Cyclades-PR1000
Installation Manual

Access Router

Cyclades Corporation

Cyclades-PR1000 Installation Manual
Version 1.2 – 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 product or 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 1.9.4 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-PR1000 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-PR1000 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-**PR1000** 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

Table of Contents

CHAPTER 1 HOW TO USE THIS MANUAL

Three Cyclades manuals are related to the PR1000.

  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.

This manual should be read in the order written, with exceptions given in the text.

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 9- Basic router configuration information for applications that do not fit any of the examples in chapter 4.

Chapter 10 - CyROS - shows how to set router specific parameters and create lists of hosts and users.

Chapter 11 - Network Address Translation - describes CyROS' NAT implementation.

Chapter 12 - Filters and Rules - demonstrates how to protect your router from undesired traffic.

Chapter 13 - IPX - presents the hidden menus available only in routers with IPX activated.

Chapter 14 - 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.

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 Cyclades-PR1000 comes in two varieties, described below. Both models are accompanied by the following accessories:

- Quick Installation Manual
- Documentation CD containing the complete Installation Manual and the CyROS Reference Guide
- Console Cable and Power Source
- Mounting Kit containing Velcro® Strips and screws.

The Documentation CD also contains a back-up copy of the op Code, in case the preinstalled copy is corrupted in some way.

The V.35/RS-232 Model

Back Panel of PR1000
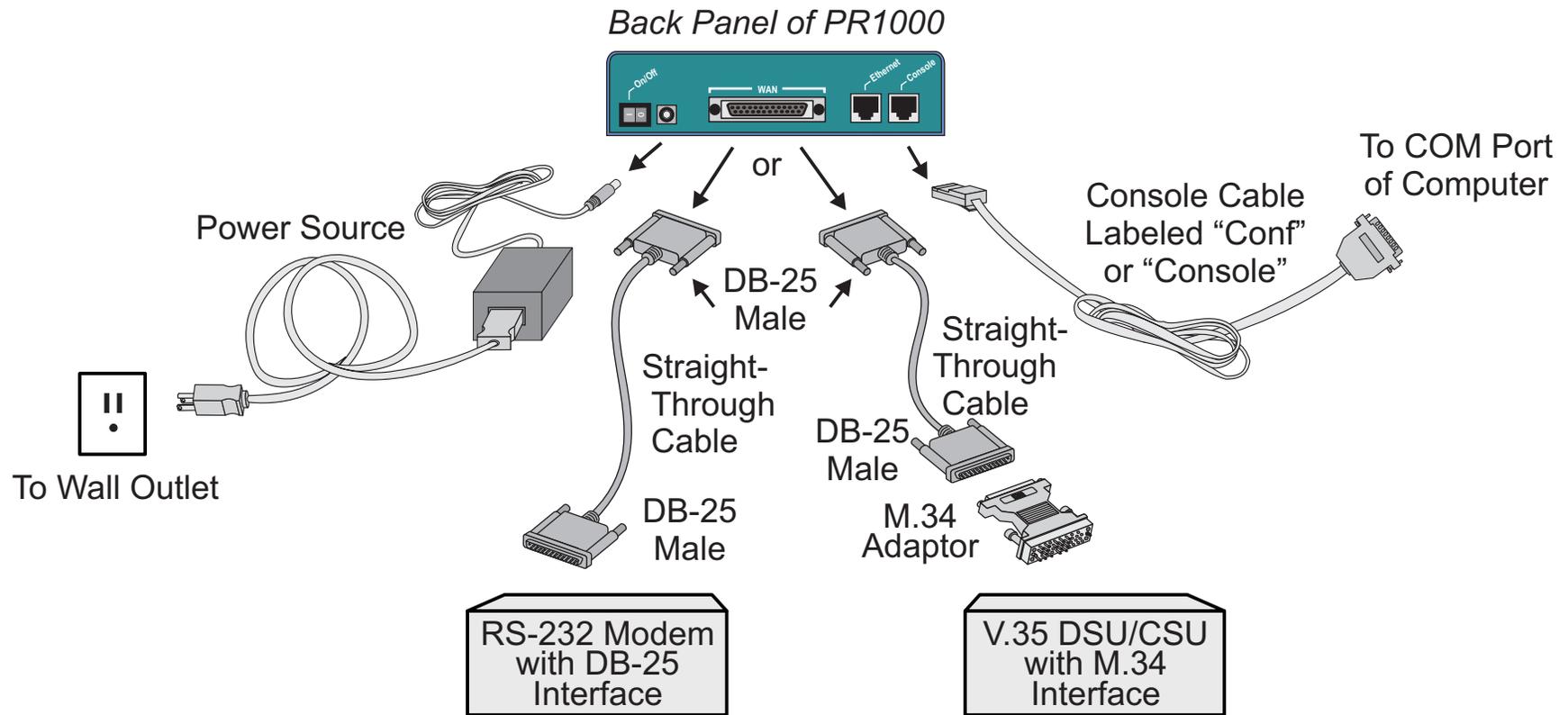
FIGURE 2.1 V.35/RS-232 MODEL

Figure 2.1 shows which cables (purchased separately) should be used for each type of modem and how everything should be connected. The pinout diagrams of these cables are provided in Appendix B of the Installation Manual.

The X.21 Model

Back Panel of PR1000

FIGURE 2.2 X.21 MODEL

Figure 2.2 shows which cable (purchased separately) should be used for an X.21 modem and how everything should be connected. The pinout diagram of this cable appears in Appendix B of the Installation Manual.

Cyclades recommends the use of Category 5, shielded twisted-pair cables for Fast Ethernet connections.

The Cyclades-PR1000 comes with rubber pads to prevent it from slipping on a horizontal surface. It may be necessary to affix the router more securely to either a horizontal or vertical surface. To this end, Velcro® strips and screws have been provided.

Horizontal Surfaces

The Velcro® strips should be used to attach the PR1000 more firmly to a horizontal surface. Remove the backing from the prickly Velcros® and attach them to the router as shown in the figure. Remove the backing from the fuzzy Velcros® and place them on the horizontal surface so they are aligned with the Velcros® on the router.

Cyclades-PR1000

Prickly Velcro®

Prickly Velcro®

Fuzzy Velcro®

Horizontal Surface Where the PR1000 Will be Secured
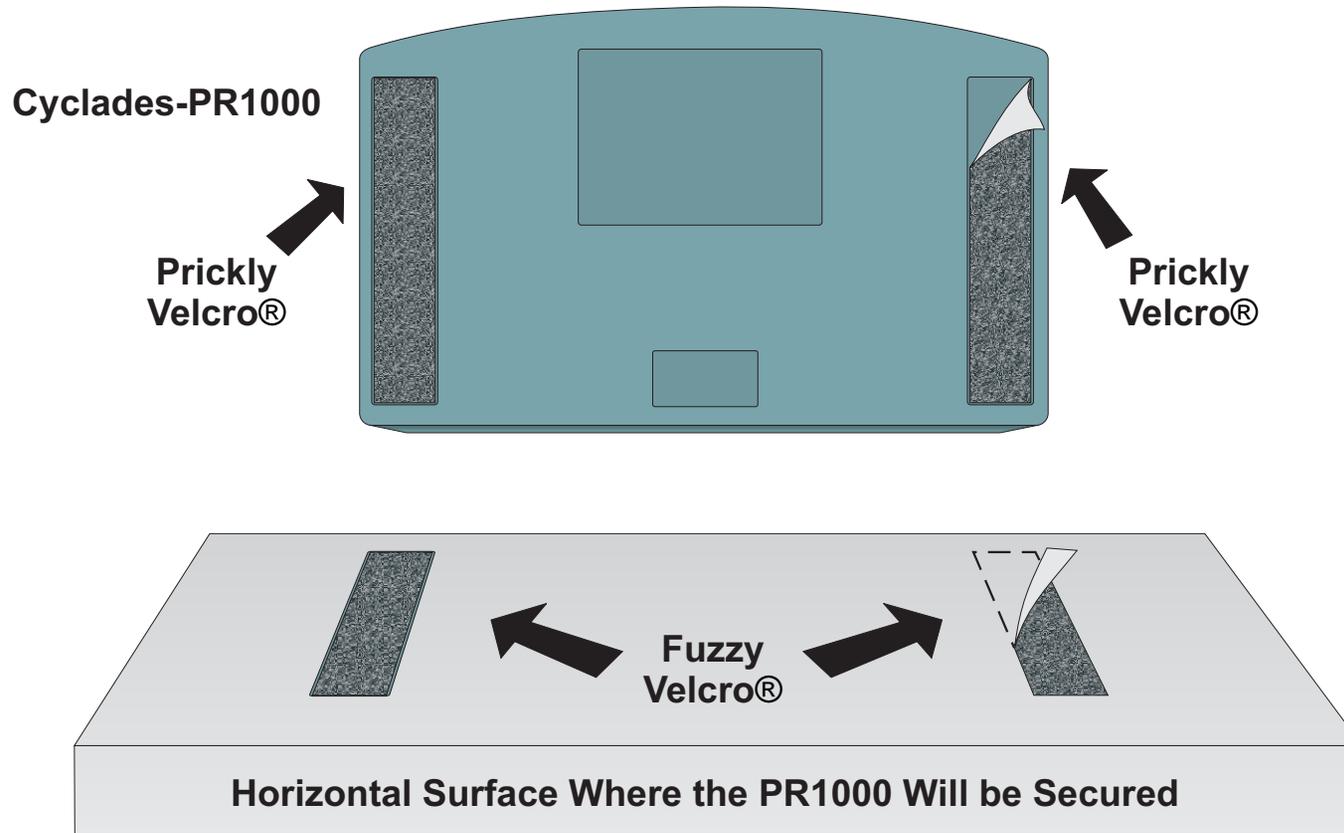
FIGURE 2.3 HOW TO ATTACH THE VELCRO® STRIPS

Next, place the PR1000 on the horizontal surface, aligning the fuzzy and prickly Velcros® as shown in Figure 2.4.

Cyclades-PR1000

Horizontal Surface Where the PR1000 Will be Secured
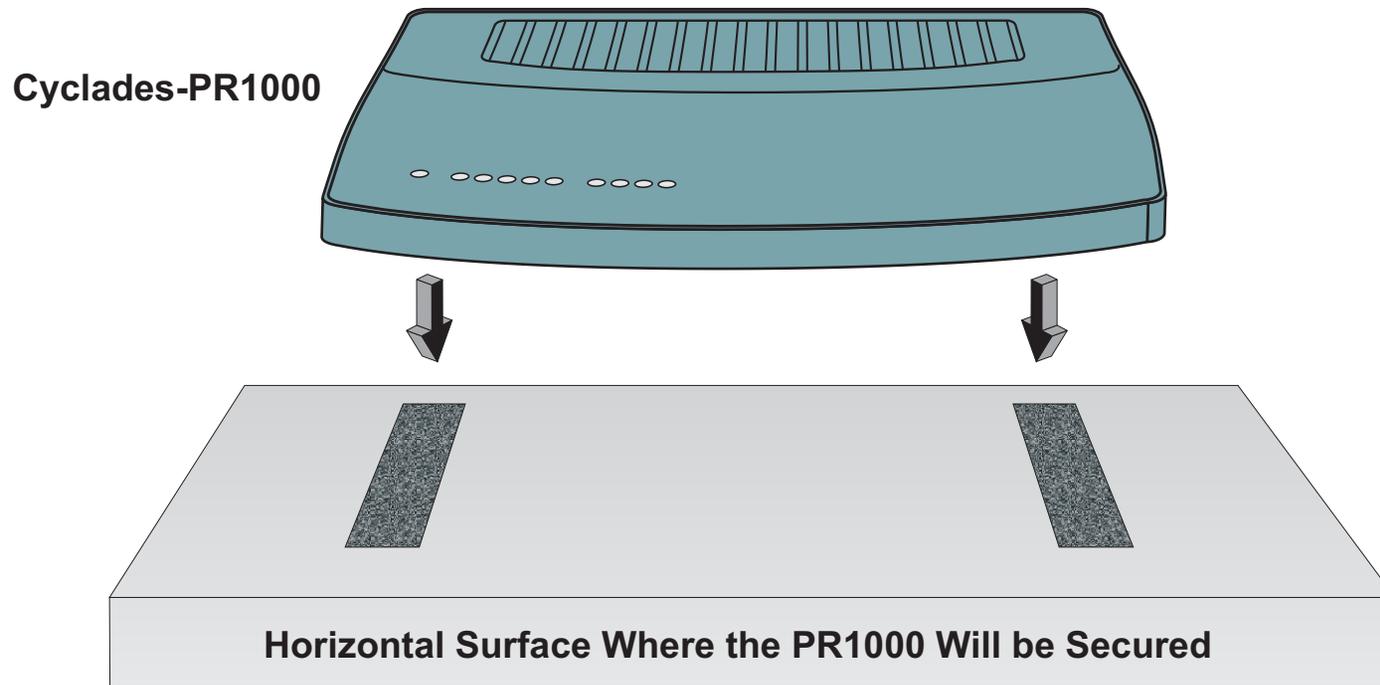
FIGURE 2.4 HOW TO ATTACH THE PR1000 TO A HORIZONTAL SURFACE

Vertical Surfaces

There are two slots in the base of the PR1000 to allow it to be affixed to a vertical surface. Screws and nylon fixings (for cement walls) are provided for this purpose.

Make holes 184,8mm (7.27 in) apart on the vertical surface. If using a drill, a 5mm bit should be used. Four millimeters (or a little more than 1/8 in) of the screw should be exposed (not counting the head).

Cyclades-PR1000

**Two 5mm Ø Screws
with Nylon Fixings**

← **Screw Slot**

←—— **184,8 mm or 7.27 in** ——→

**Vertical Surface Where
the PR1000 Will be Secured**
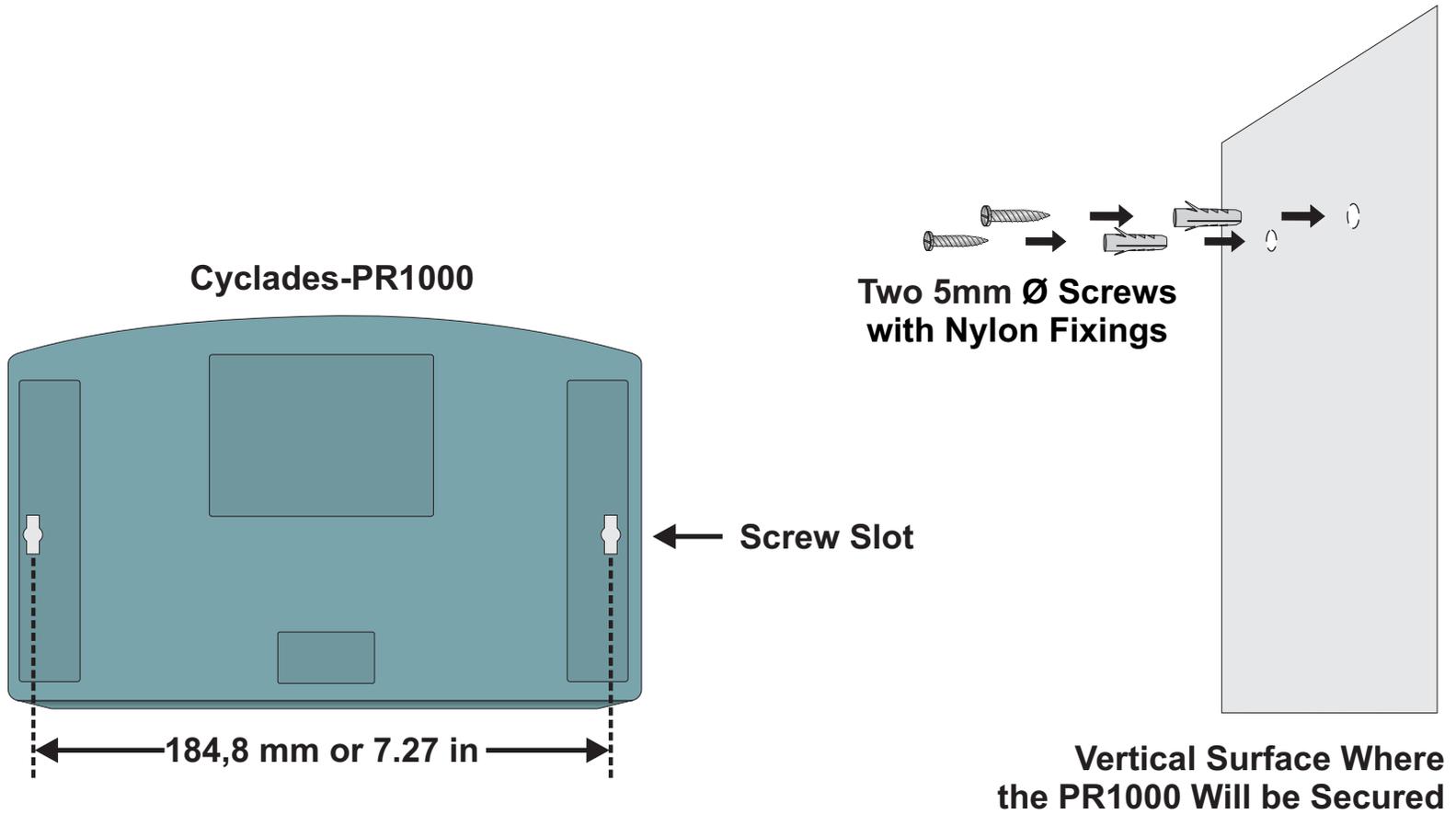
FIGURE 2.5 POSITIONING OF SCREWS

Cyclades-PR1000

Place the center of the screw slots over the screws and slide the router down so the screws hold the router in place as shown in Figure 2.6.

Cyclades-PR1000

**Vertical Surface Where
the PR1000 Will be Secured**
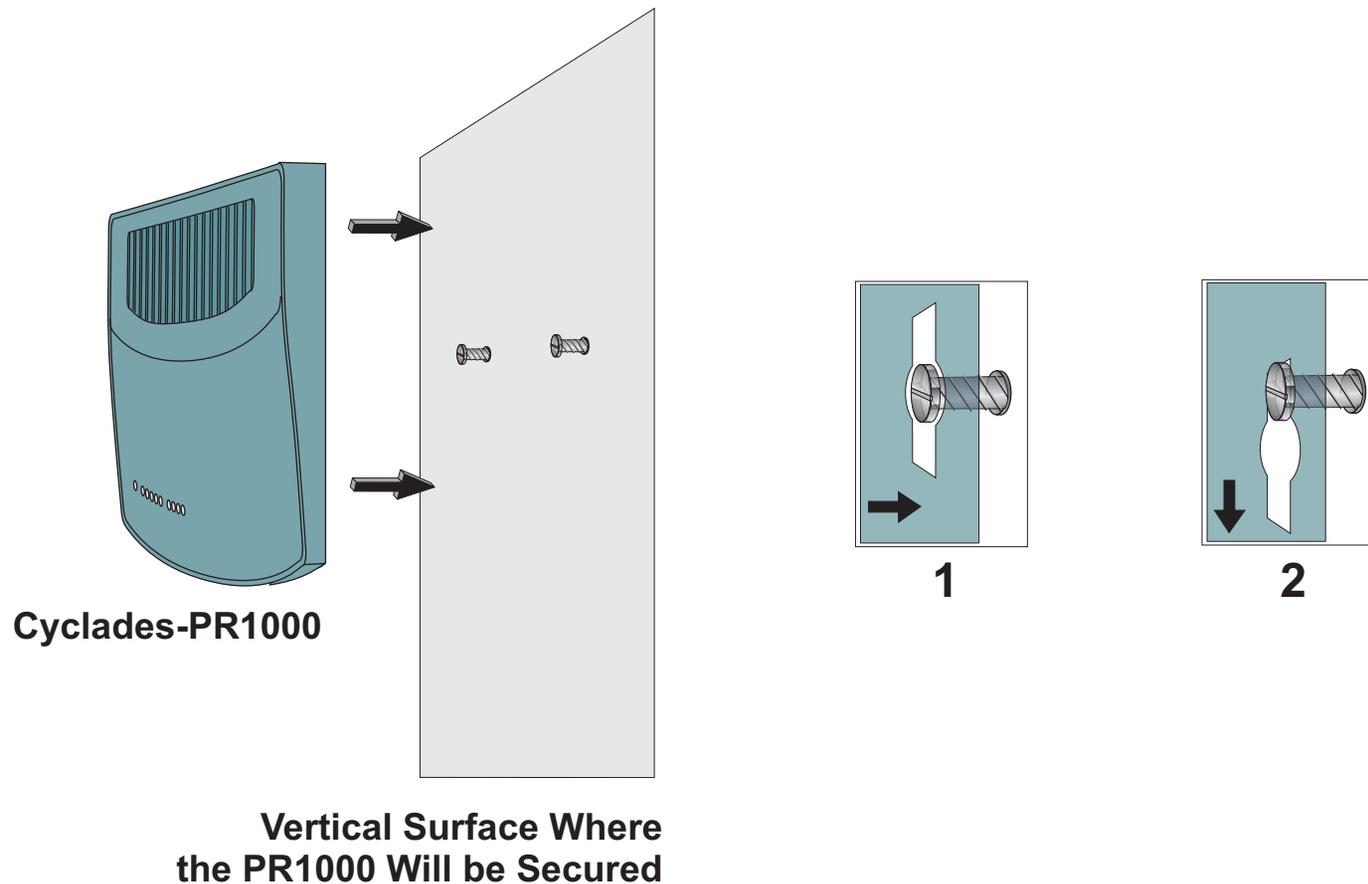
FIGURE 2.6 HOW TO ATTACH THE PR1000 TO A VERTICAL SURFACE

Note that the PR1000 can be hung with the LEDs facing up or facing down, whichever is more convenient.

Chapter 3 Using CyROS Menus

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

- Traditional menu interface using a console or Telnet session,
- CyROS Management Utility based on interactive HTML pages,
- 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

```
[PR1000] login : super
[PR1000] 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

Cyclades-PR1000

Once the console connection is correctly established, a Cyclades banner and login prompt should appear on the terminal screen. Pressing <ESC> during the boot process will temporarily halt initialization and present several options: IP address of the router, IP address of the boot server, boot from network, MAC address, etc. If the login prompt does not appear, see the first section of the troubleshooting appendix for help. Next, 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 10 of the installation manual and at the end of every example in chapter 4. The login prompts and main menu are shown in Figure 3.1.

All menus have the following elements:

- Title – In the example in Figure 3.1: "Main Menu".
- Prompt – The text: "Select Option ==>".
- 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 character ("+" 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 forwards you 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 configurations.

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 undo 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.
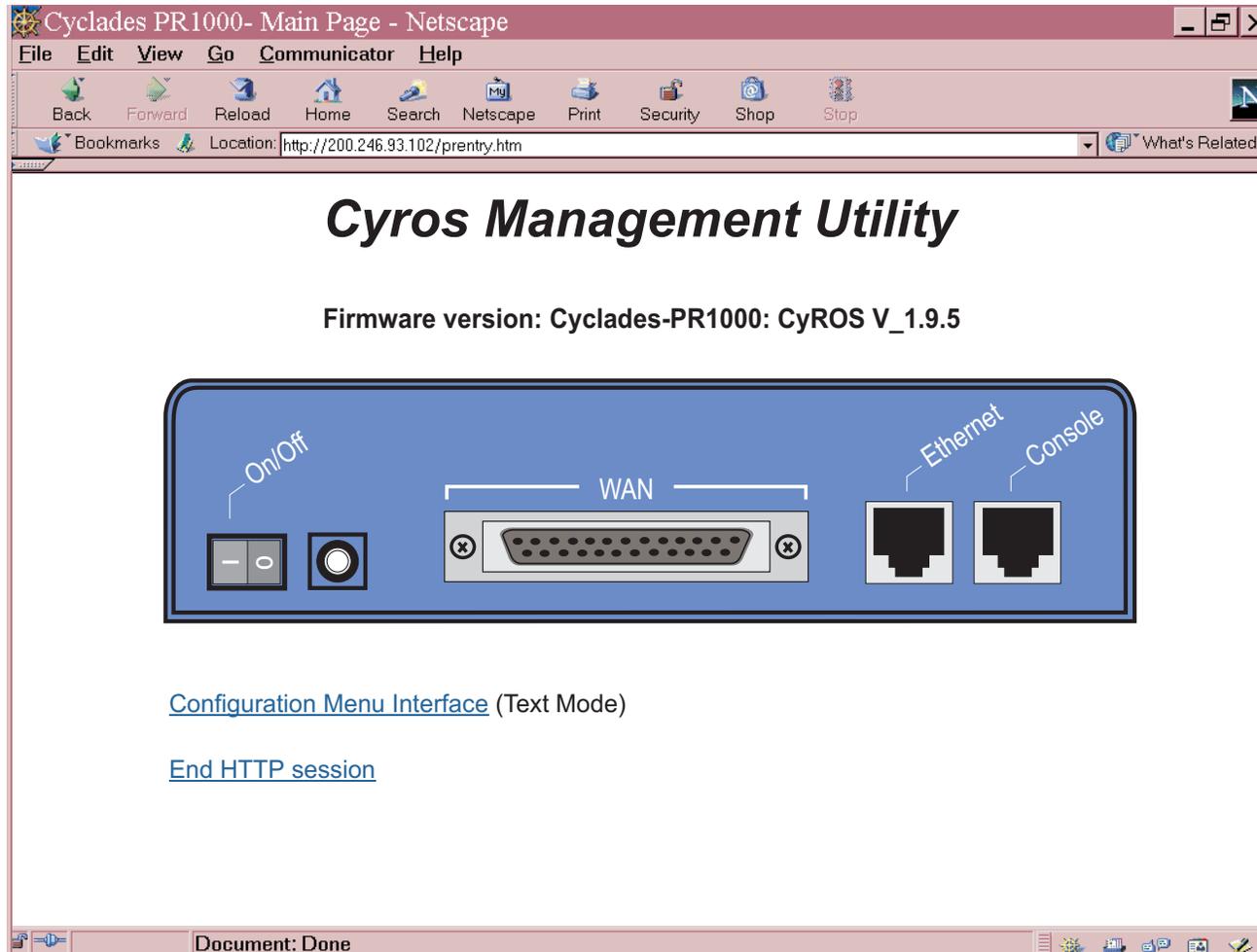
FIGURE 3.2 CYROS MANAGEMENT UTILITY HOME PAGE

Cyclades-PR1000

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. Clicking on *End HTTP Session* will terminate the connection.

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 Manual, when needed.

Example 1 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 4.1 shows the example system used in this section. Note that this example assumes that the IP address to which the network IP addresses will be translated is assigned dynamically by the Internet Service Provider. For configuration of a known IP address, see the chapter on NAT configuration in the complete Installation Manual. 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.
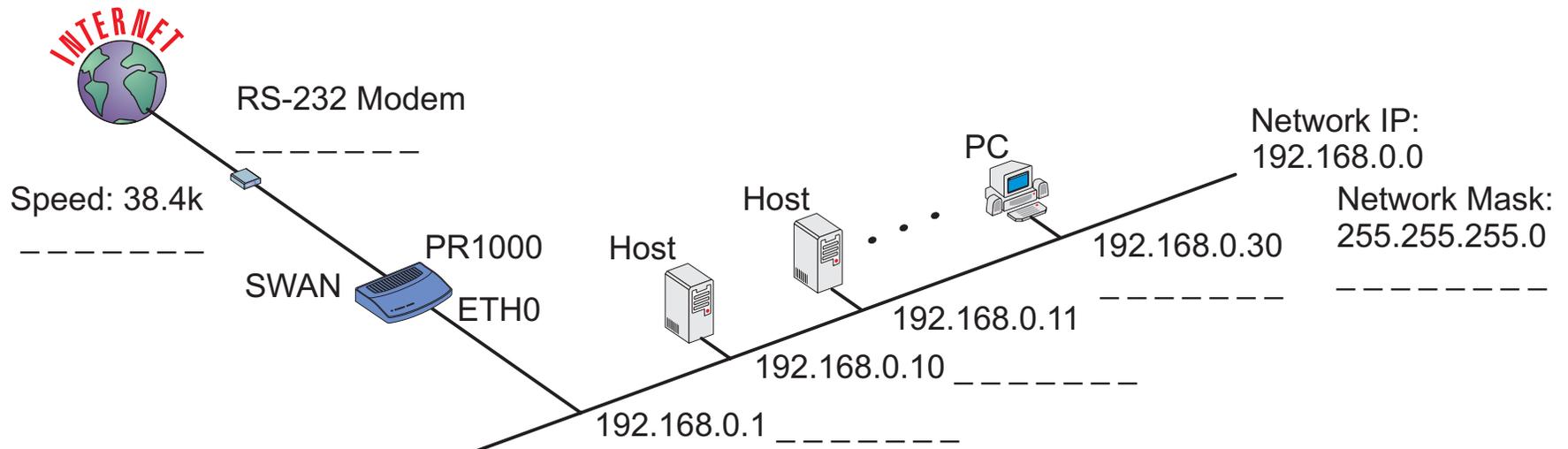
FIGURE 4.1 CONNECTION TO ACCESS PROVIDER USING A SWAN INTERFACE AND A MODEM

✅ 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 4.2. 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 Manual.

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.	
this table continued		

FIGURE 4.2 ETHERNET NETWORK PROTOCOL MENU PARAMETERS

Parameter	Example	Your Application
IP fragmentation - Ignore Bit DF	Yes	
NAT	Local	
ICMP Port	Inactive	
Incoming Rule List	None, filters are not included in this example.	
Outgoing Rule List Name	None, filters are not included in this example.	
Proxy ARP	Inactive	
IP Bridge	Inactive	

FIGURE 4.2 ETHERNET NETWORK PROTOCOL MENU PARAMETERS (CONTINUED)

STEP TWO

No more parameters are necessary for the Ethernet interface. The other interface to be configured is the SWAN. The SWAN physical media parameters are shown in Figure 4.3. Fill in the values for your application. The SWAN configuration is described in more detail in chapter 6 of the Installation Manual.

Menu CONFIG=>INTERFACE=>SWAN=>PHYSICAL		
Parameter	**Example**	**Your Application**
Mode	Asynchronous	
Speed	38.4k	

FIGURE 4.3 SWAN PHYSICAL MENU PARAMETERS

STEP THREE
The network protocol parameters, shown in Figure 4.4, are similar to those for the Ethernet interface. Fill in the parameters for your network in the right-most column.

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	
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	*Global Assigned* because the IP address of the SWAN interface will be assigned dynamically.	
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	
ICMP Port	Inactive	
Incoming Rule List Name	None, filters are not included in this example.	
Outgoing Rule List Name	None, filters are not included in this example.	
Routing of Broadcast Messages	Inactive	

FIGURE 4.4 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 8 of the Installation Manual 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	
Connection Type	Dial-Out	

FIGURE 4.5 PPP ENCAPSULATION MENU PARAMETERS

STEP FIVE

Since a modem is used in the example, the dial-out table must be configured. This is done as shown in Figure 4.6.

Menu CONFIG=>SYSTEM=>MODEMS=>DIAL OUT TABLE=>ADD		
Parameter	**Example**	**Your Application**
IP Address	Type in any valid IP address not on the local network.	
Init String	at	
Dial String	atdt+phone number of access provider.	
Authentication Method	PAP/CHAP/BOTH—depends on the service provider.	
Login Name	Login name device receiving call is expecting.	
Password	Password device receiving call is expecting.	

FIGURE 4.6 MODEM DIAL-OUT TABLE PARAMETERS

STEP SIX

Two static routes must be added to tell the router that all traffic not intended for the local LAN should be sent to the Access Provider. Chapter 9 of the Installation Manual explains static routes and other routing methods available in CyROS. Fill in the spaces in Figures 4.7 and 4.8 with the values for your application.

Menu CONFIG=>STATIC ROUTES=>IP=>ADD ROUTE		
Parameter	**Example**	**Your Application**
Destination IP Address	This IP address must match *the IP address* given in figure 4.6 (CONFIG=>SYSTEM=>MODEMS=> DIAL OUT TABLE=>ADD=>IP ADDRESS)	
Subnet Mask	The subnet mask for *the Destination IP Address*.	255.255.255.255
Gateway or Interface	Interface	
Interface	SWAN	
Is This a Backup Route?	No	
OSPF Advertises This Static Route	No	

FIGURE 4.7 STATIC ROUTE MENU PARAMETERS FOR INTERFACE ROUTE

Menu CONFIG=>STATIC ROUTES=>IP=>ADD ROUTE		
Parameter	**Example**	**Your Application**
Destination IP Address	Type in the word "DEFAULT".	
Gateway or Interface	Gateway	
Gateway IP address	Use the same value as for Destination IP Address in the previous table.	
Metric	1	
Is This a Backup Route?	No	
OSPF Advertises This Static Route	No	

FIGURE 4.8 STATIC ROUTE MENU PARAMETERS FOR GATEWAY ROUTE

STEP SEVEN

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 4.9 NAT GENERAL PARAMETERS

STEP EIGHT

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 be discarded.

Menu CONFIG =>SECURITY =>NAT =>LOCAL ADDRESS =>ADD RANGE		
Parameter	**Example**	**Your Application**
First IP Address	192.168.0.10	
Last IP Address	192.168.0.30	

FIGURE 4.10 NAT LOCAL ADDRESS RANGE MENU PARAMETERS

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

STEP NINE
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 TEN
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 backup of the configuration file (in binary) and print out a listing of the configuration.

Instructions for creating a backup 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 in a text file and/or printed on a printer.

Example 2 A LAN-to-LAN Example Using Frame Relay

This section will guide you through a complete router installation for the connection of two LANs via Frame Relay. Figure 4.11 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.

Central Office's LAN

Network IP: 100.130.130.0
_ _ _ _ _ _ _ _
Mask: 255.255.255.0
_ _ _ _ _ _ _ _

Network IP: 15.0.0.0
_ _ _ _ _ _ _ _
Mask :255.255.255.0
_ _ _ _ _ _ _ _

Remote Site's LAN

ETH0 PR1000

200.240.230.2
_ _ _ _ _ _ _ _

PR1000

100.130.130.1
_ _ _ _ _ _ _ _

SWAN

_ _ _ 128 Kbps
Connection

16

200.240.230.1
_ _ _ _ _ _ _ _

V.35 DSU/CSU
_ _ _ _ _ _ _ _

Public
Frame Relay
Network

Network IP: 200.240.230.0 _ _ _ _ _ _ _ _ _
Mask :255.255.255.240 _ _ _ _ _ _ _ _ _
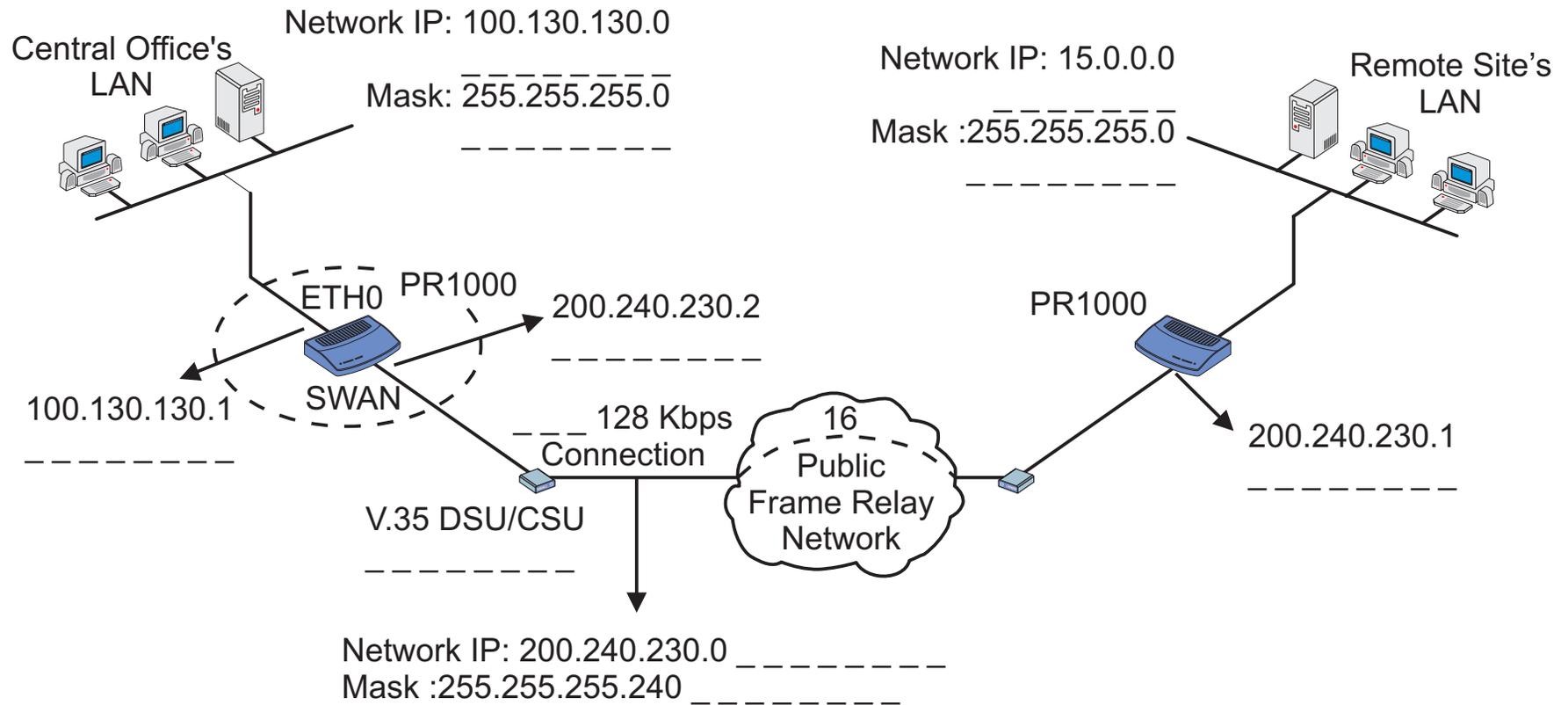
FIGURE 4.11 CENTRAL OFFICE AND REMOTE SITE CONNECTED USING SWAN INTERFACES

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 4.12. 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 Manual.

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 Unnumbered	Numbered	
Primary IP Address	100.130.130.1	
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.	
IP Fragmentation - Ignore Bit DF	Yes.	
NAT	Global, because NAT is not being used in this example.	
ICMP Port	Inactive	
Incoming Rule List	None, filters are not included in this example.	
Outgoing Rule List Name	None, filters are not included in this example.	
Routing of Broadcast Messages	Inactive	
Proxy ARP	Inactive	

FIGURE 4.12 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 4.13. Fill in the values for your application. The SWAN configuration is described in more detail in chapter 6 of the Installation Manual.

Menu CONFIG=>INTERFACE=>SWAN=>PHYSICAL		
Parameter	**Example**	**Your Application**
Mode	Synchronous.	
Clock Source	When the interface is connected to a DSU/CSU, the *Clock Source* is *External*.	
Media for SWAN Cable	V.35 in the example because the DSU/CSU is V.35. The type of cable is detected by the router, so if the correct cable is connected to the DSU/CSU the router will choose this value as the default.	

FIGURE 4.13 SWAN PHYSICAL MENU PARAMETERS

STEP THREE

The network protocol parameters, shown in Figure 4.14, are similar to those for the Ethernet interface. Fill in the parameters for your network in the right-most column.

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	200.240.230.2	
Subnet Mask	255.255.255.240 is the mask in the example.	
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.	
IP Fragmentation - Ignore Bit DF	Yes.	
NAT	Global, because NAT is not being used in this example.	
ICMP Port	Inactive	
Incoming Rule List	None, filters are not included in this example.	
Outgoing Rule List Name	None, filters are not included in this example.	
Routing of Broadcast Messages	Inactive	

FIGURE 4.14 SWAN NETWORK PROTOCOL (IP) MENU PARAMETERS

STEP FOUR

The Encapsulation parameters for Frame Relay 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 8 of the Installation Manual for more information if necessary.

Menu CONFIG=>INTERFACE=>SWAN=>ENCAPSULATION=>FRAME RELAY		
Parameter	**Example**	**Your Application**
Encapsulation Type	Choose RFC1490 unless the router at the other end of the connection uses the default Cisco standard.	
SNAP IP	*Inactive* for the example. The router on the sending end must be using the same header type (NLPID or SNAP) as the router on the receiving end.	
LMI	ANSI for the example. This must also be the same as the router on the receiving end.	
T391	Ten seconds, the interval between the LMI Status Enquiry messages.	
N391	Six.	
N392	Three.	
N393	Four. This value must be larger than N392.	
Bandwidth Reservation	Inactive. Traffic control will not be covered in this example	
FRF-12 - Fragment Size	Indicates the size of FRF-12 fragments. Use default value.	
Voice over this link	Inactive.	

FIGURE 4.15 FRAME RELAY ENCAPSULATION MENU PARAMETERS

At the end of the parameter list shown above, the DLCI menu appears. Choosing Add DLCI will lead to the parameters shown in Figure 4.16. The <ESC> key used at any time during the Frame Relay encapsulation parameter list will also bring up the DLCI menu. A DLCI entry must be created for every remote Frame Relay network to be contacted. In the example, only one is shown.

Menu CONFIG=>INTERFACE=>SWAN=>ENCAPSULATION=>FRAME RELAY=><ESC>=>ADD DLCI		
Parameter	**Example**	**Your Application**
DLCI Number	Sixteen. This number is supplied by the Public Frame Relay network provider.	
Frame Relay Address Map	*Static,* which maps one IP address to this DLCI.	
IP Address	200.240.230.1	
CIR	90 percent. 100 minus this number is the percentage of total bandwidth that may be discarded if the network is congested.	
Enable Predictor Compression	Yes, if Cyclades routers are used on both ends of the link and Predictor Compression is enabled on both routers. This feature is effective only for links running at speeds under 2 Mbps.	
Number of Bits for Compression	Sixteen when both routers are of the PR line. Ten must be used if the other router is a PathRouter.	

FIGURE 4.16 DLC CONFIGURATION MENU PARAMETERS

STEP FIVE

Now that the central office's LAN has been defined, a route must be added to tell the router that the remote site's LAN is at the other end of the line. Creating a static route is the simplest way to do this. Chapter 9 of the Installation Manual explains static routes and other routing methods available in CyROS. Fill in the spaces in Figure 4.17 with the values for your application.

Menu CONFIG=>STATIC ROUTES=>IP=>ADD ROUTE		
Parameter	**Example**	**Your Application**
Destination IP Address	15.0.0.0	
Subnet Mask	255.255.255.0	
Gateway or Interface	gateway	
Gateway IP Address	200.240.230.1	
Metric	One -- number of routers between router being configured and the destination IP address.	
Is This a Backup Route?	No	
OSPF Advertises This Static Route	No	

FIGURE 4.17 STATIC ROUTE MENU PARAMETERS

STEP SIX

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.

STEP SEVEN
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 backup of the configuration file (in binary) and print out a listing of the configuration.

Instructions for creating a backup 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 in a text file and/or printed on a printer.

CHAPTER 5   CONFIGURATION OF THE ETHERNET INTERFACE

The PR1000 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	Does not apply to Expanded NAT. Determines the type of IP address if NAT is being used. Use *Global* otherwise. See chapter 11 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 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 in chapter 10. 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 affecting 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.
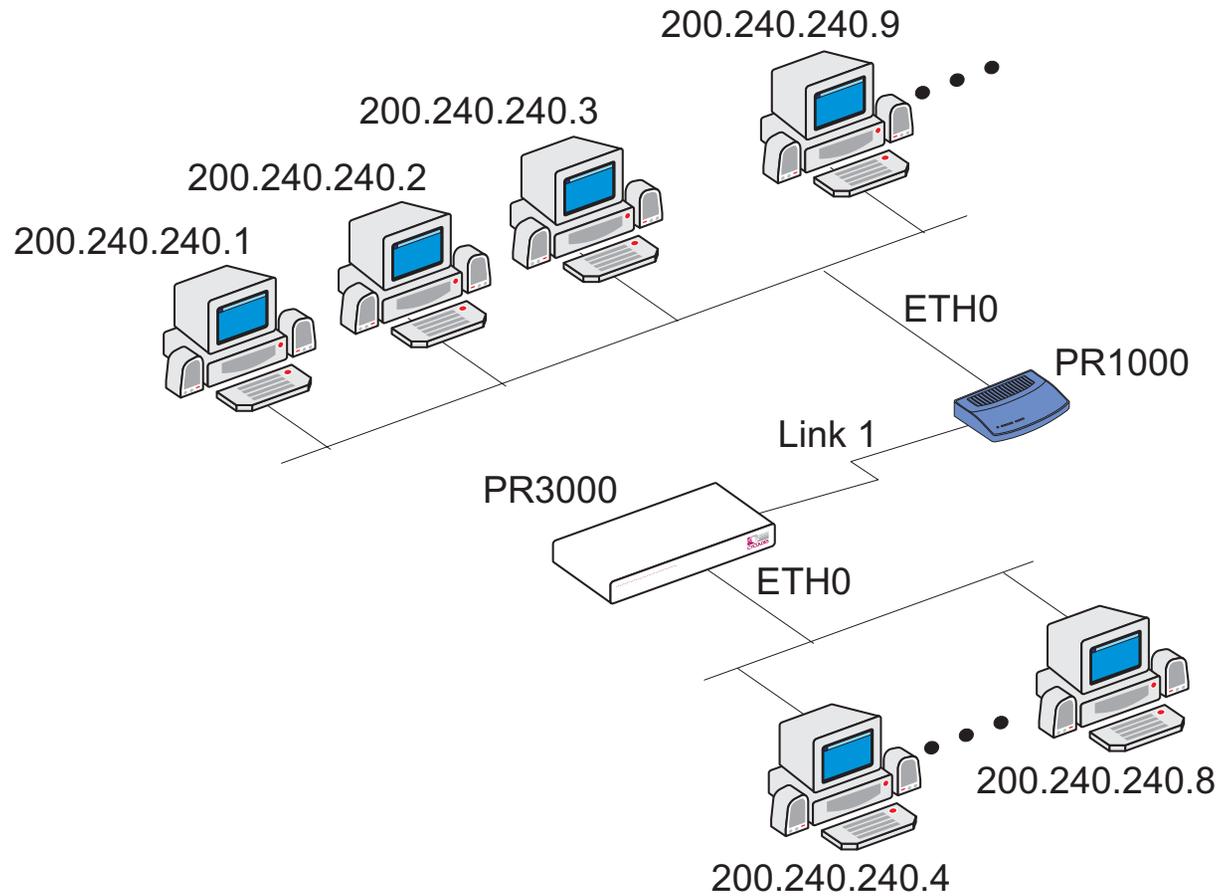
FIGURE 5.1 IP BRIDGE EXAMPLE

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 13. 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 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 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 13) 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 ┬ Status
                                       Bridge   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.
IP Fragmentation - Ignore Bit DF	When this parameter is set to No, the DF (Do Not Fragment) bit in the IP header causes IP to reject a packet that is oversized: the router sends an ICMP message back to the sender. When this parameter is Yes, the DF bit is ignored, the packet is fragmented, and no message is sent back to the sender.
NAT	Does not apply to Expanded 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 affecting 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 8 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.
Connection Type	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.

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 12 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 12. 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
Encapsulation Type	*RFC1490 - IETF* is the standard used by most equipment. The *Cisco* option should be used when the PR is communicating with a router configured to use the default Cisco standard.
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.
Bandwidth Reservation	Enables traffic control per DLCI. Traffic control options appear in the Add DLCI Menu.
Voice Over This Link	Enables the Voice over Frame Relay application.

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.
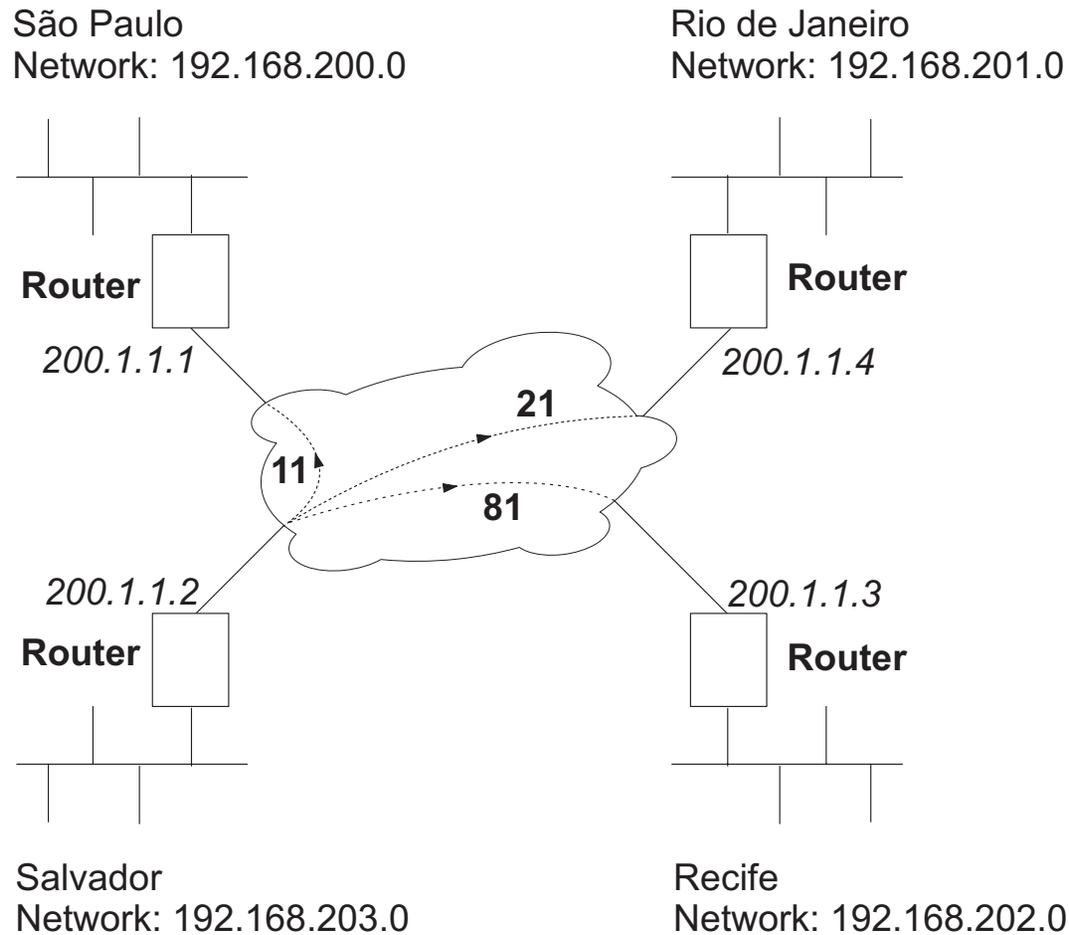

FIGURE 8.1 PERMANENT VIRTUAL CIRCUITS BETWEEN OFFICES

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.
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.
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 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.
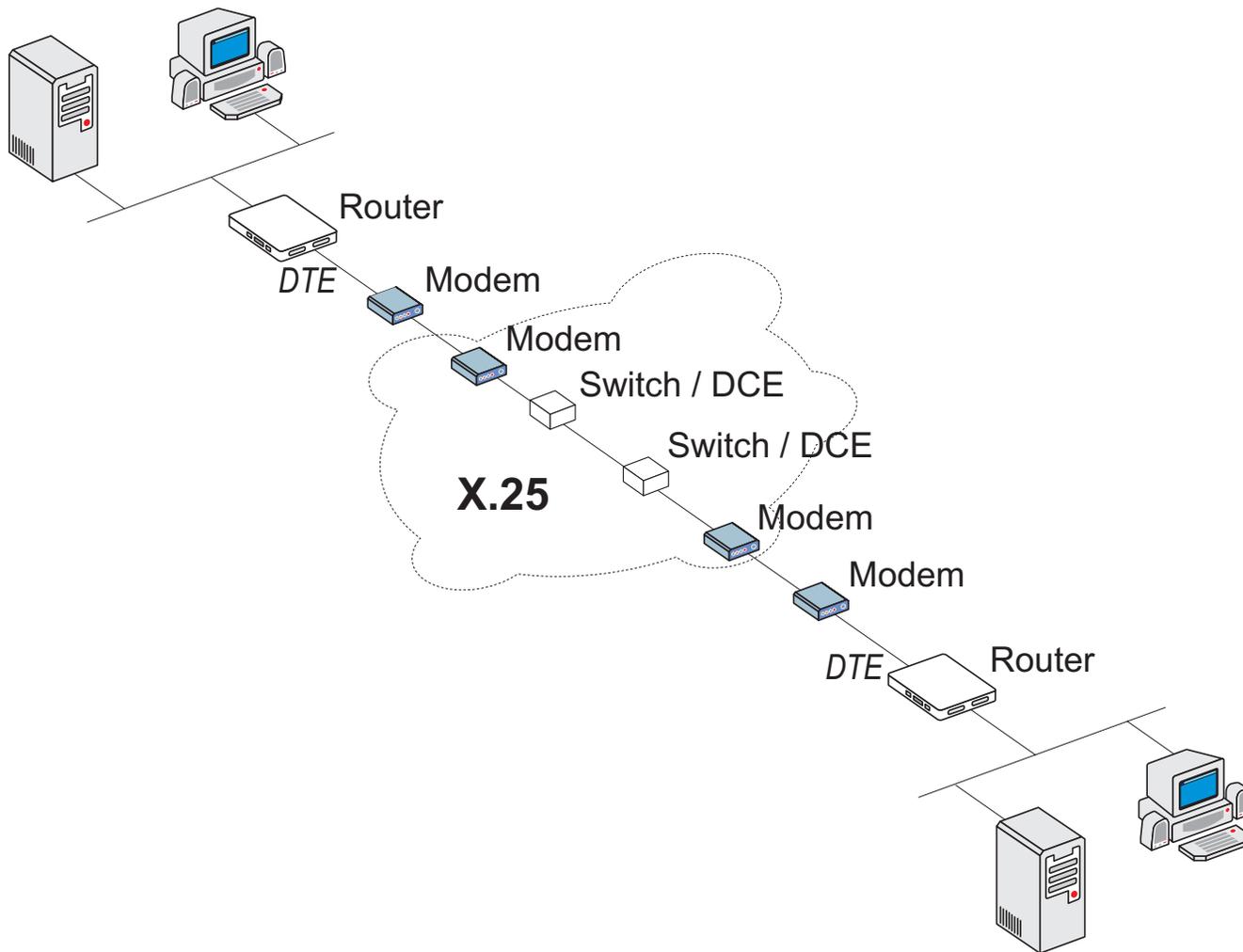

FIGURE 8.2   PUBLIC X.25 NETWORK EXAMPLE

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.

X.25 Menu (Continued)

Parameter	Description
Number of Virtual Circuits	Indicates the maximum number of virtual circuits (total of PVCs and SVCs) allowed on this interface. The maximum is 128.
Number of Permanent Virtual Circuits	Indicates the number of permanent virtual circuits that will be connected through this interface. This maximum is also 128.
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 9 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.

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.
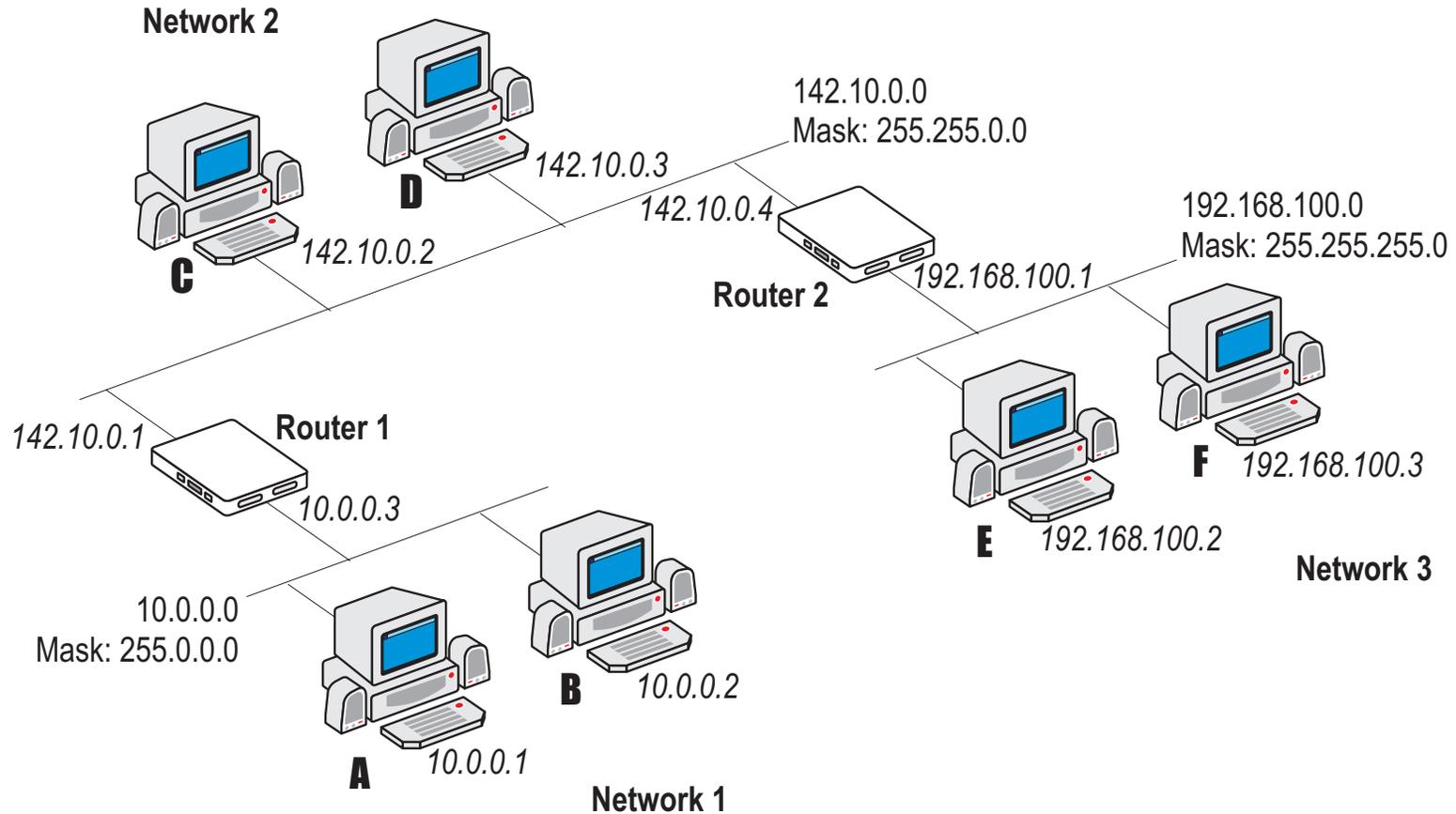
FIGURE 9.1 STATIC ROUTING EXAMPLE 1

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.
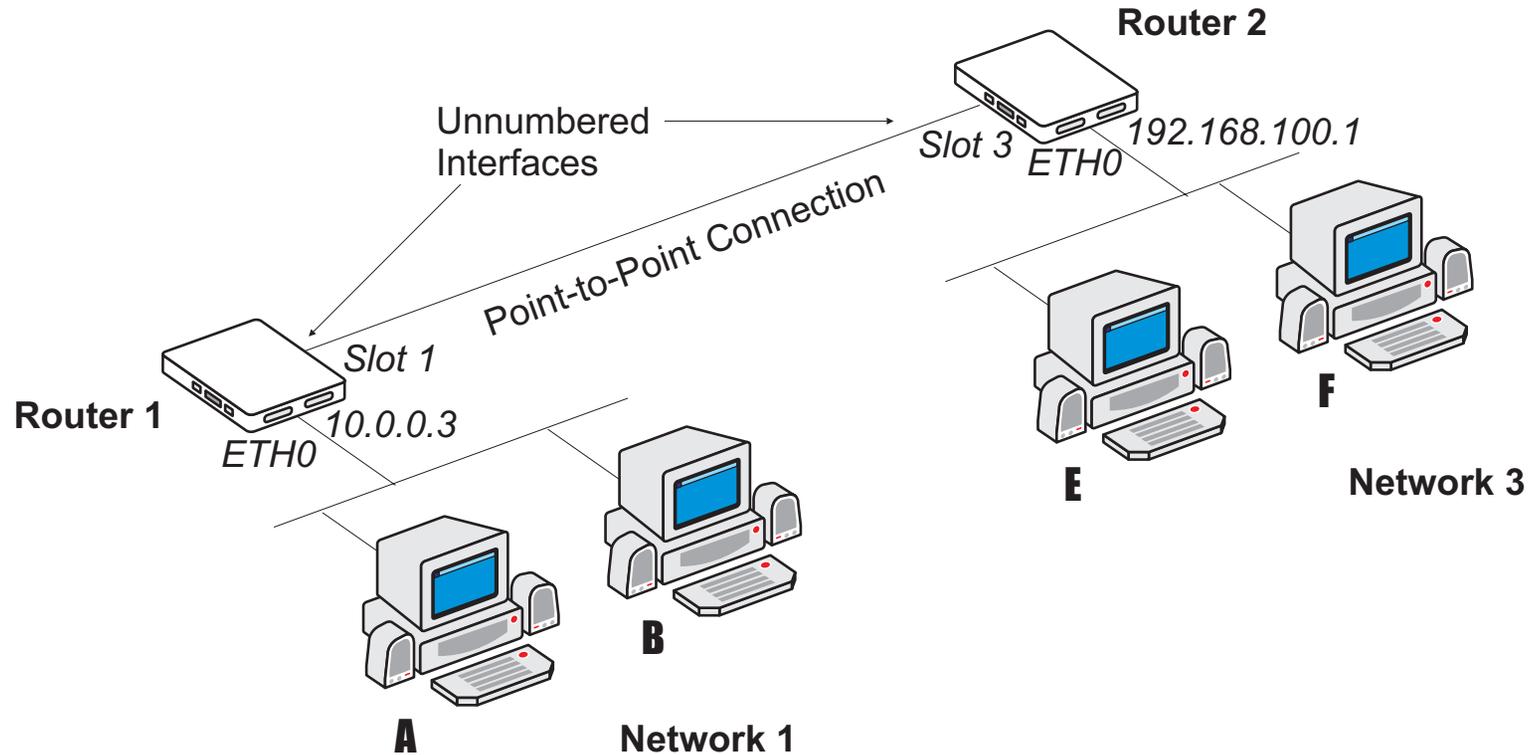
FIGURE 9.2 STATIC ROUTING EXAMPLE 2

Figure 9.2 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 9.3.
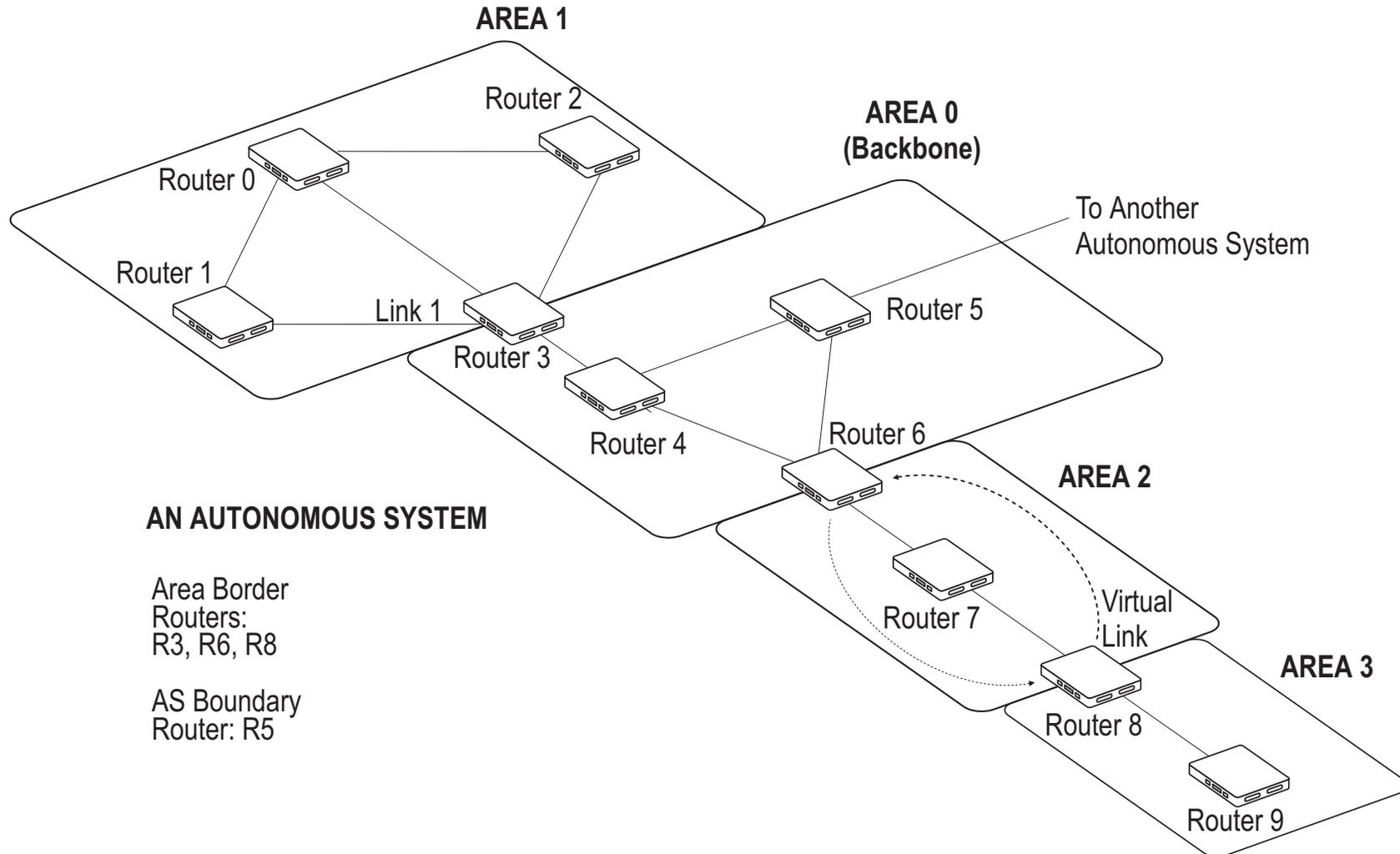

FIGURE 9.3 OSPF EXAMPLE

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).
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

OSPF Menu (Continued)

Parameter	Description
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.
Poll Interval in Seconds	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 continued	

OSPF Global Commands (Continued)

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.

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.
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.

CHAPTER 10 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 12.

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 11 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 (for reference, they are 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.16.255.255, and 192.168.0.0 - 192.168.255.255). These are used as local IP addresses. Figure 11.1 shows an example of the utility of NAT:

Global Address Range
- Network: 200.240.230.224
- Mask: 255.255.255.240

ftp
Server
192.168.0.30

Networks
192.168.0.0 &
200.200.200.0

Host

Host

200.240.230.2

PR1000 With
Expanded NAT

200.200.200.11

200.200.200.10

PC

192.168.0.5

WWW
Server
192.168.0.31

Router Ethernet Port
Primary IP Address: 192.168.0.1
Secondary IP Address: 200.200.200.1
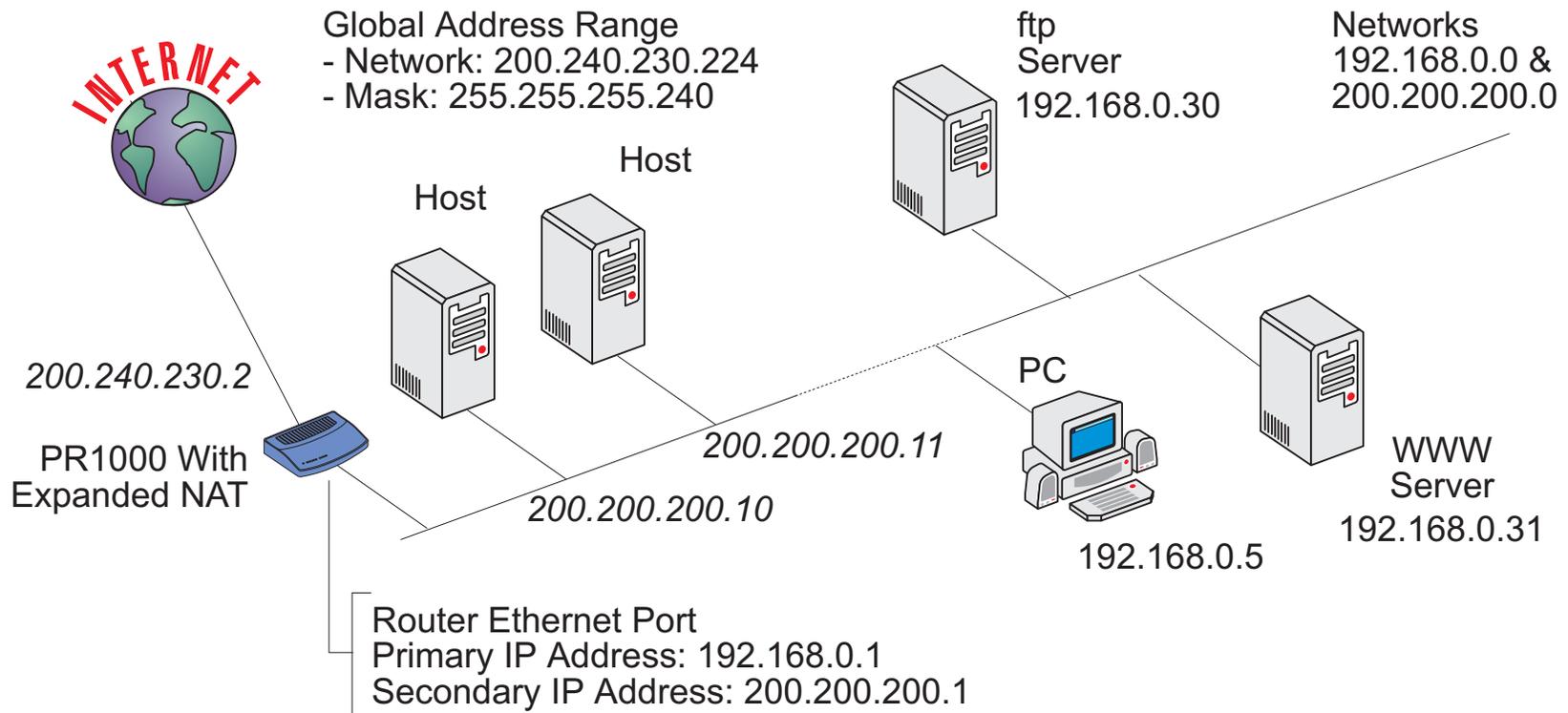
FIGURE 11.1 NAT EXAMPLE

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.

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 Expanded). Only the expanded 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 Expanded NAT version. If this parameter is changed, all NAT parameters are reset to the preset values.
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.

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	Applies to TCP and UDP protocols. 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	Applies only when Global Port provided. 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 12 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 |
  | Syslog Status |
Delete Rule — | Syslog Level |
Clear Rule List — Edit Rule

FIGURE 12.1 THE RULES LIST MENU TREE
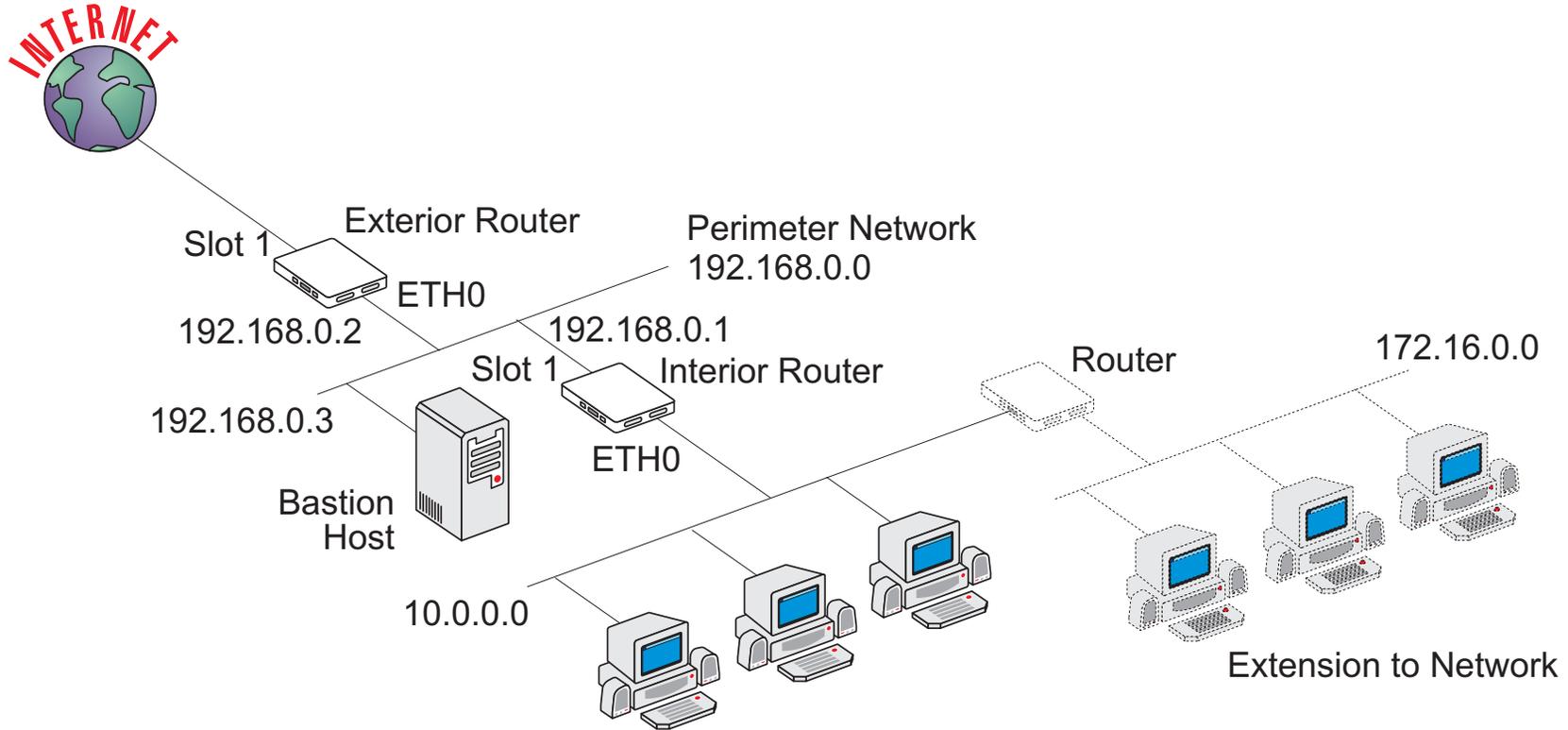
FIGURE 12.2 FIREWALL EXAMPLE

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.
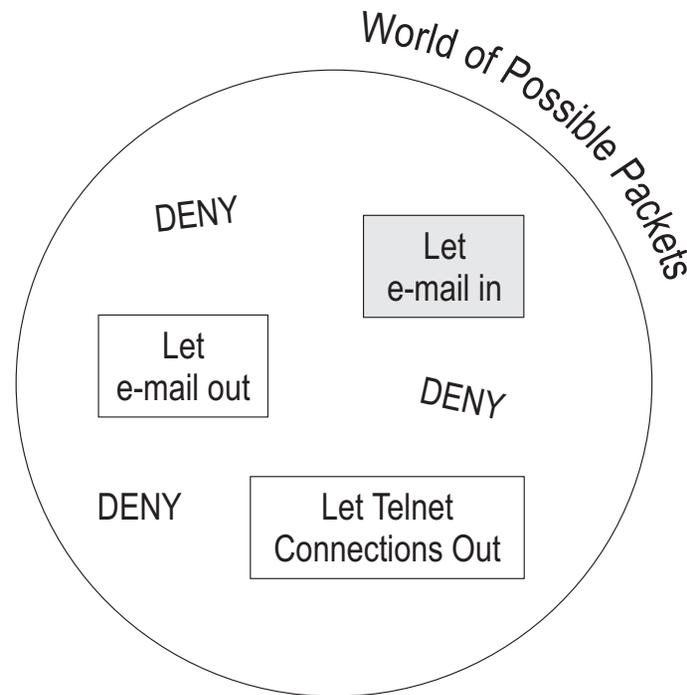

FIGURE 12.3 DENY AS DEFAULT SCOPE

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.

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.

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

## PROT OP   Source IP Address                OP    SRC PORT   CNX ACC LOG SC STA
             Destination IP Address                 DST PORT

0   TCP  --                                   --                Y   N   -  P  EN
        ==   192.168.0.3     255.255.255.255  ==      SMTP
-----------------------------------------------------------------------
FILTER_LIST NAME: exterior_out

## PROT OP   Source IP Address                OP    SRC PORT   CNX ACC LOG SC STA
             Destination IP Address                 DST PORT

0   TCP  ==   192.168.0.3     255.255.255.255  ==      SMTP    Y   N   -  P  EN
             --                                   --
```

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.
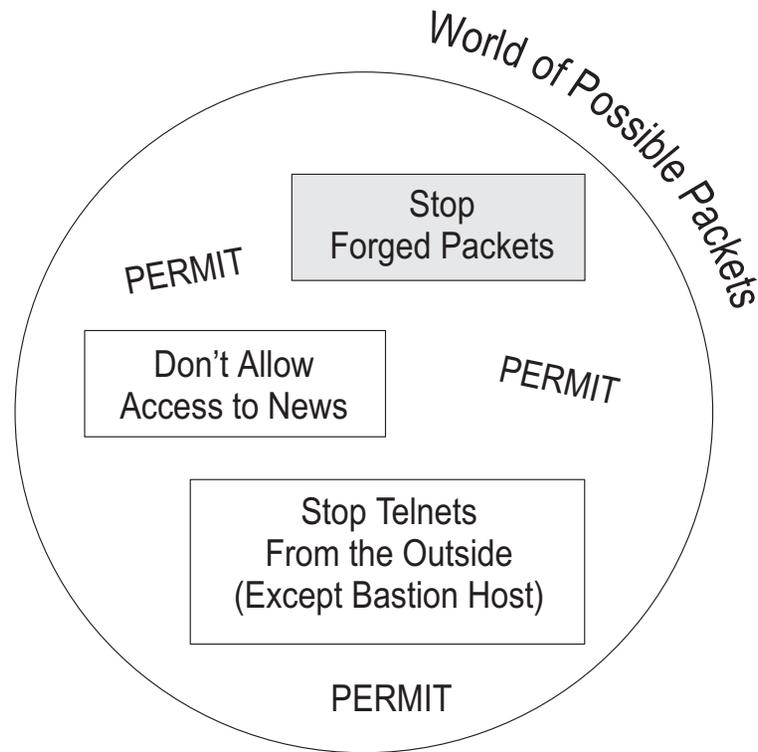

FIGURE 12.5 PERMIT DEFAULT SCOPE

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

```
Rules Lists

Rule List Name              Rule        Default    List        Linked
                            Status      Scope      Type        Rule List

Slot1_in                    Enabled     Permit     Filter


-----------------------------------------------------------------------------
FILTER_LIST NAME: Slot1_in

## PROT OP   Source IP Address                 OP    SRC PORT   CNX ACC LOG SC STA
             Destination IP Address                  DST PORT

0    -   ==  192.168.0.0      255.255.0.0      --                Y   N   -  D  EN
         --                                    --
```

`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:

Cyclades-PR1000

    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.
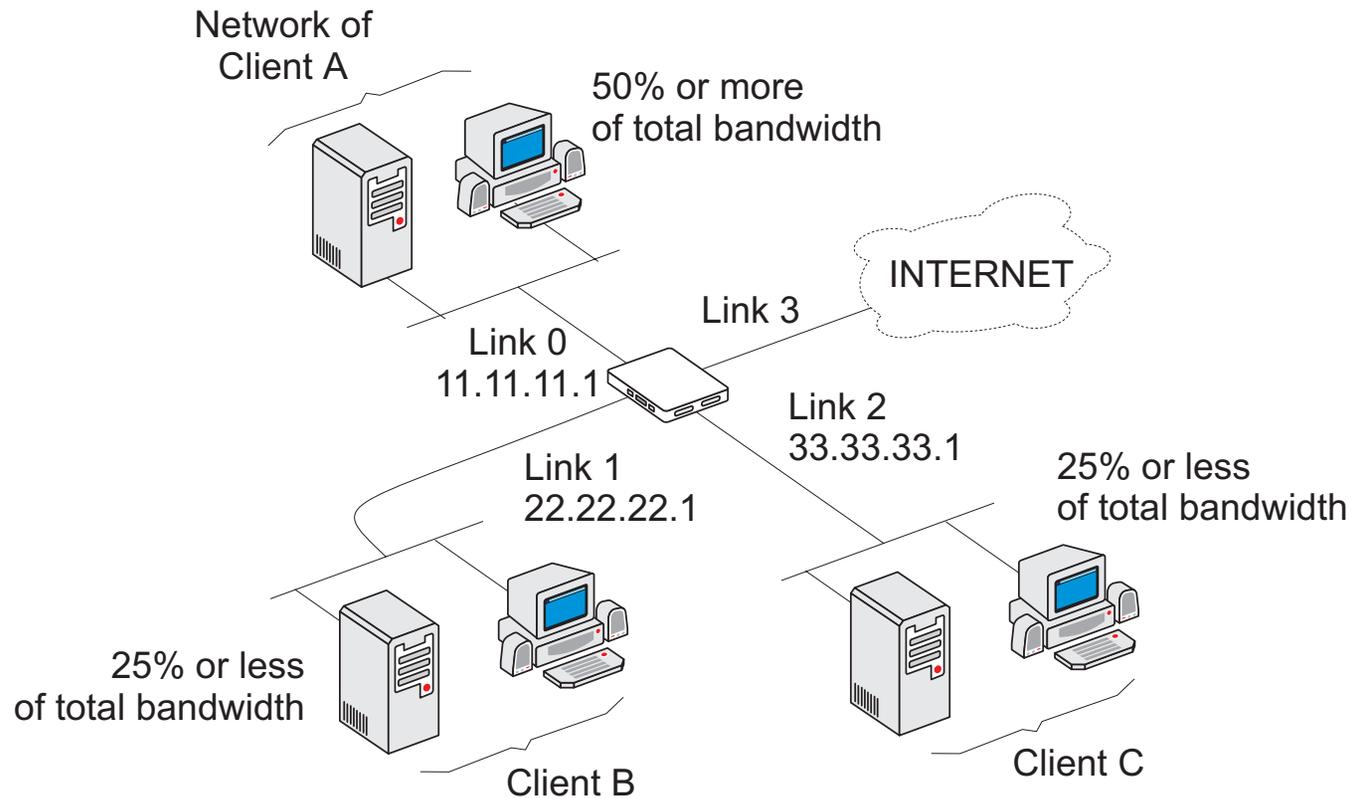
FIGURE 12.6 TRAFFIC RULE EXAMPLE 1

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.

Cyclades-PR1000

```
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         None
Operator
Source Port Operator   None
Destination Port       None
Operator
```

Cyclades-PR1000

```
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         None
Operator
Source Port Operator   None
Destination Port       None
Operator

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         None
Operator
Source Port Operator   None
Destination Port       None
Operator
```

FIGURE 12.7 OUTPUT SHOWING PARAMETERS FOR TRAFFIC RULE EXAMPLE 1

Cyclades-PR1000

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.)
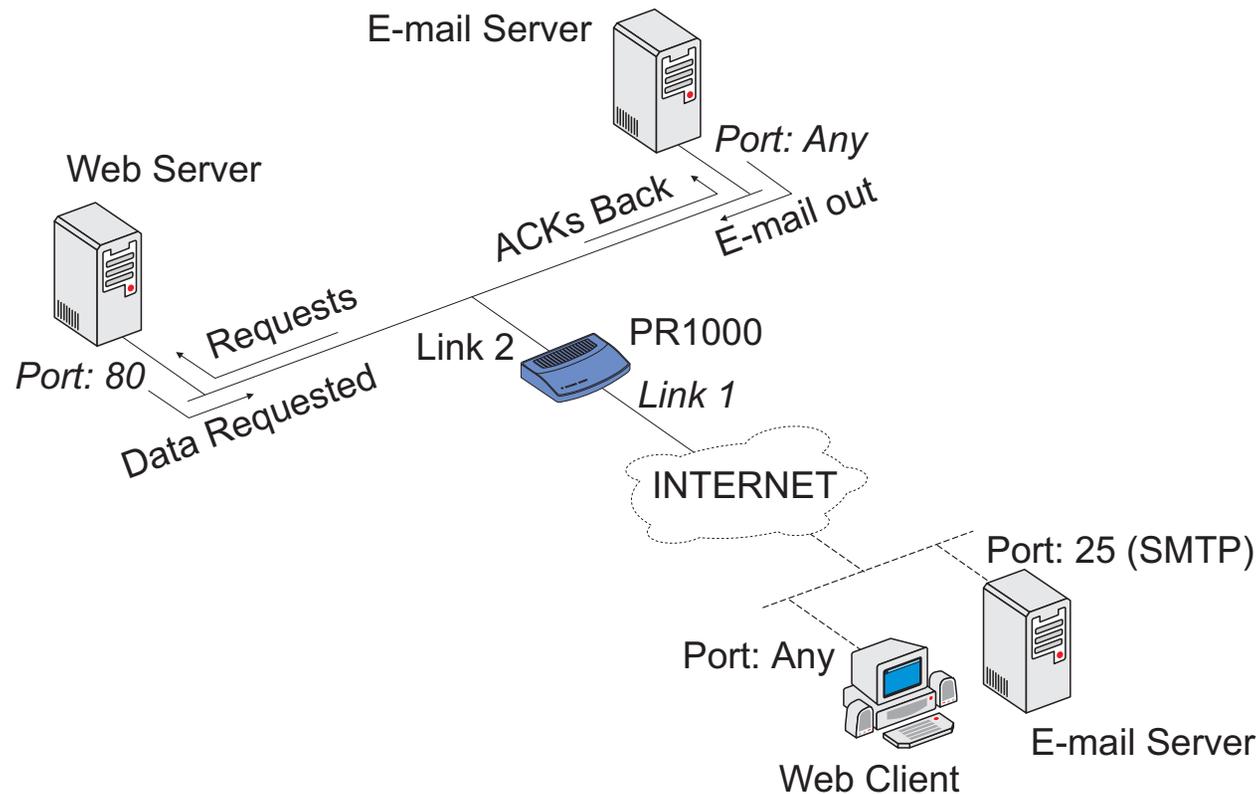

FIGURE 12.8 TRAFFIC RULE EXAMPLE 2

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

```
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
```

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.

CHAPTER 13 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.
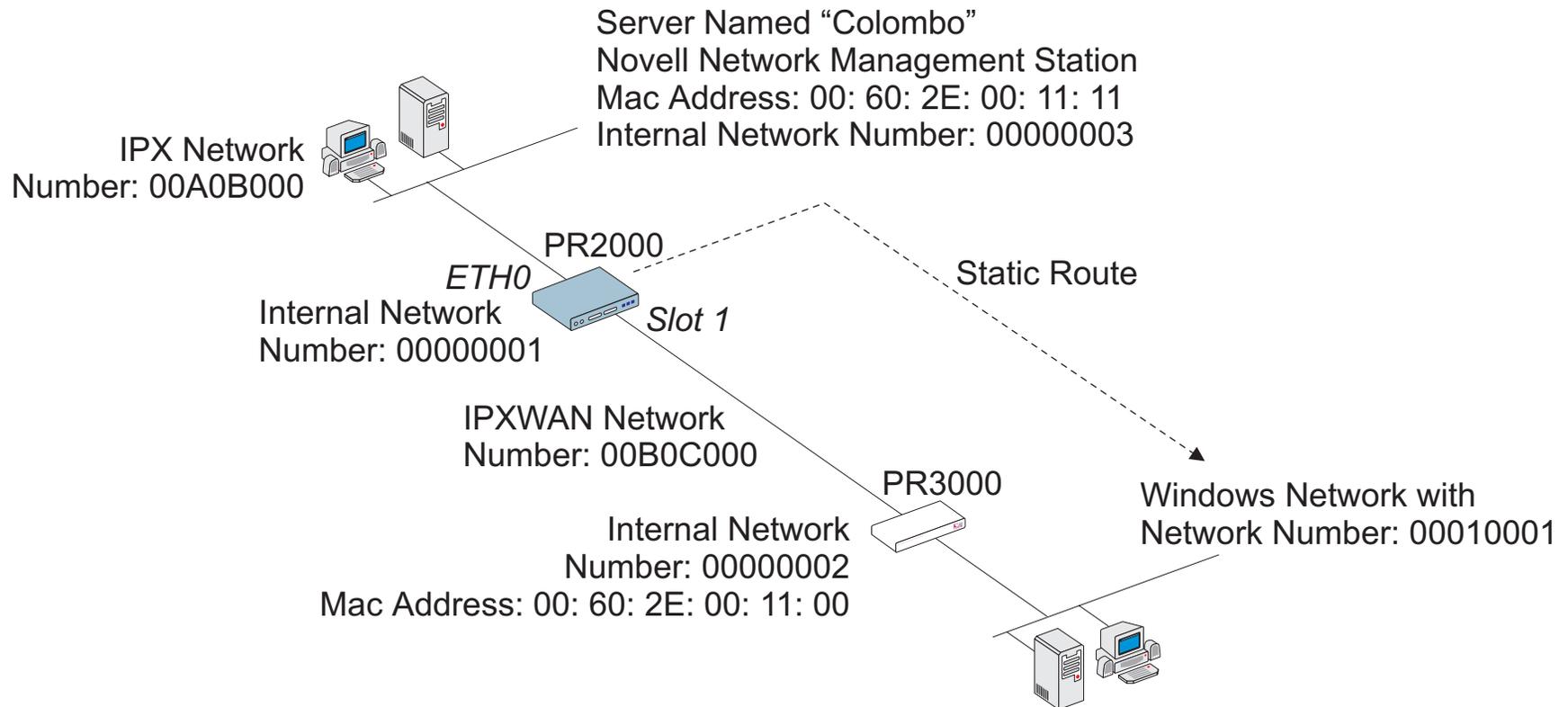

FIGURE 13.1 IPX NETWORK EXAMPLE

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 8. 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.

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 8. 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 8. 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 9. 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 14 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.
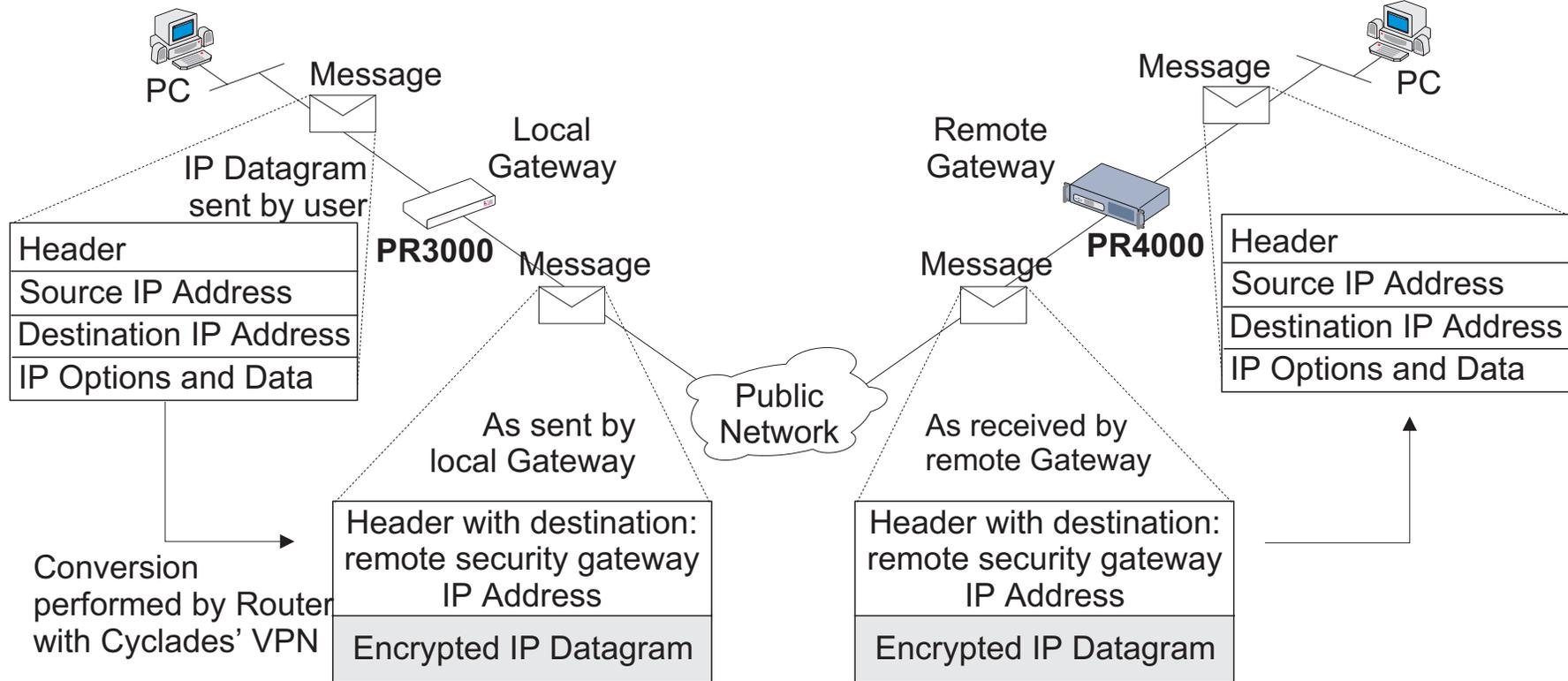
FIGURE 14.1 CONVERSION PERFORMED BY CYCLADES' VIRTUAL PRIVATE NETWORK UTILITY

Cyclades-PR1000

An example showing a local security network and two remote security networks is shown in Figure 14.2. The PR1000 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 PR1000 (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.

REMOTE SECURITY NETWORK 1

Router

Link 1
IP: 50.50.50.1

RSG1

IP:10..255.255.0

PR4000

LOCAL SECURITY NETWORK

IP: 10.0.0.0

RSG3 - Remote
Security Gateway

IP Network

Router IP Address:
9.9.9.1

Router

Link 2
IP: 190.190.190.1

Link 1
IP: 70.70.70.1

ETH0

PR3000

IP:172.16.0.0

Router IP Address:
190.190.190.1

REMOTE SECURITY NETWORK 2

Link 1
IP: 20.20.20.1

RSG2

PR2000

IP:192.168.0.0

Router IP Address:
20.20.20.1

FIGURE 14.2 VIRTUAL PRIVATE NETWORK EXAMPLE

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 9 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. Is the PC's COM port enabled? Is the Console cable being used? See Chapter 2 for instructions on which cables go where.

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.

3 While the router is booting, the LEDs labeled CPU, Tx, Rx and GP indicate the stage of the boot process, as shown in Figure A.1. When the router has started up properly, the CPU LED blinks consistently one second on, one second off.

Test	CPU	Tx	Rx	GP	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

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

1 Check that the cables are connected correctly and firmly (see chapter 2, What is in the Box, for correct cable connection information).

2 Confirm that the Link LED is lit, indicating proper Ethernet cable termination. If it is not lit, check both ends of the Ethernet cable and the hub connection.

3 Confirm that the CPU LED is blinking 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	CPU 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 CPU LED CODE INTERPRETATION

4 Make sure any external modem, DSU/CSU, or interface equipment is properly connected and that the interface configuration is correct. Many cables, for example, have a DB-25 connector, but are not interchangeable. Which cable is used for which type of modem is given in chapter 2.

Testing the Ethernet Interface

After configuring the Ethernet interface, return to the main menu using the <ESC> key as many times as is necessary. Save the configuration to flash memory (the operating system will ask how to save the configuration on the way back to the main menu). The simplest way to test the link is by using the ping application. 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.

```
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
```

Pinging the router from a host on the network should give similar results. If the test fails, confirm that the link LED 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.

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.

LEDs

The LEDs on the PR1000's case display the following information:

- **Power** - Lit when the PR1000 is turned on.
- **100TB** - Lit when the Ethernet link is being used for a fast Ethernet connection.
- **Link** - Lit when the Ethernet link is correctly terminated.
- **Col** - Indicates collisions on the LAN.
- **TX** - Indicates transmission of data to the LAN.
- **RX** - Indicates data received from the LAN.
- **CPU** - A steady one second on, one second off blinking pattern indicates that the CPU is working correctly. Other blinking patterns are described in Figure A.2.
- **TX** - Indicates transmission of data to the WAN.
- **RX** - Indicates data received from the WAN.
- **GP** - General Purpose LED reserved for future use.

Power

100BT

Col

Link

TX

RX

CPU

TX

RX

GP
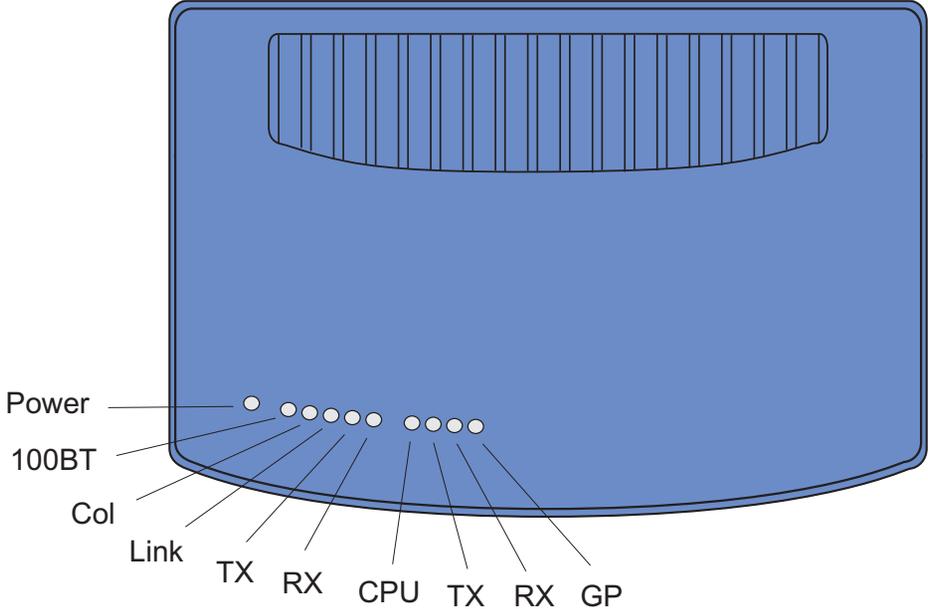
FIGURE A.3 LED PANEL

APPENDIX B HARDWARE SPECIFICATIONS

General Specifications

The Cyclades-PR1000 power requirements and environmental restrictions are listed in Figure B.1.

Power Requirements (external DC adapter)	
Input voltage range	90-264 VAC, 0.5A
Input frequency range	50-60 Hz, single phase
Maximum input surge current	40A cold start
Power dissipation max.	18W
Safety	UL1950, CUL, TUV EN60950
Line Conducted Noise	FCC PART 15J CLASS B, CISPR 22 CLA
MTBF	80,000 HOURS
Output plug	Standard DC plug, central pin positive, 2.1mm
Power Requirements (PR1000 case)	
Input voltage range	5 VDC +/- 5%
Current consumption type	0.5A @ 5VDC
Power dissipation type	2.5W
Power dissipation max.	5W
Approvals	FCC Class A, CE class A
Environmental Conditions	
Operating temperature	10C to 44C / 50F to 112F
Relative humidity	5% to 95%, non-condensing
Operating Altitude	12,000 feet max. (3660 m)

FIGURE B.1   GENERAL SPECIFICATIONS

External Interfaces

The WAN Interface

The WAN interface is provided on a DB-25 female connector. The pinout diagram is not shown here, as it depends on which protocol (RS-232, V.25 or X.21) is configured. Please see the pinout diagrams for the cables used for each protocol to determine the signals on the interface.
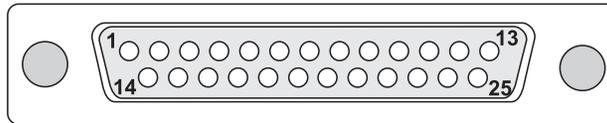

FIGURE B.2 SERIAL WAN INTERFACE - DB-25 FEMALE

The LAN Interface

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.
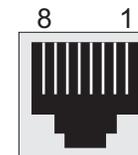
FIGURE B.3 10/100 BASE-T ETHERNET INTERFACE - RJ-45 FEMALE

The Console Interface

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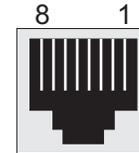
FIGURE B.4   CONSOLE INTERFACE - RJ-45 FEMALE

Cables

The 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
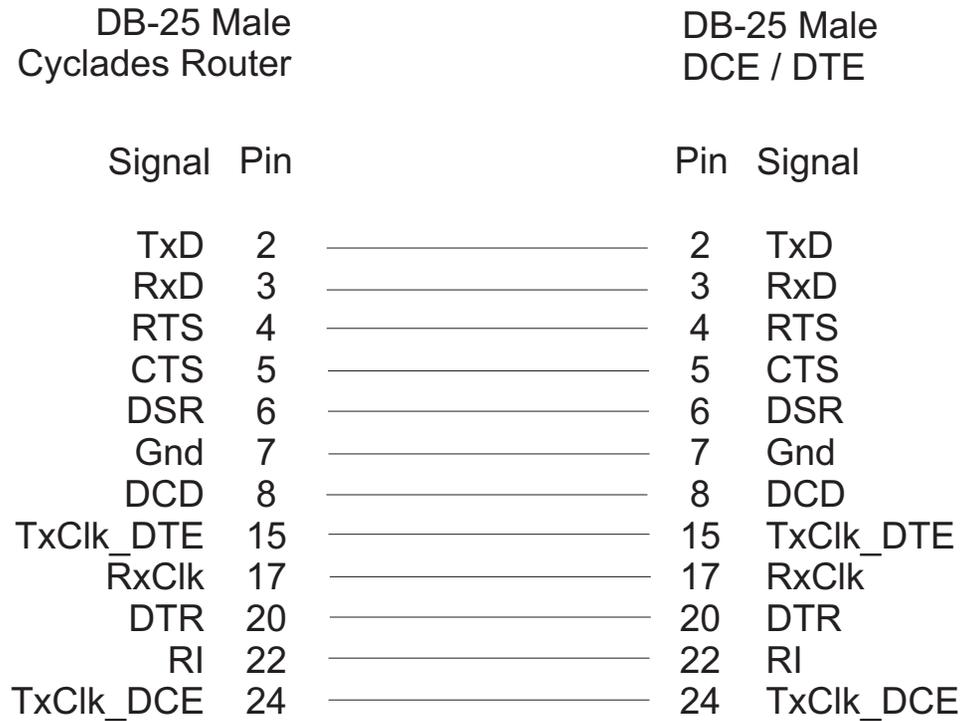
FIGURE B.5   STRAIGHT-THROUGH CABLE - DB-25 MALE TO DB-25 MALE

The DB-25 to M.34 Adapter
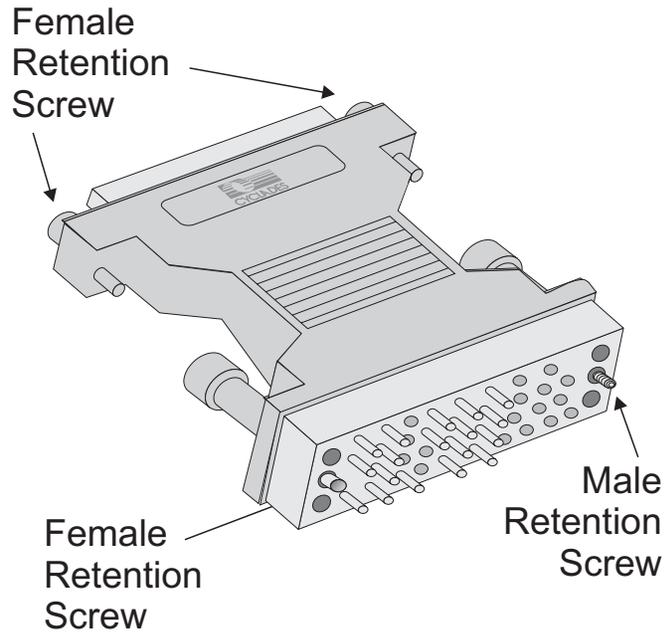
Signal	Pin		Pin	Signal
PGnd	1	———	A	PGnd
RTS	4	———	C	RTS
CTS	5	———	D	CTS
DSR	6	———	E	DSR
Gnd	7	———	B	Gnd
DCD	8	———	F	DCD
TxD/V.35 (B)	11	———	S	TxD (B)
TxD/V.35 (A)	12	———	P	TxD (A)
RxD/V.35 (B)	13	———	T	RxD (B)
RxD/V.35 (A)	14	———	R	RxD (A)
TxClk_DTE/V.35 (B)	16	———	AA	TxClk_DTE (B)
TxClk_DTE/V.35 (A)	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)

DB-25 Female   M.34 Male

FIGURE B.6 DB-25 TO M.34 ADAPTER - DB-25 FEMALE TO M.34 MALE

The X.21 Modem Cable

Cyclades-PR1000 (DB25)		X.21 Equipament (DB15)	
Pin #	Signal	Signal	Pin #
1	CGND	CGND	1
2	CLK-	CLK-	6
4	IND-	IND-	5
6	RxD-	RxD-	4
7	GND	GND	8
9	CTL-	CTL-	3
11	TxD-	TxD-	2
15	CLK+	CLK+	13
17	IND+	IND+	12
19	RxD+	RxD+	11
22	CTL+	CTL+	10
24	TxD+	TxD+	9
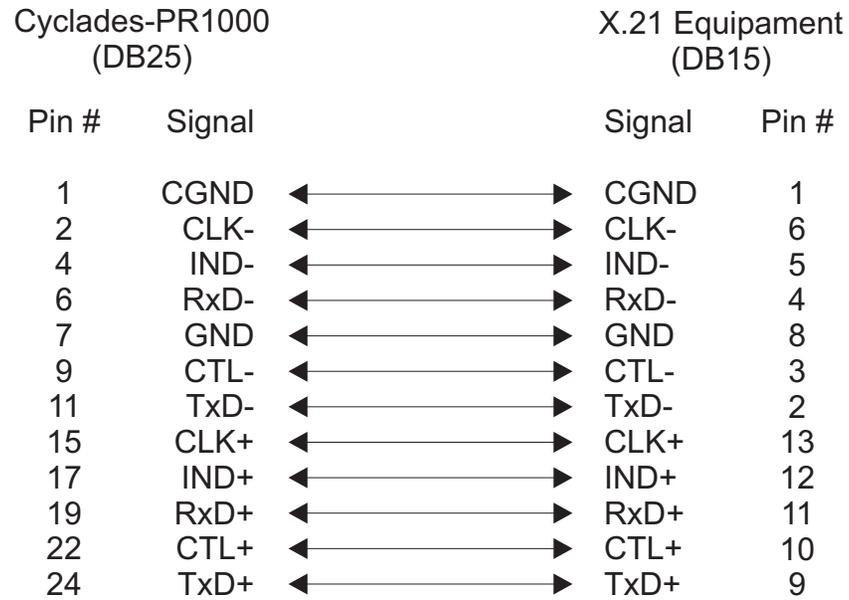
FIGURE B.6   X.21 MODEM CABLE - DB-25 MALE TO DB-15 MALE

The Loop-Back Connector

The pin-out diagram for this connector is provided for reference. This connector would only be used for testing the WAN interface.
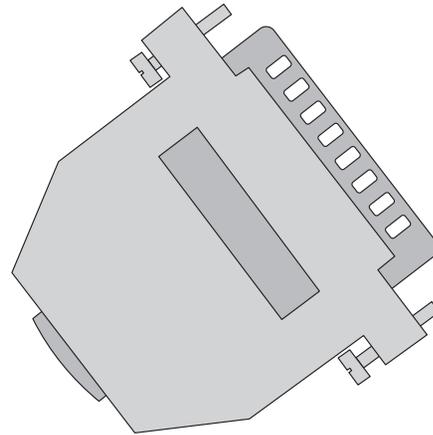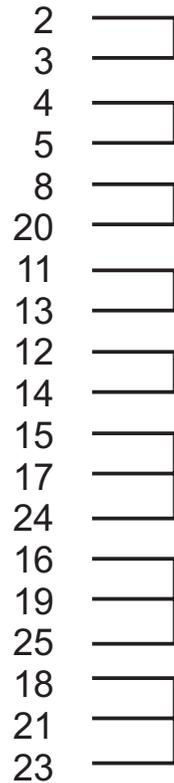
FIGURE B.8 LOOP-BACK CONNECTOR - DB-25 MALE

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.

Index

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