rule to routes containing this AS number, with the restriction given in the preceding parameter.
Rule Distr. Search Type	Applies only for *Access List Type* equal to Dist BGP. *Exact* filters rules that match the IP Address/Mask pair exactly. *Refine* matches more specific routes.
Rule Distr. Address	Applies only for *Access List Type* equal to Dist BGP. Applies the rule to routes with this IP number and the mask defined in the next parameter.
Rule Distr. Mask Bitlen	Applies only for *Access List Type* equal to Dist BGP. The shortened mask that is used with the IP address defined in the previous parameter.
Community	Applies only for *Access List Type* equal to *Community BGP*. Applies this rule to the community number entered or to well-known communities defined in RFC 1997, BGP Communities.

STEP FIVE
Each access list can be applied to more than one interface. The access list parameters in the Neighbor Menu for the appropriate neighbor should be set now, since the access lists did not exist during step two.

STEP SIX
A route map can either apply to all routes not discarded by the access lists, as shown in Figure 12.6, or to routes filtered by a particular access list, as shown in Figure 12.7.
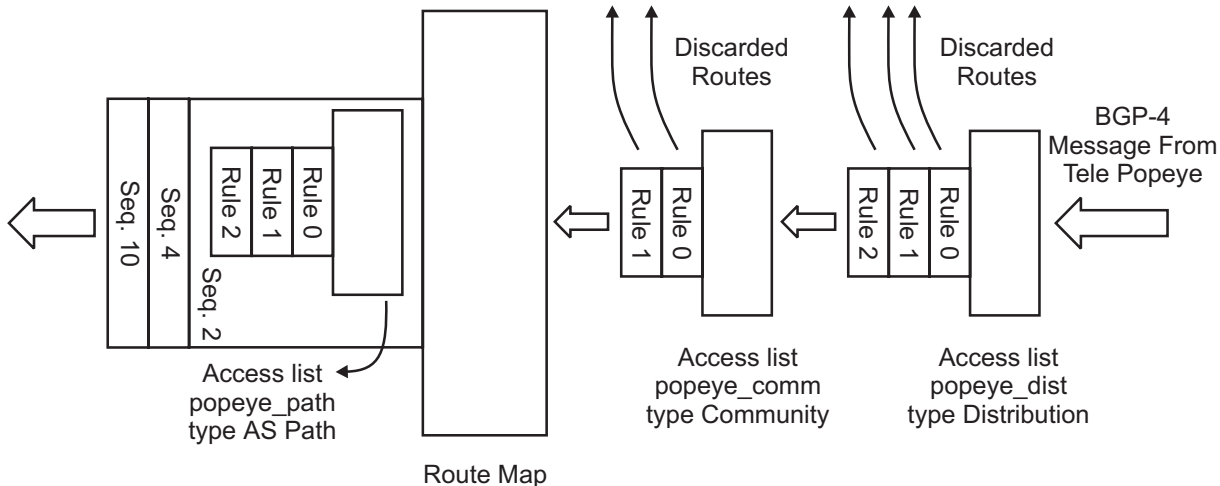
FIGURE 12.7 ROUTE MAP ASSOCIATED WITH AN ACCESS LIST

In figure 12.7, the access list popeye_path is associated with sequence 2 of Route Map 1. Instead of the access list causing the disposal of the routes that match its rules, it causes the application of the route map.

CONFIG=>IP=>BGP4=>ROUTE MAP=>ADD

Parameter	Description
Route Map Number	Identifies the route map
Sequence Number	Identifies the sequence within the route map. The numbers need not be consecutive.
Match List Name	Associates an access list with this sequence, as shown in the figure above.
Weight	Alters the weight used to determine the best path. This value replaces the importance assigned to the route by the weight parameter in the neighbor configuration.
Origin, Set Nexthop, Set Metric, Set Local Preference, Set Atomic Aggregate, Set Aggregate AS number, Set AS Path, AS Path Prepend, AS Path AS-SET	These parameters modify the path attributes with the same name in the update message.

STEP SEVEN
The neighbor definition should now be changed again to include the new route map. This is done in the Neighbor Menu described in step 2.

STEP EIGHT
This last step permits aggregation of networks inside the AS to simplify routing tables. In the example in Figure 12.4, the two networks can be aggregated to form one network with the IP address/Mask of 200.50.50.0/23.

CONFIG=>IP=>BGP4=>AGGREGATE ADDRESSES=>ADD

Parameter	Description
Number	An ID for reference.
Address	The aggregated address. In the example, 200.50.50.0.
Mask (bitlen)	The mask for the aggregated address. In the example, 23.
AS Set	*Yes* causes the route to be tagged with the AS Set path attribute. Otherwise, the AS Sequence path attribute is assigned.
Summary Only	Yes removes all more specific routes, leaving only the aggregated form. No maintains both the individual and aggregated routes.

CHAPTER 12 CYROS, THE OPERATING SYSTEM

This chapter explains various operating system features that are not covered in other chapters:

- creation of the host table
- creation of user accounts and passwords
- IP Accounting

Creation of the host table

CyROS allows identification of hosts by name. In the menu CONFIG =>SYSTEM=>HOSTS, each host is assigned a number (1 to 32), and a host name (a maximum of 8 characters). The IP address to be associated with this host name and the port to be used for telnet is then requested. This host name can be used in aplications like ping and telnet, and in some other configuration menus.

Another way to identify hosts by name is to configure access to a DNS Server. This is done in the menu CONFIG =>IP =>DNS CLIENT. The domain name where the router is located and two DNS Server IP addresses are the only parameters.

Creation of user accounts and passwords

Four users are preset:

1 **super** with the password surt,
2 **usr** with no password,
3 **auto** with no password, and
4 **pppauto** with no password

Other users can be created and the user "usr" can be assigned a password. The password of the super user should be changed as soon as possible. The menu CONFIG=>SECURITY=>USERS allows addition, deletion, and modification of the list of users. The parameters are:

- User Name,
- Password,
- User Type: Super, Usr, Auto, or PPPAuto,
- User Status: Disabled or Enabled,
- Hosts 1 through 4 (the host names entered here must already exist in the host table).
- Automatic login name for hosts 1 through 4 (only for user of type *auto*)

Then the main menu items for this user are determined:

- Telnet,
- Ping,
- Traceroute,
- PPP,
- SLIP.

Lastly, any restrictions as to how the user may log in are defined:

- Console,
- Terminal,
- PPP Terminal,
- Telnet,
- PAD Terminal.

The *super* user has access to all menus. The *usr* user is shown a menu, upon sucessful login, with the items chosen in the user's profile. The *pppauto* user is connected directly to the user via PPP. No menu appears. The *auto* user is connected via telnet directly to the host specified as host 1 in the user profile. If an *automatic login name* is indicated when the auto user is configured, the user is logged in to the remote host directly (though a password may be necessary, depending on the remote host configuration).

IP Accounting

IP Accounting is used to count the total number of packets allowed (or not) to pass through an interface. Statistics are given for packets that meet the criterions defined in a rule. (Traffic Rules are not supported). To see all packets, a special rule list permitting everything can be defined. Rules are described in chapter 14.

Two versions of the IP account table are available for viewing. The result of INFO =>SHOW ACCOUNT TABLE =>SUMMARY is shown below for four filter rules.

```
IP Accounting Table

Interface   Direction    Filter List   Rule   Bytes   Packets
Ethernet    Outgoing     generic       0      24876   3072
Ethernet    Incoming     generic       0      49254   3358
slot 3      Outgoing     swan3out      17     21362   3223
slot 3      Incoming     swan3in       15     32563   3131
```

Detailed information can be accessed via SNMP.

To use IP Accounting, two parameters must be set. When a rule is created, the parameter CONFIG =>RULES LIST =>IP =>CONFIGURE RULES =>ADD RULE =>ALLOW ACCOUNT PROCESS must be *Yes*. Additionally, when applying a rule to an interface, the parameter CONFIG =>INTERFACE =>ETHERNET =>NETWORK PROTOCOL =>IP =>DETAILED INCOMING /OUTGOING IP ACCOUNTING must also be Enabled.

CHAPTER 13 NAT (NETWORK ADDRESS TRANSLATION)

NAT exists to convert local IP addresses into Internet "global" IP addresses. Internet IP addresses are assigned by Internet providers. Due to the explosion of the internet, these numbers are scarce. Certain ranges of IP addresses are reserved for internal use only — they may not have a direct connection to the Internet. These are used as local IP addresses. Figure 11.1 shows an example of the utility of NAT:
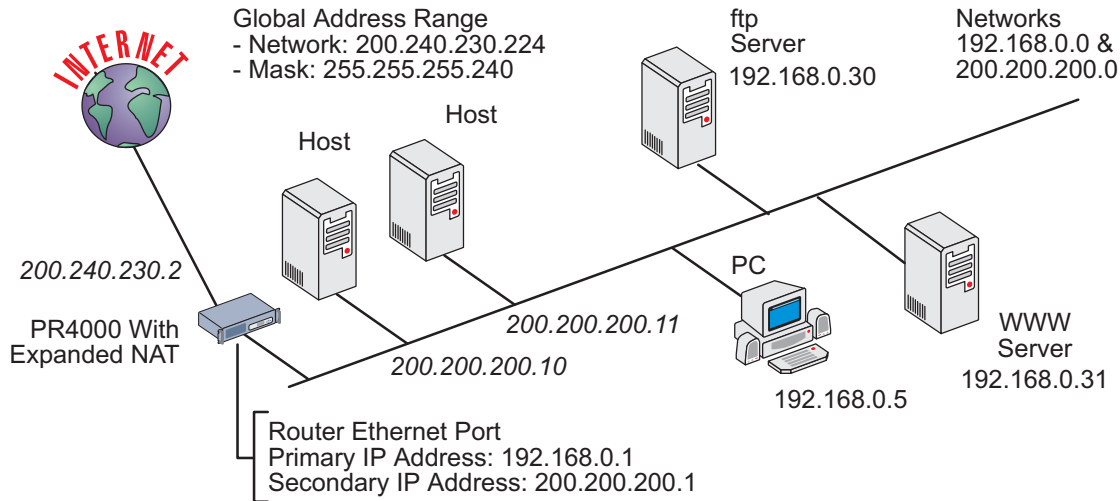
FIGURE 11.1 NAT EXAMPLE

In this example, the company has:
- 14 global IP addresses available for NAT, 200.240.230.225 to 200.240.230.238,
- Two networks connected to the router via the Ethernet Interface, one of which will be translated,
- Two servers that are accessed via the same global IP address, assigned statically.

Cyclades-PR4000

There are two types of NAT available in CyROS -- Normal NAT and Expanded NAT. This chapter describes Expanded NAT. A description of Normal NAT appears in Chapter 4 of the CyROS Reference Guide.

?	What is the difference between Expanded and Normal Mode NAT? The Normal Mode is a previous implementation of NAT used in the Power Router line. It has been maintained for backward compatibility. Expanded NAT provides static translation not only from one IP address to another, but from one IP address/port pair to another IP address/port pair.

As a preview, after configuring the router as shown in the example, CONFIG =>SECURITY =>NAT =>L will display:

```
NAT Enabled
NAT mode Expanded
Port map translation Enabled
UDP Timeout (min) 5
DNS Timeout (min) 1
TCP Timeout (min) 1440
TCP flags Timeout (min) 1

NAT Global Addresses

#    address range
1    200.240.230.225 to 200.240.230.238

NAT Local Addresses

#    address range
1    192.168.0.0      255.255.255.0       translated
```

```
NAT Static Translation Table

#   Global address  /   port     local address   /  Port    Protocol
1   200.240.230.225 /    20      192.168.0.30    /   20       TPC
2   200.240.230.225 /    21      192.168.0.30    /   21       TPC
3   200.240.230.225 /    80      192.168.0.31    /   80       TPC
```

Types of Address Translation

In **dynamic address translation**, a pool of global IP addresses is loosely related to a pool of local IP addresses. Mapping of one onto the other is done dynamically whenever a computer on the local network requests a connection to the external network. When the connection is broken, the global IP address is returned to the pool. Hosts connected via dynamic address translation must initiate all connections with the external network.

In **static address translation**, one global IP address (or global IP address / port pair) is permanently associated with one local IP address (or global IP address / port pair). In the example, the web server is connected to one of the global IP addresses for services on port 80, reducing the IP address pool to 13. Static address translation is used when the connection with the external network is to be initiated from either side — external or internal.

Translation may be done in two ways:

1 Address translation only – each global address is assigned to a single local address when necessary. In the example, there are only 13 global addresses available and more than 13 hosts . With this type of translation, only 13 servers can connect to the Internet at any given time.

2 Port and address translation — the UDP/TCP port and local IP address are translated as a pair. With this type of translation, only ONE global address is needed. All hosts can be mapped to the same global IP address. This can be used in our example to allow all hosts in the 192.168.0.0 network access to the Internet at the same time.

An overview of the NAT menu is shown in the table below.

NAT Menu CONFIG =>SECURITY =>NAT

Menu Option	Description
General	Parameters for enabling NAT and choosing the NAT Mode. Also includes port translation option.
Global Address	The first and last IP addresses in the range. In the example, these numbers are 200.240.230.225 and 200.240.230.238.
Local Address	The local network IP address and network mask, and whether or not the network should be translated. In the example, these numbers are 192.168.0.0 and 255.255.255.0.
Static Translation	Defines a static translation between a global IP address/port pair and a local IP address/port pair. In the example, three such pairs are defined.
Timeout	Definition of inactivity timeouts for UDP, DNS, and TCP dynamic NAT translations.

STEP ONE
The first step in the configuration of NAT is to enable NAT and choose the NAT Mode (Normal or Extended). Only the extended mode is discussed in this chapter. The normal mode is a previous version of NAT maintained for backwards compatability. See chapter 4 of the CyROS Reference Guide for information about the Normal Mode.

NAT Menu CONFIG =>SECURITY =>NAT =>GENERAL

Menu Option	Description
NAT Status	Enables NAT.
NAT Mode	Provides a choice between the previous NAT version (the *Normal Mode*) and the new Extended NAT version.
Disable Port Translation	Disables/enables NAT with port translation. If this parameter is changed while the router is in use, all the active translations are destroyed, and their entries are removed from the translation table.

STEP TWO

The parameters in the Timeout Menu are explained in more detail below. The preset values should be appropriate for most applications.

Timeout and Options Menu CONFIG =>SECURITY =>NAT =>TIMEOUT AND OPTIONS

Parameter	Description
UDP Timeout	Inactivity time required before a UDP translation is removed from the translation table. An entry is created in the translation table the first time a UDP packet passes through the interface. Five minutes is a reasonable time.
DNS Timeout	Inactivity time required before a DNS translation is removed from the translation table.
TCP Timeout	Inactivity time required before a TCP translation is removed from the translation table. This time should be relatively long, because under normal conditions TCP connections are formally disconnected with FIN (No more data from sender) or RST (Reset Connection) flags.
TCP Flags Timeout	Inactivity time required, after the receipt of a FIN, RST, or SYN (Synchronize sequence numbers) flag, before a TCP translation is removed from the translation table. This time can be relatively short, because after the TCP connection has been closed, there is no further need for its address translation.

STEP THREE

The next step is to define the global address range to which the local addresses will be translated. This is done in the menu CONFIG =>SECURITY =>NAT =>GLOBAL ADDRESSES =>ADD RANGE. The *First IP Address* in the example in Figure 11.1 is 200.240.230.225, while the *Last IP Address* is 200.240.230.238.

The local address ranges must also be entered into the router in the menu CONFIG =>SECURITY =>NAT =>LOCAL ADDRESSES =>ADD RANGE. Here, the Network IP Address (192.168.0.0 in the example) and Network Mask (255.255.255.0 in the example) are entered. Since this range is to be translated, the parameter *Should This Range be Translated* should be set to *Yes*. In the example, the network 200.200.200.0 is not to be translated. This can be configured by adding a new range and setting the translation parameter to *No*, or by simply not adding the range.

Chapter 13 - NAT   **121**

STEP FOUR
If static translations are to be performed, as described in the example, the parameters in the Static Translation Menu must be set. A brief explanation of each parameter is given in the table.

Static Translation Menu CONFIG =>SECURITY =>NAT =>STATIC TRANSLATION => ADD ENTRY

Parameter	Description
Global IP Address	One of the addresses assigned by the Internet access provider and included in one of the NAT global address ranges.
Protocol	TCP, UDP, ICMP, or any protocol.
Global Port	The port to be translated on the WAN side. When a request comes in on port 80 for IP 200.240.230.225 in the example, it is sent to the server with IP 192.168.0.31, port 80
Local IP Address	The IP address of the server (on the LAN, in the example) which is translated to an Internet IP address.
Local Port	The port to be translated on the LAN side. When a request comes in on port 80 for IP 200.240.230.225 in the example, it is sent to the server with IP 192.168.0.31, port 80.

STEP FIVE
After the NAT menu parameters have been set, the NAT property in the Network Protocol Menu of each interface must be configured. In the example, the IP Address of the Ethernet interface is not assigned dynamically. The parameter CONFIG =>INTERFACE =>ETHERNET =>NETWORK PROTOCOL =>IP=>NAT - DYNAMIC ADDRESS ASSIGNMENT should be set to *Inactive*. The IP address of the interface connecting the router to the Internet is also assigned by the super user in the example, rather than dynamically. The parameter CONFIG =>INTERFACE =>SWAN =>NETWORK PROTOCOL =>IP=>NAT - DYNAMIC ADDRESS ASSIGNMENT would also be set to *Inactive*.

After NAT has been configured and is running, the menu option INFO =>SHOW STATISTICS =>NAT will show Network Address Translation Statistics.

CHAPTER 14 RULES AND FILTERS

There are four basic types of rules:

1 IP filter rules,
2 Radius rules (actually a combination of previously defined IP filter rules),
3 traffic control rules, and
4 transparent bridge rules (similar to IP filter rules, but for applications that use a transparent bridge).

IP filter rules and traffic control rules will be covered in detail in this chapter. See section 4.7 of the CyROS Reference Guide for more information about all four types of rules.

As an introduction, the Rules List Menu Tree is presented in Figure 12.1. First, a rule list is created and named. Second, rules are added to the list and defined.

Configuration of IP Filters

IP Filter rules are a very important part of a network's firewall. They permit packets into or out of the network depending on the source and destination IP addresses, the source and destination ports, the protocol used, and the ACK bit for TCP packets. The Syslog can be used to monitor the packets that meet the rules applied in this menu.

Config — Rules List — IP — Add Rule List —————————————— Rule List Name
                     Rule Status
                     Rule List Type
                     Default Scope
     Edit Rule List — *Same as Add Rule List*   Incoming Rule List Name
                     Outgoing Rule List Name
                     Linked Rule List Name N

     Configure Rules — Rule List Name   Insert as Rule Number
             Add Rule   Rule Status
                     Scope
                     Rule Priority Level
                     Reserved Bandwidth
                     Bandwidth Priority Level
                     Protocol
                     Source IP Operator
                     IP Address Start Mask
                     IP Address Start
                     IP Address End
                     Destination IP Operator
                     IP Address Start Mask
                     IP Address Start
                     IP Address End
                     Source Port Operator
                     Source Port Start
                     Source Port End
                     Destination Port Operator
                     Destination Port Start
                     Destination Port End
                     Allow TCP connections
                     Allow Account Process

             Delete Rule — Rule to delete
     Clear Rule List   Edit Rule ——— *Same Parameters as Add Rule*
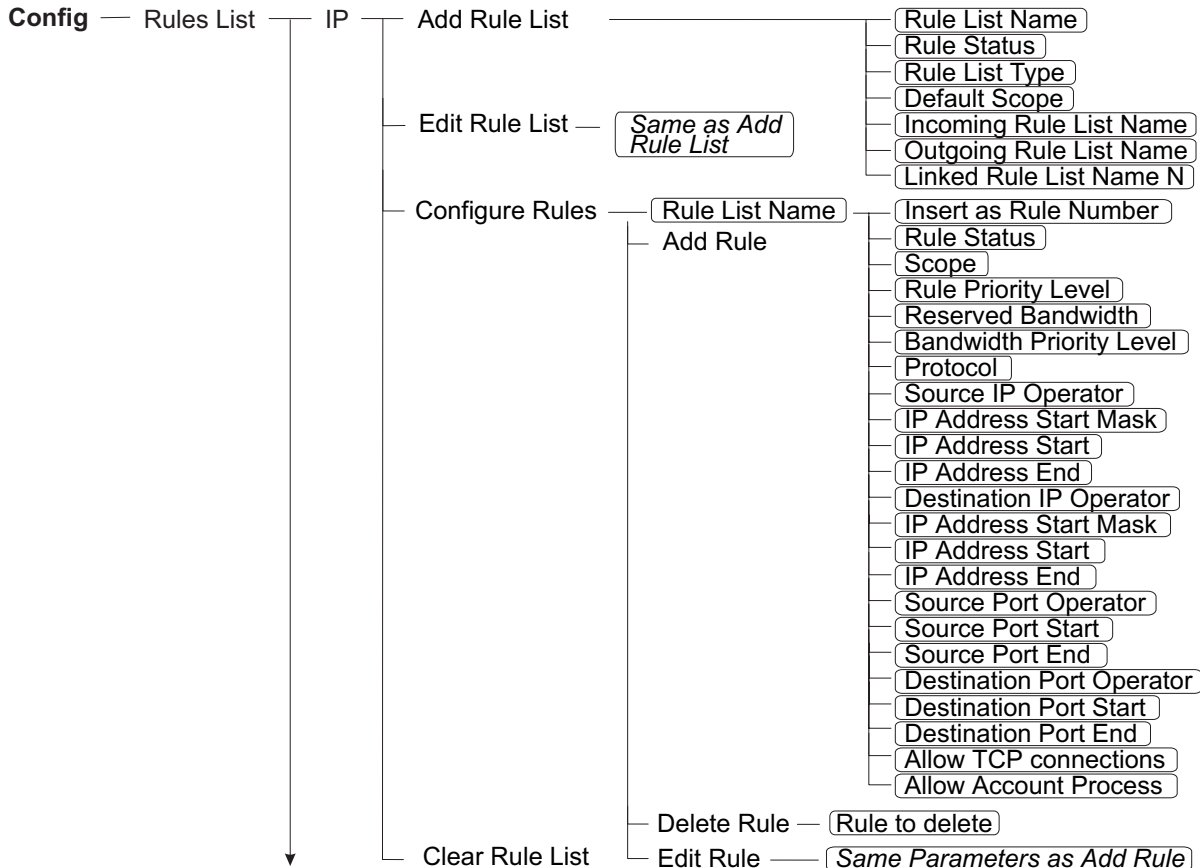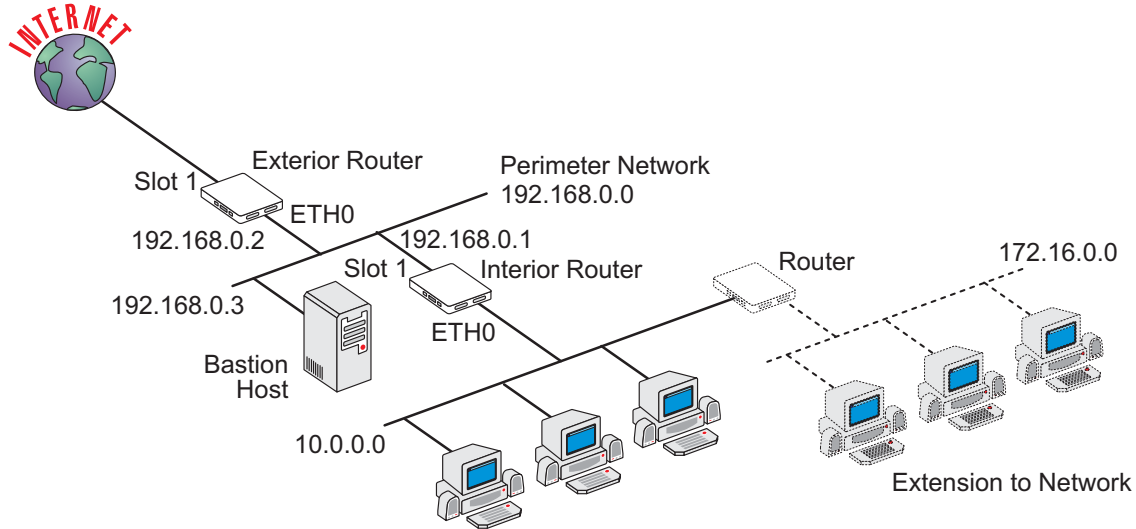
FIGURE 12.1 THE RULES LIST MENU TREE

FIGURE 12.2 FIREWALL EXAMPLE

Figure 12.2 will be used to show how both an exterior router and an interior router would be configured using the filters available in CyROS.

Exterior Router

The exterior router is the network's first defense against attacks. For this reason, it is reasonable to prohibit all packets except for those explicitly allowed. This is done by choosing the *Default Scope* to be *Deny*. Thus, ALL desired traffic must be expressly allowed by the rules in the rule list.
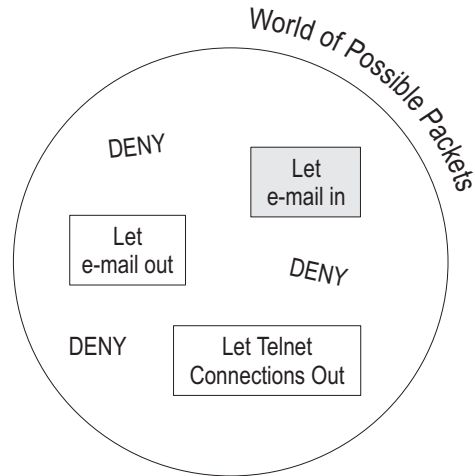

FIGURE 12.3 DENY AS DEFAULT SCOPE

In Figure 12.3, a conceptual equivalent of the interface is shown. All packets except those which fall into the holes in the ball will be denied entry in to or out of the network.

Cyclades-PR4000

Steps necessary to activate filtering on the exterior router in the example:

1 There are two interfaces with two directions each. Filtering on link 1 requires the creation of two rule lists, called `exterior_in` and `exterior_out`. Create them using the menu CONFIG =>RULES LIST =>IP =>ADD RULE LIST and the following parameters:
   Rule List Type = Filter
   Default Scope = Deny
   Linked Rule List Name = None

2 Create the rules for each rule list in the order in which they should be evaluated. The order is important and mis-ordering the rules can cause unexpected results. This is done in the menu CONFIG =>RULES LIST =>IP =>CONFIGURE RULES. The parameters for rules 0 and 1 in the example are shown in Figure 12.4.

3 Link the rule lists to the respective interface parameters in the menu CONFIG =>INTERFACE =>*<INTERFACE>* =>NETWORK PROTOCOL =>INCOMING/ OUTGOING RULE LIST NAME. exterior_in should be set as the incoming rule list name and exterior_out should be set as the outgoing rule list name.

`Exterior_in, rule 0,` allows a remote computer to connect to the bastion host using the TCP protocol on its SMTP port. `Exterior_out, rule 0,` allows the Bastion Server to RESPOND to the connection started by the remote computer. To send e-mail *out*, two more rules would be needed. If all the router needs to do is receive e-mail, the configuration is done. If not, other "holes" must be created in the deny ball.

Cyclades-PR4000

The configuration for "Let e-mail in" is shown in the following figure (obtained by selecting CONFIG =>RULES LIST =>IP =>L in the menus):

```
Rules Lists
Rule List Name   Rule        Default    List      Linked
                 Status      Scope      Type      Rule
                                                  List
exterior_in      Enabled     Deny       Filter
exterior_out     Enabled     Deny       Filter


Filter_list Name exterior_in
Rule 0
Status                     Enabled
Scope                      Permit
Protocol                   TCP
Source IP Operator         None
Destination IP Operator    Equal
Destination IP start       192.168.0.3
Destination IP Mask        255.255.255.255
Source Port  Operator      Greater than
Source Port Start          1023
Destination Port  Operator Equal
Destination Port Start     SMTP
TCP connections allowed    Y
Account Process allowed    N
```

Cyclades-PR4000

```
Filter_list Name exterior_out
Rule 0
Status                     Enabled
Scope                      Permit
Protocol                   TCP
Source IP Operator         Equal
Source IP start            192.168.0.3
Source IP Mask             255.255.255.255
Destination IP  Operator   None
Source Port  Operator      Equal
Source Port Start          SMTP
Destination Port  Operator Greater than
Destination Port Start     1023
TCP connections allowed    N
Account Process allowed    N
```

FIGURE 12.4 OUTPUT FOR IP FILTERING EXAMPLE

Interior Router

If an interior router exists in the network, the administrator may decide to use a *Default Scope* of *Permit*. In this case, all undesired traffic must be excluded by a rule in the rule list. In Figure 12.5, a conceptual equivalent of the interface is shown.

All packets except those which fall into the holes in the ball will be allowed entry in to or out of the network.
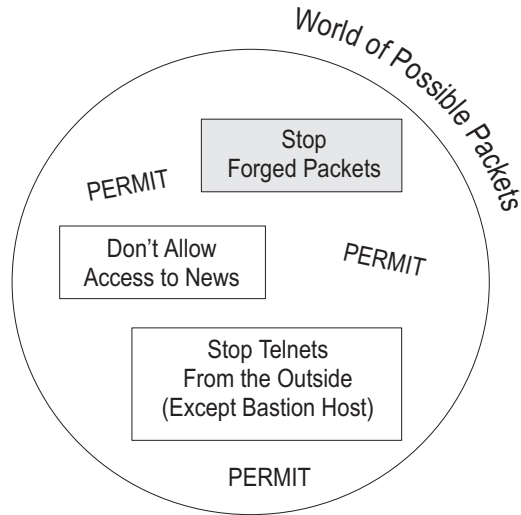
FIGURE 12.5 PERMIT DEFAULT SCOPE

The configuration for "Stop forged packets" is shown in the following listing:

Cyclades-PR4000

```
Rules Lists
Rule List Name      Rule            Default      List        Linked
                    Status          Scope        Type        Rule
                                                             List
slot1_in            Enabled         Permit       Filter

Filter_list Name slot1_in
Rule 0
Status                          Enabled
Scope                           Deny
Protocol                        0
Source IP Operator              Equal
Source IP start                 10.0.0.0
Source IP Mask                  255.0.0.0
Destination IP  Operator        None
Source Port Operator            None
Destination Port Operator       None
TCP connections allowed         Y
Account Process allowed         N
```

`Slot1_in, rule 0,` prohibits any incoming packets with source IP addresses of the internal network. Since the addresses used for internal networks cannot be routed on the Internet, they cannot be valid unless there is a leak of traffic through another router to the perimeter network.

Imagine that, as shown in the figure, the network is expanded and another range of IP addresses is used (not a sub-network). `Rule 0` in the list `Slot1_in` will not protect this network. Either another rule can be added to this list, or the new router can filter packets into its area (or both).

Traffic Rule Lists

There are three kinds of traffic rules that can be configured in CyROS. The first two determine a division of bandwidth for traffic flowing out of the router:

  1 Traffic Shaping (the division of bandwidth is strictly adhered to),
  2 Bandwidth Reservation (the division with the larger priority can steal bandwidth from the others),

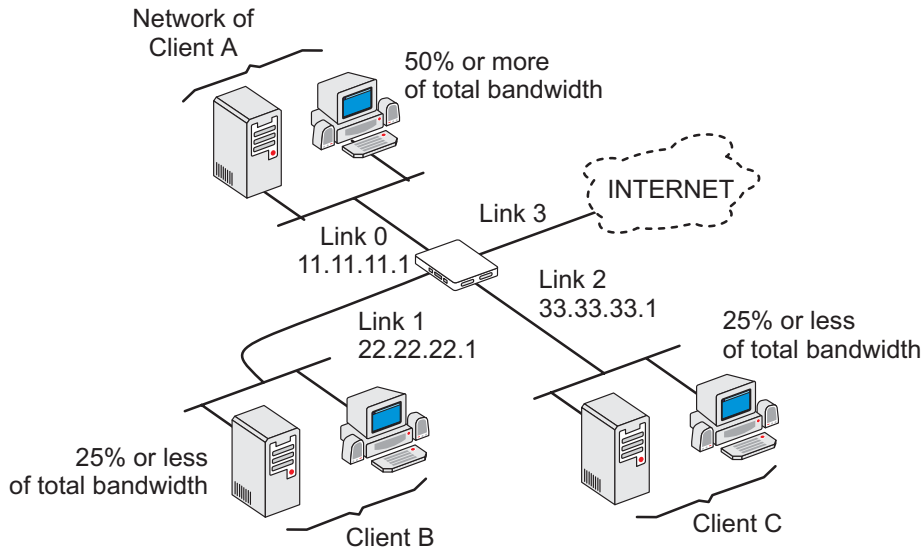An example showing the first two types is given in figure 12.6.

FIGURE 12.6 TRAFFIC RULE EXAMPLE 1

The third determines which services have priority flowing through the router:

3 Service Prioritization.

An Internet provider has three clients connected to the same router. Client A is larger and without traffic control would overwhelm the router to the exclusion of Clients B and C. The administrator decides to divide the flow out of the router (to the Internet) into three portions: 50% guaranteed for Client A, and the rest divided equally between Clients B and C. Since he does not want to limit Client A needlessly, the bandwidth Client A uses can be increased on demand if the total bandwidth is not being used up by the other two clients. This is Bandwidth Reservation.
The two clients with 25% bandwidth each are given lesser, but equal priorities. They can not share bandwidth or steal it from Client A. However, each has the right to 25% of the total bandwidth on link 3 if it is needed. This is Traffic Shaping.
Note that this rule list is applied to link 3, and not separately on links 0-2.

Steps for this configuration.

1 Create a Traffic Rule list `traffic_1`. This is done in the CONFIG =>RULES LIST =>IP => ADD RULE LIST menu with the *Rule List Type* set to *Traffic*.

2 Create rules for each of the three source IP addresses. This is done in the CONFIG =>RULES LIST =>IP =>ADD RULE menu. The parameters for each rule are shown in Figure 12.7. Of the traffic parameters, only the *Reserved Bandwidth* and *Bandwidth Priority* parameters are important in this example. *Flow Priority* is not used.

3 Enter into the configuration for link 3 and change the parameter CONFIG =>INTERFACE =>*<INTERFACE>* =>TRAFFIC CONTROL =>GENERAL =>IP TRAFFIC CONTROL LIST = `traffic_1`.

Note that the bandwidth used for the percentage calculation is that set in CONFIG =>INTERFACE =>*<INTERFACE>* =>TRAFFIC CONTROL =>GENERAL =>BANDWIDTH, and not the actual bandwidth available in the link.

```
Rules Lists
Rule List Name   Rule        Default     List       Linked
                 Status      Scope       Type       Rule
                                                    List
traffic_1        Enabled                 Traffic

Filter_list Name traffic_1

Rule 0
Status                  Enabled
Flow priority           0
Rule bandwidth          50%
Bandwidth priority      1
Protocol                0
Source IP Operator      Equal
Source IP start         11.11.11.0
Source IP Mask          255.255.255.0
Destination IP Operator None
Source Port Operator    None
Destination Port Operator  None
```

```
Rule 1
Status                     Enabled
Flow Priority              0
Rule bandwidth             25%
Bandwidth priority         2
Protocol                   0
Source IP Operator         Equal
Source IP start            22.22.22.0
Source IP Mask             255.255.255.0
Destination IP Operator    None
Source Port Operator       None
Destination Port Operator  None

Rule 2
Status                     Enabled
Flow Priority              0
Rule bandwidth             25%
Bandwidth priority         2
Protocol                   0
Source IP Operator         Equal
Source IP start            33.33.33.0
Source IP Mask             255.255.255.0
Destination IP Operator    None
Source Port Operator       None
Destination Port Operator  None
```

FIGURE 12.7 OUTPUT SHOWING PARAMETERS FOR TRAFFIC RULE EXAMPLE 1

An example showing the third type of traffic control is given in Figure 12.8. The network administrator wants to

prioritize the access to his web server. He also wants to prioritize e-mail sent by his SMTP server, but the priority should be lower. All other traffic should have the lowest priority. For web server access, the important flow direction is not the user requests, but rather the data requested. The traffic control rule must be placed on link 2. In the case of e-mail, the important flow is the data leaving the e-mail server, and not the acknowledgements back. This is also governed by link 2. (Note: flow control could be placed on the data request packets and the SMTP acknowledgements by associating rules to link 1.)
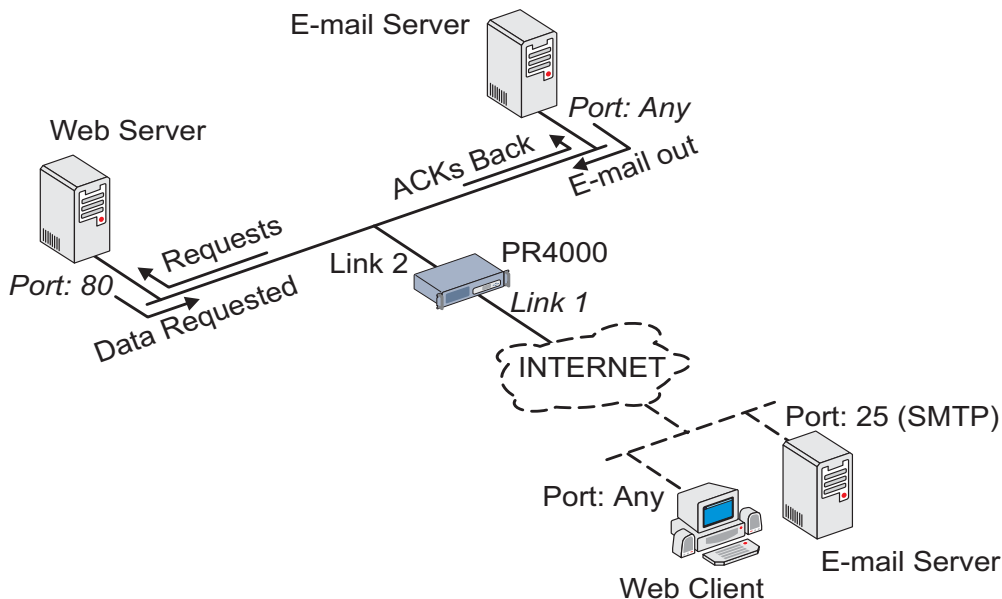

FIGURE 12.8 TRAFFIC RULE EXAMPLE 2

Chapter 14 - Filters and Rules   **136**

Cyclades-PR4000

The configured rules will appear as shown in the following listing.

Note that for this type of traffic control, of the traffic-specific parameters only *Flow Priority* is used. The *Reserved Bandwidth* and *Bandwidth Priority* parameters are not important. A system needing all three is conceivable, but much too complicated to show in this manual.

```
Rules Lists
Rule List    Rule       Default   List       Linked
Name
             Status     Scope     Type       Rule
                                             List
web_access   Enabled              Traffic


Filter_list Name web_access

Rule 0                                  Rule 1
Status                Enabled           Status                Enabled
Flow priority         1                 Flow Priority         2
Rule bandwidth        0%                Rule bandwidth        0%
Bandwidth priority    0                 Bandwidth priority    0
Protocol              TCP               Protocol              TCP
Source IP Operator    None              Source IP Operator    None
Destination IP        None              Destination IP        None
Operator                                Operator
Source Port Operator  Equal             Source Port Operator  None
Source Port Start     80                Destination Port      Equal
                                        Operator
Destination Port      None              Destination Port      SMTP
Operator                                Start
```

CHAPTER 15 IPX (INTERNETWORK PACKET EXCHANGE)

IPX is an alternative to IP, proprietary to Novell. When IPX is activated, many new menus appear to allow configuration of this type of network. IP and IPX can both be active in the router simultaneously, and an interface can have both IP and IPX traffic passing through it. IPX is not discussed in the other chapters of this manual to avoid confusion for those who are using IP.
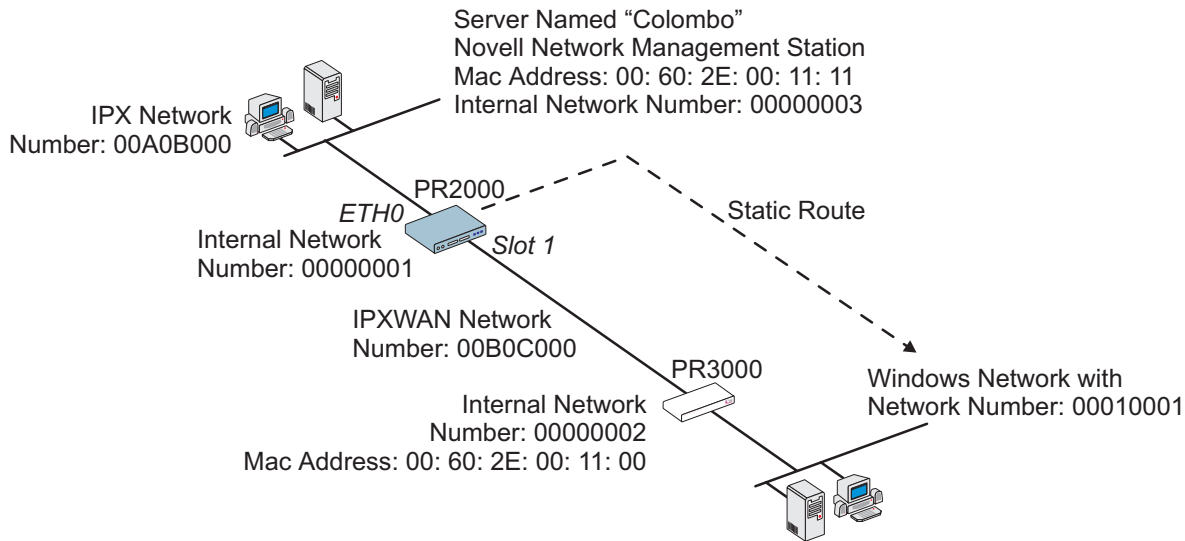

FIGURE 13.1 IPX NETWORK EXAMPLE

Enabling IPX

The first step is to activate the IPX feature in the router. This is accomplished using the menu option ADMIN =>ENABLE FEATURES => IPX. The IPX protocol must also be activated in the menu CONFIG =>IPX => GENERAL. In this menu, the *Internal Network Number* (the unique number assigned to the router) and the *Maximum Number of Hops* must be defined. The maximum number of hops defines how many routers can be on the path from this router to the destination of any packet sent through this interface.

Configuring the Ethernet Interface

The example in Figure 13.1 will be used to explain the remaining parameters that must be configured. The Ethernet interface for the PR2000 is examined first. In the menu CONFIG =>INTERFACE => ETHERNET => ENCAPSULATION, the Ethernet interface must be activated. The MAC address should be correct, as it is preset at the factory. For IPX, the *Encapsulation* parameter should be set according to the value used by the servers on the network..

In the menu CONFIG =>INTERFACE => ETHERNET => NETWORK PROTOCOL => IPX, the protocol should be activated and the LAN Network Number (00A0B000 in the example) set. All other parameters are explained in chapter 5.

Configuring Other Interfaces

This stage depends on which board is occupying slot 1 and which encapsulation will be used. Each encapsulation option will be discussed separately. Read the chapter describing the configuration for the appropriate interface, consulting this section for details on IPX-specific parameters.

PPP

The parameters for the PPP data-link protocol are discussed in chapter 10. Only the parameters particular to the IPX protocol will be described here. The are located in the CONFIG =>INTERFACE =><INTERFACE> =>ENCAPSULATION =>PPP. The first parameter is the *IPXWAN Network Number*, shown in Figure 13.1 as 00B0C000. *IPX Compression* can be enabled, and if so the *Number of Compression Slots* determined. If enabled, it must be used on both sides of the link (both routers in Figure 13.1) in order for the link to work.

Chapter 15 - IPX   **139**

The parameter *Send SAP Update* can be set to Demand, Periodic, or None. This parameter affects both SAP and RIP. *Periodic* causes the router to send these messages every minute, while choosing *Demand* will cause the router to send messages only when a message request is received.

Frame Relay

Frame Relay parameters are explained in chapter 10. The IPX-protocol-specific parameters are the same as those described in the preceding section, but are located in the menu CONFIG =>INTERFACE =><INTERFACE> =>ENCAPSULATION =>FRAME RELAY => <ESC> => ADD DLCI.

X.25

X.25 is explained in chapter 10. The IPX-protocol-specific parameters are the same as those described in the PPP section, but are located in the menu CONFIG =>INTERFACE =><INTERFACE> =>ENCAPSULATION =>X25 => <ESC> => ADD DTE.

Routing

Routing can be done statically, by configuring static routes, or dynamically using RIP. RIP is described in chapter 11. To create a static route, as shown in Figure 13.1, navigate to the menu CONFIG => STATIC ROUTES => IPX =>ADD ROUTE. The parameters for the system shown in the example are the following:

Add IPX Static Route Menu CONFIG => STATIC ROUTES => IPX =>ADD ROUTE

Parameter	Value for the Example
Destination Network Number	00010001
Interface	Slot 1
Next Hop Node	00602e001100
Number of Hops	1 (one router is between the router being configured and the network to be reached)
Number of Ticks	1 (related to the time necessary to reach the network)

The routing table is displayed by the menu option INFO => SHOW ROUTING TABLE => IPX. For the example, and using only the static route created above, the routing table appears as in Figure 13.2.

```
Destination  Interface/ Subinterface/   hops  ticks   Type
             Remote address
00000001                                0     1       PrimaryNet
00A0B000     Ethernet                   0     1       Connected
00010001     Slot1  Node 00602E001100   1     1       Static
00B0C000     Slot1                      0     1       Connected
```

FIGURE 13.2 ROUTING TABLE FOR THE EXAMPLE

The SAP (Service Advertisement Protocol) Table

In Novell networks, a given server can provide various services. In order for the router to identify these servers, their locations and services are entered into a SAP table in the router. This is done using the menu CONFIG =>IPX => SAP TABLE. The parameters for each entry are shown in the table.

SAP Table Menu CONFIG =>IPX => SAP TABLE

Parameter	Description
Service Type	Service this server offers. ? provides a list of valid codes. For the server Columbo, in the example, this code is 0166.
Server Name	In the example, the name is Columbo.
Service Network Number	00000003
Server Node	00602e001111
Server Socket Number	? provides a list of valid codes.
Number of Hops	Number of routers between this router and the server. 0 in the example.

CHAPTER 16 VIRTUAL PRIVATE NETWORK CONFIGURATION

The Virtual Private Network utility can be used on any link using IP routing. It is used to provide greater security between two or more networks connected through a public communications network. The basic concepts are presented in Figure 14.1. An IP datagram is sent by a device on the LAN. The message arrives at the router. The router has two tables. One with all the IP addresses contained in the Local Security Network and another with all the IP addresses in the Remote Security Networks. If the source IP address is contained in the Local Security Network list and the destination IP address is contained in the Remote Security Network list, the message is encrypted and encapsulated. The only destination address is that for the remote gateway (defined in the Remote Security Network list). Upon arrival at the remote gateway, the packet is unwrapped and sent to its destination.
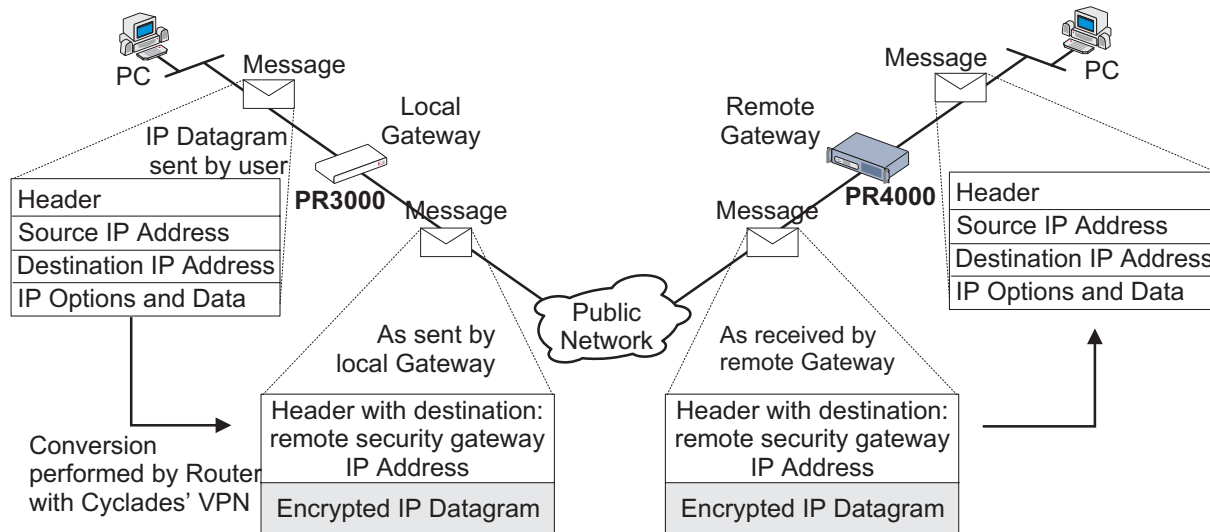

FIGURE 14.1 CONVERSION PERFORMED BY CYCLADES' VIRTUAL PRIVATE NETWORK UTILITY

Cyclades-PR4000

An example showing a local security network and two remote security networks is shown in Figure 14.2. The PR4000 in the local security network will be configured step by step. (Which network is considered local and which network is considered remote depends on the router being configured.)

STEP ONE
The Virtual Private Network Utility must be Enabled in the ADMIN =>ENABLE FEATURES =>VPN menu before it can be used. Navigate to this menu and enter the password supplied by Cyclades to activate VPN.

STEP TWO
Link 1 of the PR4000 (RSG3) should be fully configured and operational before beginning the VPN configuration. Each router has an IP address (with optional secondary IP addresses) for each numbered interface. In addition, each router has a Router IP Address which is one of the interface IP addresses. This router IP address is used whenever a single IP address is needed to identify the router. It is critical that each router being used as a remote security gateway have this parameter defined. It is NOT defined automatically. Navigate to CONFIG =>IP =>ROUTER IP and confirm that this parameter has been defined and is set to the value desired. An address that can be routed on the internet is generally used.

Important!! The Router IP Addresses for the other Remote Security Gateways (RSG1 and RSG2 in the example) must also be known before beginning the configuration of RSG3.
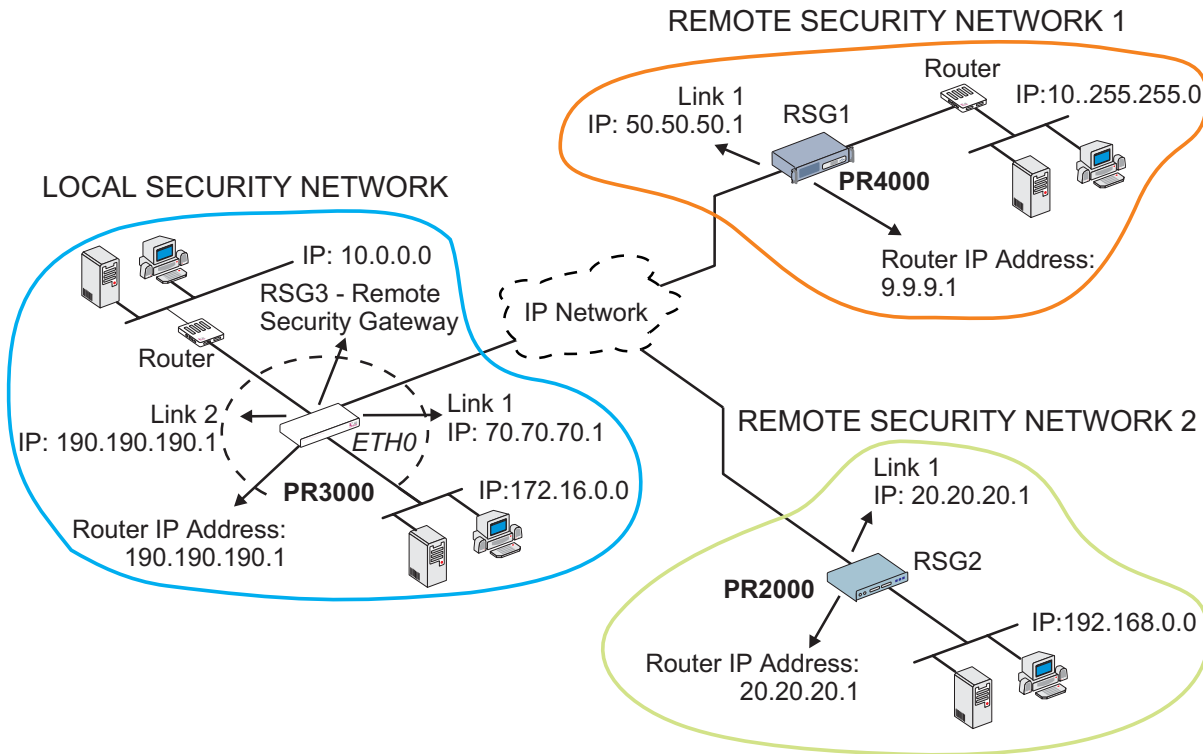
FIGURE 14.2 VIRTUAL PRIVATE NETWORK EXAMPLE

Cyclades-PR4000

STEP THREE
Use the menu item INFO =>SHOW ROUTING TABLE to confirm that the other Remote Security Gateways (RSGs), and all the networks included in the Remote Security Networks, are reachable. In the example, this would require that all of the following appear in RSG3's routing table:

- RSG1 router IP address: 9.9.9.1
- Network connected to RSG1 that will be included in Remote Security Network 1: 10.255.255.0
- RSG2 router IP address: 20.20.20.1
- Network connected to RSG2 that will be included in Remote Security Network 2: 192.168.0.0

These IP addresses should appear as a destination or be contained in one of the destination networks listed in the routing table. If an address is not in the routing table, add it following the instructions given in chapter 11 for static routes.

STEP FOUR
The next step is to define the devices contained in the Local Security Network. Navigate to the menu CONFIG =>SECURITY =>VPN =>LOCAL IP NETWORKS =>ADD NETWORK. Enter the Network IP address and mask for all devices to be included in the local network for VPN purposes. In the example, the networks 10.0.0.0 and 172.16.0.0 must be added.

> Traffic from other networks attached to the router will still be routed. The only difference is that the messages will be forwarded without processing and encryption by the VPN software.

STEP FIVE
The Gateways (represented by RSG1 and RSG2 in the example) must be defined. The Router IP address for each gateway is requested, along with a secret. This secret is not global, but rather applies to each pair of RSGs. If RSG3 defines the secret for RSG1 as rumpelstiltskin, then RSG1's secret for RSG3 must also be rumpelstiltskin. It is critical that the Router IP Address (as described in step two) be used, and not the IP address of the link connected to the IP network (unless the two IP addresses happen to be the same).

STEP SIX
Now, the Remote Security Networks must be defined. This is done in the CONFIG =>SECURITY =>VPN
=>REMOTE IP NETWORKS =>ADD NETWORK menu. The IP address and network mask must be defined for
all remote devices to be included in the remote network for VPN communication. The Remote Security Gateway
IP address (set in step five) must also be given for each network. In the example, the RSG IP address for the
network 10.255.255.0 is 9.9.9.1, and the RSG IP address for the network 192.168.0.0 is 20.20.20.1.

STEP SEVEN
The last step is to activate VPN and configure the VPN options. Be aware that after activating VPN on the local
network, data sent to the remote network will not be forwarded until VPN is configured and activated on that
network too. The VPN Options Menu parameters should be set using the guidelines given below. The options
should be defined identically for all Remote Security Gateways in a VPN.

VPN Options Menu CONFIG =>SECURITY =>VPN =>OPTIONS

Parameter	Description
Cyclades VPN Status	Activates the Virtual Private Network. Warning: until VPN is activated on both ends of a given tunnel, all traffic will halt.
Tunnel Keepalive Timeout	Keepalive messages are sent across each tunnel with this frequency, to make sure that the router on the other end of the connection is operating.
Tunnel Keepalive Retries	If a keepalive message reply is not received, the router sends the request again this number of times.
Tunnel Inactivity Timeout	If no messages are passed for this time period (keepalive messages not included), the tunnel will be disconnected.
Time Interval for VPN Retries	This is the time between retries (for either tunnel creation or keepalive requests that are not acknowledged).

APPENDIX A TROUBLESHOOTING

What to Do if the Login Screen Does Not Appear When Using a Console.

1 Check the configuration of the terminal. The correct values are given in chapter 2.

2 Check to see if the router booted correctly. Before the login screen appears, boot messages should appear on the screen. If the system halts while booting, the last message on the screen should give an indication of what went wrong. Boot messages will also appear on the LCD display on the front panel of the PR4000. When the boot process is complete, the Cyclades logo will appear on the screen.

3 While the router is booting, the LEDs labeled Port 1 and Port 2 indicate the stage of the boot process, as shown in Figure A.1.

Test	"CPU"	3"	2"	"1"	Boot Code step
1	Off	Off	Off	On	Boot Code CRC check
2	Off	Off	On	off	Configuration vector load
3	Off	Off	On	on	DRAM test
4	Off	On	Off	off	Flash memory - Configuration validation
5	Off	On	Off	on	Flash memory - Code validation
6	Off	On	On	off	Interface cards detection
7	Off	On	On	on	Ethernet port detection
8	On	Off	Off	off	Real Time Clock test
9	On	Off	Off	on	Boot code selection
10	On	off	On	off	Load of the operating code
11	On	off	On	on	Control is being passed to the operating code

FIGURE A.1 ILLUMINATION OF LEDS WHILE ROUTER IS BOOTING.

Note that all four LEDs blinking simultaneously indicates a memory problem, such as when no RAM is installed.

What to Do if the Router Does Not Work or Stops Working.

1 Check that the cables are connected correctly and firmly.

2 Confirm that the Link LED is lit for the (Fast) Ethernet Port being used, indicating proper Ethernet cable termination. If it is not lit, check both ends of the (Fast) Ethernet cable and the hub connection. If it is lit, test the interface as described in the next section.

3 If port 2 is not being used, the port 2 LED doubles as a CPU status LED. If port 2 is being used, disconnect the cable temporarily to see the CPU status. The Port 2 LED should blink consistently one second on, one second off. If this is not the case, see figure A.2 for an interpretation of the blink pattern.

Event	Port 2 LED Morse code
Normal Operation	S (short, short, short...)
Flash Memory Error – Code	L (long, long, long, ...)
Flash Memory Error – Configuration	S, L
Ethernet Error	S, S, L
No Interface Card Detected	S, S, S, L
Network Boot Error	S, S, S, S, L
Real-Time Clock Error	S, S, S, S, S, L

FIGURE A.2 PORT 2 (CPU) LED CODE INTERPRETATION

Note: The Ethernet error mentioned in Figure A.2 will occur automatically if the Fast Ethernet link is not connected to an external hub during boot. If the Fast Ethernet is not being used or is connected later, this error can be ignored.

4 Make sure any external modem, DSU/CSU, or interface equipment is properly connected and that the interface configuration is correct. Many cables have the same connector, but are not interchangeable.

5 Make sure that the line (T1 or E1) is active. The menu command INFO=>SHOW STATUS will show the status of each channel. A status of Not Synchronized could mean that the problem is related to the line. The line provider should be able to test the connection. If, after testing the line, the not synchronized status persists, try testing the T1/E1 ports as described later in this chapter.

6 Confirm that the interface configuration is correct and has been saved to either flash or run, and that the Controller Menu parameters are correct. Compare the cable pinout to the connector pinout (shown in Appendix B of the Installation Manual). Different standards exist and an adaptor may be necessary.

7 Place a call to the PR4000 and see if a modem is being allocated. The menu command INFO=>SHOW DIGITAL MODEMS=>SHOW STATUS displays the status of each modem and related information. This information is also available using the CyROS Management Utility or the LCD display on the front panel. See chapter 3 for more information on using CyROS.

8 Setting the menu item CONFIG=>SYSTEM=>SYSLOG to level 7 will cause the syslog to show if incoming calls are reaching the PR4000. The menu INFO=>SHOW STATISTICS may also show useful information.

9 Many problems are due to an incorrect configuration of the switch on the part of the line provider. See chapter 2, What is in the Box, for guidance in the solution of problems of this type.

Testing the Ethernet Interface.

The simplest way to test the link is by using the ping application. (If the Ethernet Interface appears to not be working, it will be necessary to connect the console cable and access CyROS using a Computer or terminal.) From the main menu, choose APPLICATIONS =>PING. Enter the IP number of a host on the network for the HOST parameter and accept the preset values for the rest of the parameters. The output on the screen should appear as shown below.

Cyclades-PR4000

Pinging the router from a host on the network should give similar results. If the test fails, confirm that the link LED on the front panel is lit and that the IP Address and Subnet Mask parameters in the Network Protocol menu are correct for the network to which the router is attached. The command CONFIG =>INTERFACE =>ETHERNET =>L will display the current values of the interface parameters.

```
Host [host00] : 200.246.93.37
packet size (number from 32 to 1600) [32] :
count (0 if forever or 1 to 30000) [5] :
interval in ms (20 to 60000) [1000] :
PING 200.246.93.37 (200.246.93.37): 32 data bytes
32 bytes from (200.246.93.37): icmp_seq=1 ttl=127 time=1.96 ms
32 bytes from (200.246.93.37): icmp_seq=2 ttl=127 time=1.02 ms
32 bytes from (200.246.93.37): icmp_seq=3 ttl=127 time=0.99 ms
32 bytes from (200.246.93.37): icmp_seq=4 ttl=127 time=0.99 ms
32 bytes from (200.246.93.37): icmp_seq=5 ttl=127 time=0.98 ms
--- 200.246.93.37 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.98/1.19/1.96 ms
```

Testing the WAN Interface

The WAN interface can be tested using ping as described in the previous section. If the ping is not successful, check the routing table to see if a route to the destination exists (INFO =>SHOW ROUTING TABLE). The menu items INFO =>SHOW STATISTICS =>SWAN and INFO =>SHOW STATUS =>SWAN may also provide useful information.How to Test if the T1/E1 Ports are Working

If the PR4000 does not seem to be working properly, and none of the above advice has located the problem, the hardware interfaces should be tested. This will determine if the problem is hardware, software, or configuration related. If the T1/E1 ports pass the test below, the problem must be external (line) or due to an incorrect configuration or software problem.

Use of a Cross Cable for Testing T1/E1 Ports and Modems

Two tests can be performed with the cross cable: one tests the two T1/E1 ports while the other tests the 2 ports and the modems. The pin diagram of the cross cable is shown in Appendix B. Before starting the tests, connect the two T1/E1 ports using the cross cable.

Testing the Two T1/E1 Ports

1. In the CyROS main menu, choose the following menu options: DEBUG =>HARDWARE TESTS=>HW DEBUG. Choose to test ports T1/E1 2 and T1/E1 3. (Slot 2 is T1/E1 port 1 and slot 3 is T1/E1 port 2.)

2. In the T1/E1 2 Tests Menu, select Comm. Test (master).

3. In the T1/E1 3 Tests Menu, select Comm. Test (slave).

The screen output of the test should appear as shown in the following figure.

```
Daughter Boards tests statistics:
Slot 2 (E1) - Communication test:
Last            Line Mode        Status      Bandwidth     Clock
Status:         Synchronized    Master      Fractional    Slave
General statistics:
Sent:           3 packets/273 bytes.
Received:       3 packets/471 bytes.
No errors.
Slot 3 (E1) - Communication test:
Last            Line Mode        Status      Bandwidth     Clock
Status:         Synchronized    Slave       Fractional    Master
General statistics:
Sent:           3 packets/471 bytes.
Received:       3 packets/273 bytes.
No errors.
```

Appendix A - Troubleshooting **151**

Cyclades-PR4000

Let the test run for at least 1 minute. If both slots show no errors, the test was sucessful.

How to Test the Modems

1. In the CyROS main menu, choose the following menu options: DEBUG=> HARDWARE TEST=>DSP TEST.

2. The first parameter will be Number of Modems to be Tested Each Time. Enter the number of modems in your system. The maximum is 62.

3. The second parameter is Number of Tests to be Performed. Enter zero for continuous tests. Tests can be stopped at any time with the escape key.

The test will be performed repeatedly until you use the <ESC> key. After each test, results similar to the following will be displayed on the screen:

```
*****TEST NUMBER 1 - TESTING 12 MODEMS. ********
Resetting communication ...
Waiting for the lines and the modems ... OK
Allocating modems ... 60 modems connected
DSPs connection timeout
Starting data communication ...
Communication completed!
```

Cyclades-PR4000

```
          *    *    *    DPS TEST RESULTS   *    *    *
          Errored Seconds: first line->0; second line->0
    link   Slot   Out    In     Tx     Tx   Time  RXErr  TXNOK   Conn
                  DSP   DSP  PCKts  Bytes
      1      1     56    57    100  25000    13      0      0     OK
      2      2     58    59     97  24250    28      0      3     OK
      3      3     60    61     96  24000    33     31      4     OK
      4      4     62    63     88  24500    23      0      2     OK
      5      5      0     1     91  22750    57     35      9     OK
      6      6      2     3     98  24500    23      0      2     OK
      7      7      4     5     97  24250    28    110      3     OK
      8      8      6     7     99  24750    18     46      1     OK
      9      9      8     9      0      0     0      0      0    NOK
     10     10     10    11    100  25000    14      0      0     OK
     11     11     12    13     98  24500    23    106      2     OK
     12     12     14    15     98  24500    23      0      2     OK
```

The Conn column often shows a NOK for a few modems each test due to the short timeout value. After a few tests, the NOKs should dissapear.

Cyclades-PR4000

Let the test run for a while. After typing <ESC> to end the tests, CyROS will compile a summary of the data similar to the following:

```
          * * * * * F I N A L  S T A T I S T I C S * * * * *
DSP Board number 1 :

DSP    N.       Not    Dis    Out-     RXERR    TXERR  TXBYTES  RXBYTES
ID     Tests    Conn   Conn   bound
0      2        0      0      1        0        0      50056    49846
1      2        0      0      1        0        1      50058    49979
2      2        0      0      1        113      6      50042    49373
3      2        0      0      1        0        0      50016    49944
4      2        0      0      1        74       5      50084    49419
5      2        0      0      1        135      2      50106    49491
6      2        0      0      1        112      11     50094    49177
7      2        0      0      1        102      4      50070    49789
```

The exact numbers in this output are not important. If the ratios RXERR/RXBYTES and TXERR/TXBYTES are both less than 0.02, then the test was sucessful.

APPENDIX B. HARDWARE SPECIFICATIONS

General Specifications

The Cyclades-PR4000 power requirements, environmental conditions and physical specifications are listed in the table below.

Power Requirements	
Input voltage range	115 to 230 VAC. Some models have an external switch to select between 115 and 230 VAC. Models with a universal power supply have an input voltage range of 110-240 VAC.
Input frequency range	50/60 Hz, single phase
Power (base unit)	250W
Environmental Conditions	
Operating temperature	32° to 112° F (0° to 44° Celsius)
Relative humidity	5% to 95%, non-condensing
Altitude	Operating 10,000 feet max. (3000 m)
Physical Specifications	
External dimensions	17"W x 8.5"D x 3.5"H
Weight (base unit only)	3.0 Kg (6.6 pounds)

External Interfaces

Console Port

An RS-232 DTE port is provided for communication with a configuration terminal. A maximum speed of 115.2kbps is supported on this port. Use a straight-through cable to connect to DCE devices (modems, for example). Use a cross-cable to connect to a DTE device (terminal, host computer, etc). The pinout diagram is shown below.

CONSOLE PORT	
Pin	RS-232 Signal
1	RTS
2	DTR
3	TX
4	Ground
5	CTS
6	RX
7	DCD
8	DSR
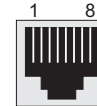
FIGURE B.1 CONSOLE PORT - RS-232 INTERFACE WITH AN RJ-45 FEMALE CONNECTOR

Appendix B - Hardware Specifications

156

Ethernet Port

The PR3000 Ethernet port meets IEEE I802.3 physical specifications. It provides a single Ethernet interface and supports 10Base-T (Unshielded Twisted Pair) on a standard RJ-45 female connector.

ETHERNET PORT	
Pin	Ethernet Signal
1	TPTX+
2	TPTX-
3	TPRX+
4	N.C.
5	N.C.
6	TPRX-
7	N.C.
8	N.C.
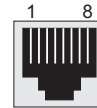
FIGURE B.2 ETHERNET PORT - RJ-45 FEMALE CONNECTOR

T1 and E1

Both the T1 and E1 interfaces use an 8-pin RJ-48C female connector.

T1/E1 Interface	
Pin	**Signal**
1	RXTIP
2	RXRING
3	N.C.
4	TXTIP
5	TXRING
6	N.C.
7	N.C.
8	N.C.

FIGURE B.3 T1 OR E1 - RJ-48C FEMALE CONNECTOR

Cables

Please refer to chapter 2, *What is in the Box*, to see which cables are provided with the PR4000 and which cables are optional.

Straight-Through Cable

Straight-Through Cable

DB-25 Male Cyclades Router				DB-25 Male DCE / DTE	
Signal	Pin			Pin	Signal
TxD	2	————		2	TxD
RxD	3	————		3	RxD
RTS	4	————		4	RTS
CTS	5	————		5	CTS
DSR	6	————		6	DSR
Gnd	7	————		7	Gnd
DCD	8	————		8	DCD
TxClk_DTE	15	————		15	TxClk_DTE
RxClk	17	————		17	RxClk
DTR	20	————		20	DTR
RI	22	————		22	RI
TxClk_DCE	24	————		24	TxClk_DCE
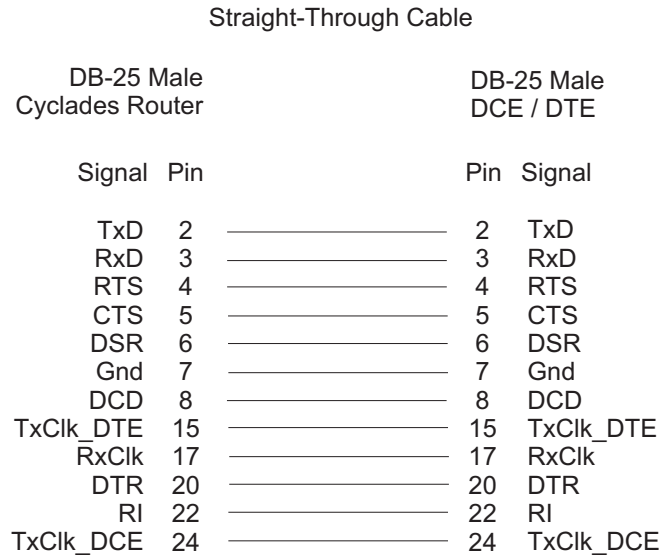
FIGURE B.4 PINOUT DIAGRAM OF THE STRAIGHT CABLE - DB-25 MALE TO DB-25 MALE

Cross Cable

Cross Cable

DB-25 Male			DB-25 Male	
Signal	Pin		Pin	Signal
PGnd	1		1	PGnd
TxD	2		3	RxD
RxD	3		2	TxD
RTS	4		4	RTS
CTS	5		5	CTS
Gnd	5		5	Gnd
DCD	7		7	DCD
DTR	8		8	DTR
DSR	20		20	DSR
TxD V.35 + (B)	6		6	RxD V.35 + (B)
RxD V.35 + (B)	11		13	TxD V.35 + (B)
TxD V.35 - (A)	13		11	RxD V.35 - (A)
RxD V.35 - (A)	12		14	TxD V.35 - (A)
TxClk_DTE (A)	14		12	TxD V.35 - (A)
RxClk	15		24	RxClk
TxClk_DCE	17		17	TxClk DCE
TxClk_DTE V.35 + (B)	24		15	TxClk_DCE V.35 + (B)
RxClk V.35 + (B)	16		19	RxClk V.35 + (B)
TxClk DCE V.35 - (B)	25		25	TxClk DTE V.35 - (B)
TxClk_DTE V.35 - (A)	19		16	TxClk_DCE V.35 - (A)
RxClk V.35 - (A)	18		21	RxClk V.35 - (A)
TxClk DCE V.35 - (A)	23		13	TxClk DTE V.35 - (A)
	21		18	

FIGURE B.5 PINOUT DIAGRAM OF THE CROSS CABLE - DB-25 MALE TO DB-25 MALE

Router-MD / V.35 Cable

Signal	Pin (DB-25 Male Cyclades Router)		Pin (DB-25 Male Telebrás CSU/DSU)	
PGnd	1		1	- A
RTS	4		5	- C
CTS	5		7	- D
DSR	6		9	- E
Gnd	7		13	- B
DCD	8		10	- F
TxD/V.35 (B)	11		15	- S
TxD/V.35 (A)	12		2	- P
RxD/V.35 (B)	13		17	- T
RxD/V.35 (A)	14		4	- R
TxClk_DTE/V.35 (B)	16		16	- AA
TxClk_DTE/V.35 (A)	18		3	- Y
TxClk_DCE/V.35 (B)	19		24	- W
TxClk_DCE/V.35 (A)	21		11	- U
RxClk/V.35 (A)	23		6	- V
RxClk/V.35 (B)	25		19	- X
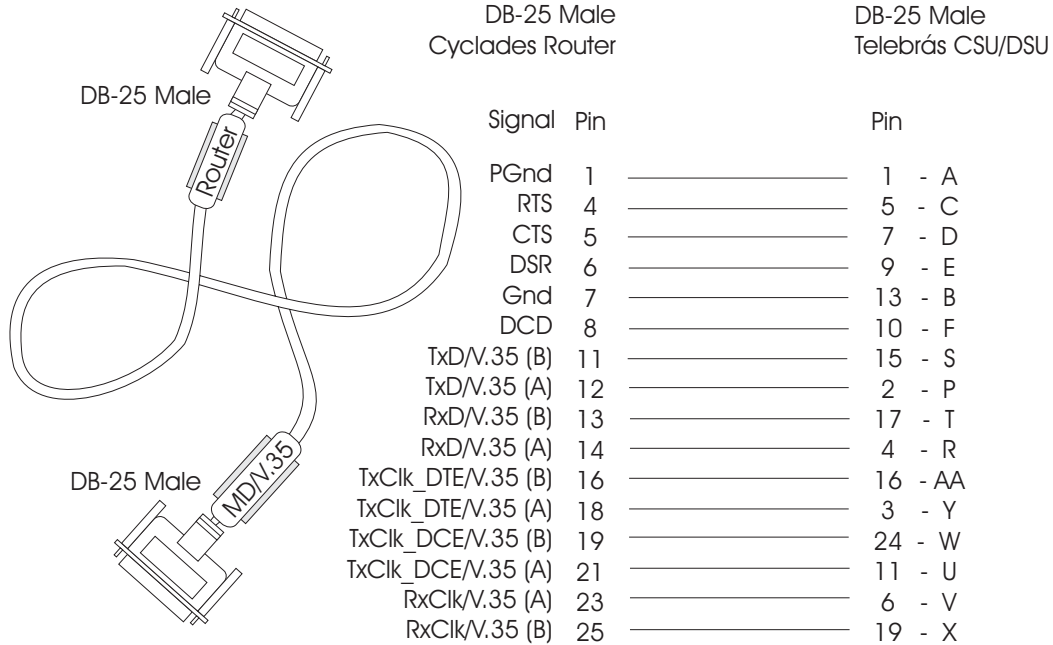
FIGURE B.6 ROUTER MD / V.35 CABLE - DB-25 MALE TO DB-25 MALE

DB-25 to M.34 Adapter
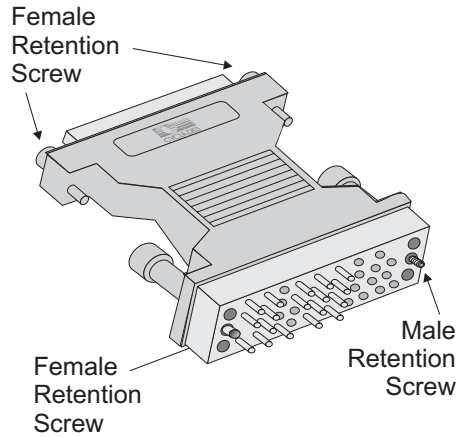
		DB-25 Female		M.34 Male
Signal	Pin		Pin	Signal
PGnd	1	————	A	PGnd
RTS	4	————	C	RTS
CTS	5	————	D	CTS
DSR	6	————	E	DSR
Gnd	7	————	B	Gnd
DCD	8	————	F	DCD
TxD/V.35 (B)	11	————	S	TxD (B)
TxD/V.35 (A)	12	————	P	TxD (A)
RxD/V.35 (B)	13	————	T	RxD (B)
RxD/V.35 (A)	14	————	R	RxD (A)
TxClk_DTE/V.35 (B)	16	————	AA	TxClk_DTE (B)
TxClk_DTE/V.35 (A)	18	————	Y	TxClk_DTE (A)
TxClk_DCE/V.35 (B)	19	————	W	TxClk_DCE (B)
DTR	20	————	H	DTR
TxClk_DCE/V.35 (A)	21	————	U	TxClk_DCE (A)
RxClk V.35 (A)	23	————	V	RxClk (A)
RxClk V.35 (B)	25	————	X	RxClk (B)

Female Retention Screw
Female Retention Screw
Male Retention Screw

FIGURE B.7 DB-25 TO M.34 ADAPTER

Cross Cable for Testing the T1/E1 Ports

Please see appendix A for a description of the use of this cable.

Loopback Cable

RJ-48C   RJ-48C

RxTip 1 ——————— 4 TxTip
RxRing 2 ——————— 5 TxRing
TxTip 4 ——————— 1 RxTip
TxRing 5 ——————— 2 RxRing
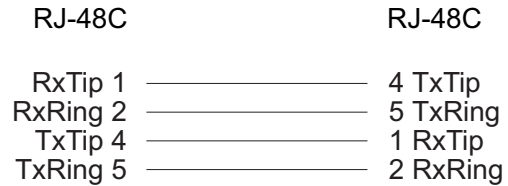
FIGURE B.8 PINOUT DIAGRAM OF THE CROSS CABLE FOR TESTS, RJ-48C MALE TO RJ-48C MALE

ISO 2110 Standard Cable

Signal	Pin		Pin	
PGnd	1	————	1	- A
RTS	4	————	4	- C
CTS	5	————	5	- D
DSR	6	————	6	- E
Gnd	7	————	7	- B
DCD	8	————	8	- F
TxD/V.35 (B)	11	————	14	- S
TxD/V.35 (A)	12	————	2	- P
RxD/V.35 (B)	13	————	16	- T
RxD/V.35 (A)	14	————	3	- R
TxClk_DTE/V.35 (B)	16	————	12	- AA
TxClk_DTE/V.35 (A)	18	————	15	- Y
TxClk_DCE/V.35 (B)	19	————	11	- W
TxClk_DCE/V.35 (A)	21	————	24	- U
RxClk/V.35 (B)	23	————	17	- V
RxClk/V.35 (A)	25	————	9	- X
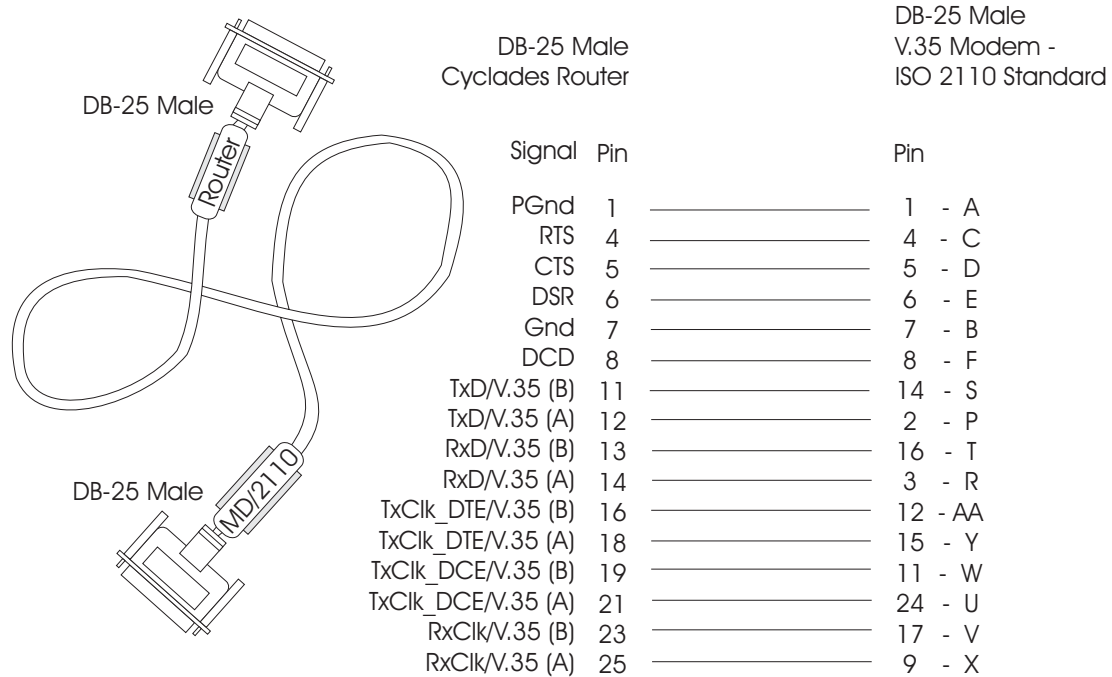
FIGURE B.9 PINOUT DIAGRAM OF THE ISO 2110 STANDARD CABLE- DB-25 MALE TO DB-25 MALE
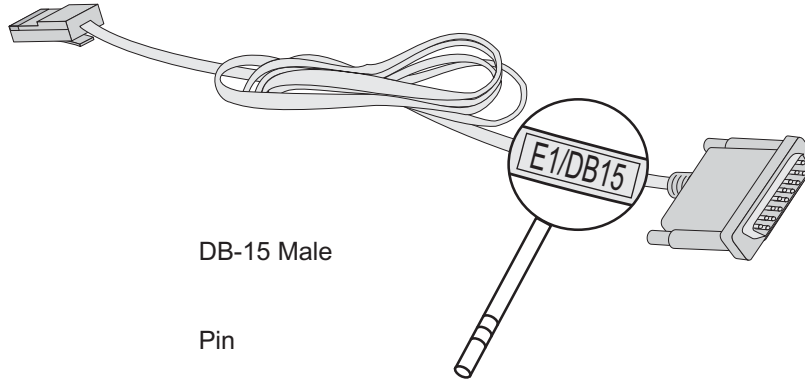
E1 / DB-15 Cable

RJ-45 Male   DB-15 Male

Pin   Pin

1 ——————— 3
2 ——————— 11
4 ——————— 1
5 ——————— 9

B. 10 PINOUT OF THE E1 / DB-15 CABLE - RJ-45 MALE TO DB-15 MALE

APPENDIX C CONFIGURATION WITHOUT A CONSOLE

When a terminal or PC is not available for use as a console, the router has a special feature that allows configuration of the Ethernet interface from any PC on the LAN. The router "adopts" the destination IP address of the first non-UDP packet received from the LAN and accepts the connection. (After configuration of the Ethernet interface, with or without a console, the remaining configuration can be done via telnet.)

It is recommended that a console be used for the initial configuration of the router, due to the hardware and software diagnostic messages given on the console screen. If a console is not available, follow the instructions in this appendix to configure the Ethernet interface.

Requirements

The router must be set to the factory default. If the router is being moved from one location to another, the configuration should be reset using the menu option ADMIN =>LOAD CONFIGURATION =>FACTORY DEFAULTS before the router is moved.

Procedure

1 Edit the ARP table of the PC in the LAN and associate the MAC address of the router (affixed to the underside of the router) to the IP address for the interface. In Unix and Microsoft Windows systems, the command to manipulate the ARP table is something similar to arp -s <IP address> <MAC address>. In Unix, type **"man arp"** for help. In Microsoft Windows, type **"arp /?"** for information about this command.

2 Telnet to the IP address specified above. The router will receive the packet because of the modified ARP table and use the IP address for its Ethernet interface.

3 The new IP address is saved only in run memory. The configuration must be explicitly saved to flash using the menu option ADMIN =>WRITE CONFIGURATION =>TO FLASH. Do this now.

4 The Ethernet and other interfaces can now be configured using the telnet session established.

If the connection fails or if the link goes down before the IP address is saved to flash, a console must be used.

APPENDIX D INSTALLATION OF ADDITIONAL DIGITAL MODEMS

The purpose of this appendix is to describe the correct procedure for the installation of the digital modem board in the PR4000. When the PR4000 is purchased with modems, the modems are installed at the factory. This chapter should be read ONLY when modems are purchased at a later date.

The modems are extremely sensitive to static electricity, (more so than RAM), and should be handled with caution. The body carries static electricity and if the person installing the board is not correctly grounded, the modem board could suffer irreversible damage. Please follow the instructions outlined below carefully to avoid damaging the board.

Step One:
Unplug the PR4000 from the power source and remove the power cord. Remove all cables connecting the PR4000 to other devices.

Step Two:
Carry the PR4000 to a workbench or table with an anti-static surface and wrist-strap. If a workbench of this type is not available, use the wrist strap sent with the modems (a wrist-strap is not included for all countries due to differences between electrical installations). The directions should be followed carefully. Please note that the wrist-strap should not be connected to the PR4000 because it is no longer plugged in and thus no longer connected to ground.

Step Three:
Remove the four top screws and the eight screws on the bottom edges of the PR4000, as shown in the figure.

Appendix D - Installation of Additional Digital Modems   **167**
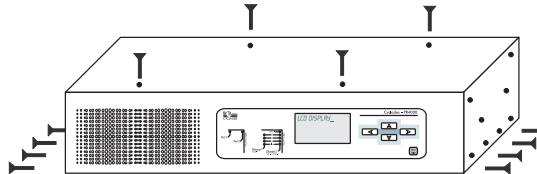
Step Four:
Attach the wrist-strap to your wrist.
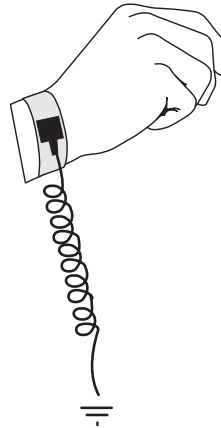
Step Five:
Remove the PR4000's cover. Be careful to not touch any components inside the PR4000's case, as they also can be damaged by static electricity.

Base   Cover

Appendix D - Installation of Additional Digital Modems   **168**
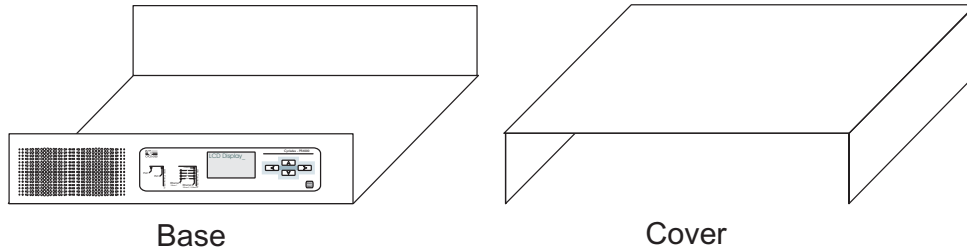
Step Six:
Open the clamps on the slot where the board will be installed, as shown in the figure.

Clamp

Slot

The slots are numbered from 0 to 7. The software does not depend on the board being installed in a particular slot, but installing the first board in slot 0, the second in slot 1, and so on makes the installation of each succeeding board easier. It is important that each board be handled as few times as possible.

Step Seven:
Confirm that the wrist-strap is grounded. Remove the modem board from its anti-static packaging, being careful to not touch the components or metal parts of the board (see the figure).

Appendix D - Installation of Additional Digital Modems **169**
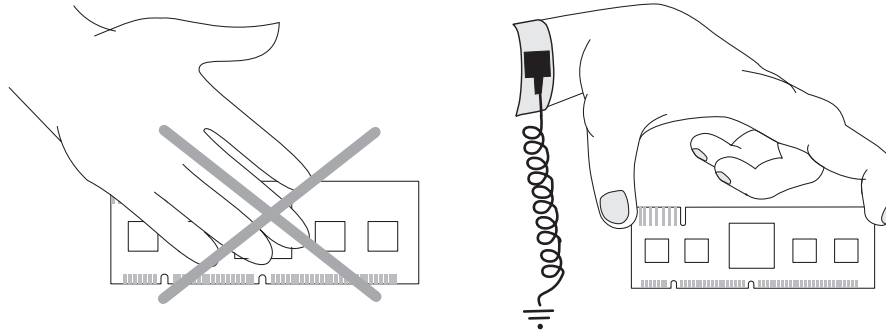
Step Eight:
Insert the board carefully into the slot, aligning the indentations in the board with the guides of the slot. Forcing the board or pushing it in at an angle can damage the board and the slot.

Trava do
Slot
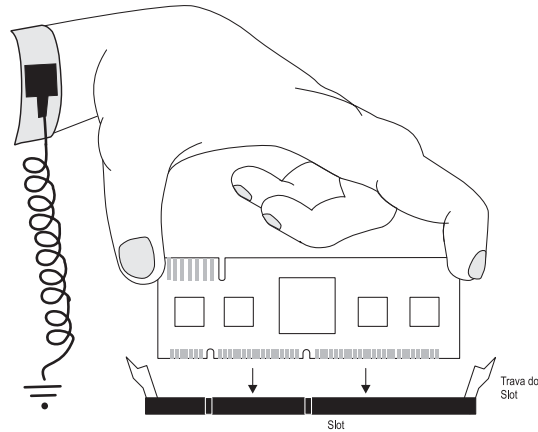
Slot

Step Nine:
Push the board into the slot until the clamps close around the board.

Clamp

Slot

Appendix D - Installation of Additional Digital Modems
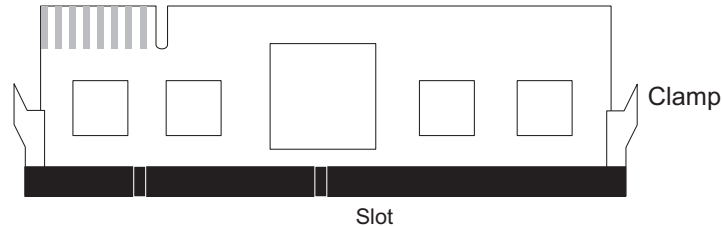
Step Ten:

Replace the PR4000's cover and replace the screws. Now you can remove the wrist-strap.

Step Eleven:

Reconnect the PR4000's cables, including the console cable. Start up the terminal program used to access the PR4000. Plug in the power cable and turn the PR4000 on. When the PR4000 boots, the following messages should appear (two boards are shown in this example):

```
DSP Cards Detected . . . . . . . . . . . . OK
8-DSP CARD on DIMM 1
8-DSP CARD on DIMM 2
Loading modem 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,
14, 15, 16 . . . done
```

If there is a problem with the board or if the messages shown above (for the correct number of modems) do not appear, call Cyclades' Technical Support.

⚠	The board should be connected to the PR4000 only by its presence in the slot. The terminals on the opposite side of the board are not intended to be used for a connection.

Index

Cyclades-PR4000

Cyclades Australia
Phone: +61 7 3279 4320
Fax: +61 7 3279 4393
www.au.cyclades.com

Cyclades Corporation
41829 Albrae Street
Fremont, CA 94538 - USA
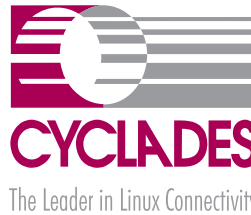Phone: (510) 770-9727
Fax: (510) 770-0355
www.cyclades.com

Cyclades South America
Phone: 55-11-5033-3333
Fax: 55-11-5033-3388
www.cyclades.com.br

Cyclades Philippines
Phone: (632) 813-0353
Fax: (632) 655-2610
www.ph.cyclades.com

Cyclades Italy
Phone: +39 329 0990451

CYCLADES
The Leader in Linux Connectivity

Cyclades UK
Phone: +44 1724 277179
Fax: +44 1724 279981
www.uk.cyclades.com

Cyclades Germany
Phone: +49 (0)81 22 90 99-90
Fax: +49 (0)81 22 90 999-33
www.cyclades.de

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com