Configuration Guide for PortMaster Products

Livingston Enterprises, Inc.
6920 Koll Center Pkwy #220
Pleasanton, CA 94566
(800) 458-9966
(510) 426-0770

December 1995

950-1201B

Copyright and Trademarks

Disclaimer

Livingston Enterprises, Inc. makes no express or implied representations or warranties with respect to the contents or use of this manual, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Livingston Enterprises, Inc. further reserves the right to revise this manual and to make changes to its content at any time, without obligation to notify any person or entity of such revisions or changes.

FCC Class A Notice - United States

Computing devices and peripherals manufactured by Livingston Enterprises, Inc. generate, use, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions contained in this manual, may cause interference to radio communications. Such equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of the FCC Rules, which are designed to provide reasonable protection against radio interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user — at his own expense — will be required to take whatever measures may be required to correct the interference.

Some components may not have been manufactured by Livingston Enterprises, Inc. If not, Livingston Enterprises has been advised by the manufacturer that the component has been tested and complies with the Class A computing device limits as described above.

End User Product Agreement

This End User Product Agreement (the "Agreement") is a legal agreement between yourself, the individual or enterprise (the "Customer") which has acquired the hardware and software internetworking products contained in this packaging (the "Products"), and Livingston Enterprises, Inc., a California corporation ("Livingston"). You are requested to please carefully read the following terms and conditions. By using the enclosed Products, you accept this Agreement, and further agree to be bound by the terms and conditions contained herein. If you are not willing to be bound by the terms and conditions of this Agreement, then you must promptly return the Products to where you obtained them, or to Livingston, whereupon you will be provided with a full refund of your money, provided that there has been no damage to the Products which has been incurred due to your negligent use or handling thereof.

1. **License Grant**. Livingston grants to Customer the non-exclusive, non-transferable right and license to use the applicable Livingston proprietary software, whether enclosed herein in whatever form or media, or acquired electronically, as follows: (i) Customer shall have the right to use one (1) copy of the Livingston operating system ("ComOS") software on each hardware product acquired hereunder, and (ii) Customer shall have the right to reproduce, copy, use and distribute, in machine-readable (object code) form only, the Livingston software which is provided to Customer for administration, host device emulation and client remote access, provided however, that the use of such software must be made solely in conjunction with Livingston manufactured hardware products.

2. **License Restrictions**. Customer agrees that it will not attempt to reverse engineer, decompile or disassemble any Livingston software provided hereunder. Customer further agrees that it will not sublicense, rent, lease or assign any Livingston software provided hereunder, except that Customer may assign the software with the Products to a third party by operation of law, provided that the assignee is bound to the terms and conditions contained in this Agreement as a condition of assignment.

3. **Ownership and Copyright**. The Products provided to Customer hereunder are proprietary to Livingston and the software is protected by copyright, under the United States copyright laws and certain international treaties. Customer acknowledges and agrees that, while it shall acquire title to the hardware, it is acquiring only the right to use the software as provided for hereunder, and that all ownership and intellectual property rights not herein specifically granted to Customer are expressly reserved by Livingston.

4. **Limited Warranty**. Livingston warrants to the benefit of Customer only, for a term of one (1) year from the date of delivery of the Products to Customer, that under normal use and service: (i) the hardware and the software media shall be free from any defects in materials and workmanship, and (ii) the software will substantially conform to the functional specifications which are set forth in the applicable Product User's Manual.

5. **Livingston Obligations; Customer Remedies**. Livingston's sole obligation and liability under this limited warranty shall be to repair or replace any defective hardware or software media component and to remedy any substantial non-conformance of the software to the functional specifications set forth in its applicable User's Manual. If Livingston is unable to satisfy the foregoing limited warranty obligations during the warranty term, then Livingston shall, upon Customer's request for termination of the Agreement and return of the Products, refund to Customer all sums paid to Livingston for the purchase and licensing of the Products hereunder. THE FOREGOING REMEDIES ARE THE SOLE AND EXCLUSIVE REMEDIES AVAILABLE TO CUSTOMER FOR THE BREACH OF THE LIMITED WARRANTY SET FORTH IN THIS SECTION 5.

6. **Disclaimer of Implied Warranties**. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 5 ABOVE, LIVINGSTON MAKES NO OTHER EXPRESS WARRANTIES. TO THE EXTENT AUTHORIZED BY APPLICABLE LAW, LIVINGSTON SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

7. **Limitation of Liability**. Livingston's cumulative liability to Customer, or any third party, for loss or damages resulting from any claim, demand or action arising out of or relating to this Agreement or the use of Livingston Products, shall not exceed the amount paid to Livingston for the purchase and licensing of the Products. IN NO EVENT SHALL LIVINGSTON BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF LIVINGSTON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR SUCH DAMAGES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

8. **U.S. Government Restricted Rights**. If the Products are acquired by or on behalf of a unit or agency of the United States Government, by GSA or otherwise, then the Products are provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the Government is subject to restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights, at 48 CFR 52.227-19, as applicable. Manufacturer is Livingston Enterprises, Inc., 6920 Koll Center Parkway, Pleasanton, California 94566, (510) 426-0770.

9. **Export Law Assurances**. Customer agrees and certifies that the Products will not be shipped, transferred or re-exported, directly or indirectly, into any country prohibited by the United States Export Administration Act and the regulations promulgated thereunder, and that use of the Products will not be prohibited by such laws.

10. **Term**. This Agreement shall be effective upon the Customer's opening of the Product packaging and shall continue until terminated. Customer may terminate at any time by discontinuing use of the Products. Livingston may terminate this Agreement upon a material breach by Customer that remains uncured for a period of thirty (30) days after notice to Customer by Livingston specifying such material breach.

11. **Integration; Governing Law.** This Agreement represents the entire Agreement between the parties hereto and supersedes any prior or contemporaneous proposal, representation or understanding. The Agreement shall be construed and enforced in accordance with the laws of the State of California, USA. If the Products are distributed outside of the USA, then the United Nations Convention on Contracts for the International Sale of Goods is expressly disclaimed, and shall not apply to the performance or interpretation of this Agreement.

Table of Contents

Figures

Tables

Preface

About This Guide

This guide provides general information about networking and network configuration as well as specific information needed to configure PortMaster™ products. This guide should be reviewed thoroughly before you configure your PortMaster. The Configuration Guide provides all of the settings required for the most commonly used PortMaster configurations.

This guide is designed to be used by qualified system administrators and network managers. Knowledge of basic networking concepts is required to successfully install the PortMaster.

Preview of this Guide

This guide is designed to provide you with the information needed to configure the PortMaster. However, specific information about using the PMconsole™ user interface can be found in the *Administrator's Guide* for your interface. See "Related Documentation" for more information about Livingston documentation. The *Configuration Guide for PortMaster Products* includes the following chapters:

Chapter 1, "Introduction to PortMaster Products" describes each of the Portmaster products and how you can use them to accomplish your network goals.

Chapter 2, "Networking Concepts" describes the networking concepts you need to understand in order to make decisions about how to configure the PortMaster.

Chapter 3, "How PortMasters Work" briefly describes the operation of a PortMaster and the different kinds of uses for asynchronous ports.

Chapter 4, "Configuring a PortMaster" reviews each of the steps required to configure a PortMaster. This chapter also includes a detailed description of each of the global configuration parameters and how to set static routes.

Chapter 5, "Configuring the Ethernet Interface" describes each of the Ethernet port configuration parameters and its options.

Chapter 6, "Configuring an Asynchronous Port" describes each of the asynchronous port configuration parameters and its options. This chapter also describes how to configure modems.

Chapter 7, "Configuring a Synchronous WAN Port" describes each of the synchronous port configuration parameters and its options.

Chapter 8, "Configuring Dial-In Users" describes how to configure dial-in users by managing the Users Table.

Chapter 9, "Configuring Dial-Out Locations" describes each of the parameters used to set dial-out locations using the Location Table.

Chapter 10, "Configuring Filters" describes all of the parameters and options used to set input and output packet filters.

Chapter 11, "Connecting a Branch Office to the Main Office" describes the specific configuration options used to configure your PortMaster for a connection to another office. This chapter also describes how to setup multi-line load-balancing, which provides additional network bandwidth on-demand.

Chapter 12, "Connecting Your Office to the Internet" describes how to configure the PortMaster for a continuous connection to an Internet Service Provider (ISP).

Chapter 13, "Configuring User Dial-In Access" describes how to configure the PortMaster to allow login users to access available hosts. This application is useful for telecommuters, universities, and Internet Service Providers (ISP).

Chapter 14, "Configuring the PortMaster to Access Shared Devices" describes how to configure PortMasters to allow access to shared devices such as modems, printers, and other RS-232 devices.

Chapter 15, "Synchronous Leased Line Connections" describes how to configure a PortMaster synchronous port for a leased line connection.

Chapter 16, "Synchronous Frame Relay Connections" describes how to configure a PortMaster synchronous port for a Frame Relay connection.

Chapter 17, "Synchronous V.25bis Dial-Up Connections" describes how to configure a PortMaster synchronous port for V.25bis dialing using a switched 56K or an ISDN terminal adapter.

Chapter 18, "ISDN Connections" describes how to configure ISDN on PortMaster products.

Chapter 19, "Troubleshooting the PortMaster Configuration" provides information about analyzing and solving network problems.

Chapter 20, "Command Line Summary" provides a quick reference guide to the syntax of all of the PortMaster commands.

A glossary, list of references, and index are also included.

Related Documentation

The *PortMaster Hardware Installation Guide* gives instructions for installing the PortMaster hardware on your network. Read the *Hardware Installation Guide* that came with your system before you attempt to configure your communications server or router.

The PMconsole user interface can be used to perform the actual configuration tasks. PMconsole comes in several versions including: PMconsole for Windows and PMconsole for X Windows. Use the *Administrator's Guide* that is appropriate for your chosen interface.

The PortMaster can also be configured using the Command Line Interface, either by attaching a console terminal or PC to the service port or connecting to the port using telnet. A quick reference guide for the command syntax is given in Chapter 20.

Document Conventions

The following table describes the type changes and symbols used in this guide.

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, parameters, and directories; on-screen computer output.	Use `version` to display the version number.
`AaBbCc123`	What you type, contrasted with on-screen computer output.	`login:` **`!root`** `Password:`

Typeface or Symbol	**Meaning**	**Example**
`AaBbCc123` (italic)	Command-line placeholder: replace with a real name or value.	To set baud rate, type: **set s0 speed** *baud_rate*
[AaBbCc123]	Commands in brackets denote a key to press.	`login:` **!root [Return]**

Contacting Livingston Technical Support

Every Livingston product comes with free lifetime software technical support and a one year hardware warranty.

Livingston Enterprises provides free technical support via voice, FAX, and electronic mail. Technical support is available Monday through Friday 6am-5pm Pacific Time (GMT-8).

To contact Livingston technical support:

- By voice, dial 1 800 458 9966 within the US or +1 510 426 0770 outside the US
- By FAX, dial +1 510 426 8951
- By electronic mail, send mail to `support@livingston.com`
- Through the World Wide Web at the URL `http://www.livingston.com/`
- Upgrades and new releases are available by anonymous FTP at `ftp://ftp.livingston.com/pub/livingston/`

Note – An Internet mailing list for PortMaster users is available.
To subscribe to the mailing list, send electronic mail to
`portmaster-users-request@livingston.com`
and in the body of the message, include the line:
`subscribe`

To subscribe to a daily digest instead, send electronic mail to
`portmaster-users-digest-request@livingston.com`
and in the body of the message include the line:
`subscribe`

Introduction to PortMaster Products 1

This chapter describes the PortMaster family of products and includes the following information:

- An overview of the various PortMaster products
- A detailed description of the PortMaster hardware
- An overview of how PortMaster routers and communication servers are used
- An overview of how to install and configure PortMasters
- Sample applications for PortMaster communication servers

PortMaster Products

PortMaster products offer advanced technology solutions for internetwork connectivity. Livingston products are designed to provide connectivity for sites requiring high speed dedicated links and for sites needing cost-effective dial up connections to other offices or the Internet.

PortMaster products support three types of service:

- Routing services that support both Internet Protocol (IP) and Novell Internet Packet Exchange (IPX) routing. The dial on-demand feature allows the use of dial-up telephone lines when there is data to send between networks.
- Terminal services that connect asynchronous devices and terminal emulation software for telnet and rlogin connections to host computers. Terminal services also allow a user to access a server port as if it were a UNIX tty device for use with any standard serial device.
- Telecommuting services that connect devices over telephone lines using Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP). Security is accomplished using password protection, user authentication, packet filtering, and the Remote Authentication Dial In User Service (RADIUS) protocol.

Figure 1-1 shows how PortMaster products can be used to provide the network connectivity and services described in this section.

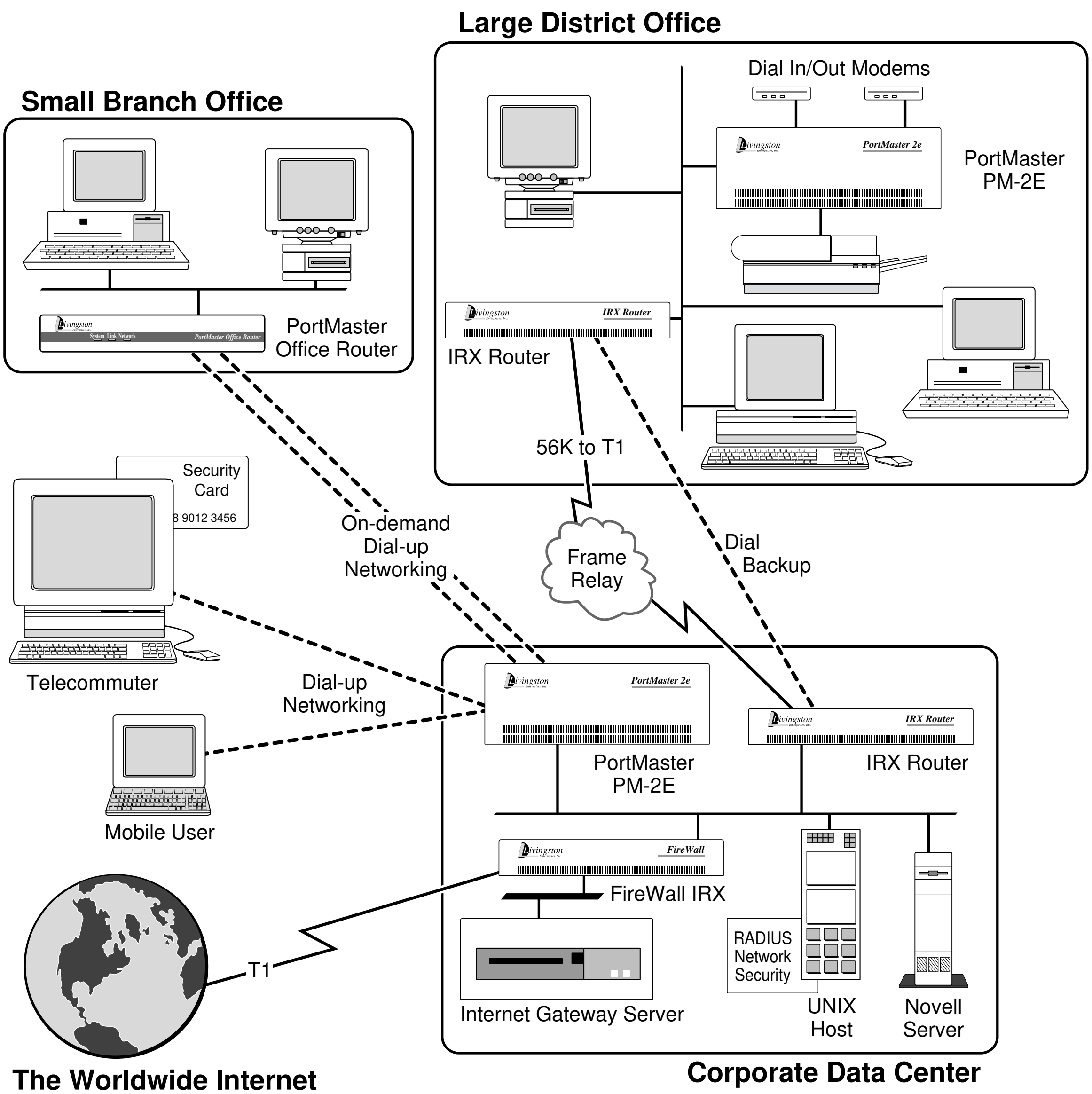

Figure 1-1 PortMaster Product Applications

Livingston offers the PortMaster products shown in Table 1-1; each product was developed for a specific application.

Table 1-1 PortMaster Products

Product	**Features**	**Applications**
PortMaster Communications Servers	Communications server with: • 10, 20, 25, or 30 asynchronous 115.2kbps serial ports • 0, 5, or 10 ISDN BRI ports • Security features including: dial-back, password, packet filtering, PPP authentication protocols (PAP and CHAP), and RADIUS support • Dial on-demand, continuous, scheduled, dynamic routing (RIP), and SAP support • Optional synchronous routing port over DDS, T1, E1, Frame Relay, ISDN, or leased lines • Support for TCP, IP, IPX, SPX, SAP, RIP, SLIP, CSLIP, ICMP, UDP, ARP, telnet, rlogin, and PPP protocols • TCP/IP host device emulation for connection to shared devices (on supported hosts)	Terminal services, telecommuting, and router for enterprise-wide connections
IRX Routers	1 to 4 port multiprotocol router for interfacing to other wide-area routers. Supports networking speeds up to T1 for TCP/IP and NetWare networks. Supports synchronous, asynchronous, Frame Relay, and PPP connections.	High speed routing between remote sites
FireWall IRX Router	Enables secure Internet access without allowing access to internal networks and data. Provides a firewall using: • T1/E1 synchronous port for PPP or Frame Relay • Asynchronous port for dial-up networking • 2 local Ethernet ports • Enhanced filtering • Packet logging • Network isolation	High speed routing to gateway servers and the Internet

Table 1-1 PortMaster Products *(Continued)*

Product	Features	Applications

Office Router	Small dial-up router for connecting to other offices or the Internet. Provides:
	• 1 Ethernet port for local connection
	• 1 asynchronous port for administration or dial-up connections
	• Multiprotocol, filtering, routing support
	• One of the following:
	  • 1 PCMCIA port for dial connections
	  • 1 ISDN BRI port
		On-demand routing to other offices or cost-effective Internet connection

PMconsole	Multiplatform graphical user interface for configuring PortMaster products.	Configuring PortMasters
RADIUS	Remote Authentication Dial In User Service, which is an extensible security system that allows authentication and authorization of network users.	Network and data security
TelePath	Client software that provides a PPP serial interface for remote access to Novell NetWare and TCP/IP networks.	Allows remote network access

PortMaster Ports

PortMasters have configurable Ethernet, asynchronous, synchronous, ISDN BRI, and parallel ports. Table 1-2 shows each of the configurable ports by model.

Table 1-2 Available Port Types by PortMaster Model

	Ports				
Product	**Ethernet**	**Async**	**Sync (T1)**	**Sync (64K)**	**Parallel**
OR-M	ether0	s0-s1			
OR-U[1]	ether0	s0		s1-s2	
PM-2	ether0	s0-s9			p0
PM-2E-10	ether0	s0-s9			p0
PM-2E-20[2]	ether0	s0-s19			p0
PM-2E-30[2,3]	ether0	s0-s29			p0

Table 1-2 Available Port Types by PortMaster Model *(Continued)*

Product	Ports				
	Ethernet	**Async**	**Sync (T1)**	**Sync (64K)**	**Parallel**
PM-2R	ether0	s0-s9	w1		
PM-2ER-10	ether0	s0-s9	w1		
PM-2ER-20[2]	ether0	s0-s19	w1		
PM-2ER-30[2,3]	ether0	s0-s29	w1		
PM-25	ether0	s0-s24			
IRX-111	ether0	s0	s1		
IRX-112	ether0	s0	s1	s2	
IRX-114	ether0	s0	s1, s3	s2, s4	
IRX-211	ether0-1	s0	s1		

1. ISDN BRI port.
2. Ports s10-s19 may be replaced by 5 ISDN BRI ports if a MOD-10I-U board is installed.
3. Ports s20-s29 may be replaced by 5 ISDN BRI ports if a MOD-10I-U board is installed.

PortMaster Communications Servers

The PortMaster Communications Servers include the following models:

- PM-2
- PM-2E
- PM-2R
- PM-2ER
- PM-25

PortMaster Communications Servers are versatile network access devices for Novell/IPX, TCP/IP, and mixed network environments. These products provide secure remote access for telecommuters and portable computer users, while reducing costs by managing a pool of modems used for remote access dial in and network user dial out. Some models provide synchronous ports for high-speed connections and parallel ports for additional devices.

All of the communications servers have some combination of Ethernet, asynchronous, synchronous, and parallel ports. Figure 1-2 shows an example of a generic PM-2.

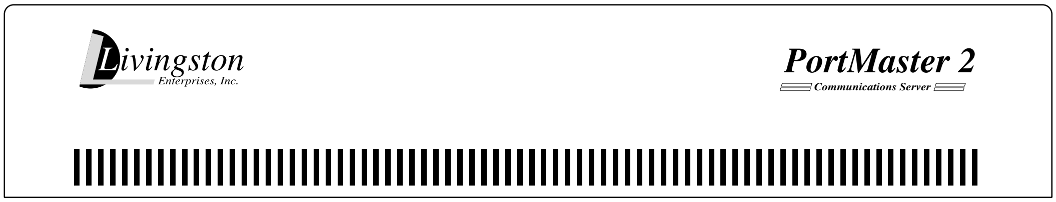

Figure 1-2 PortMaster PM-2

PortMaster IRX Internetwork Routers

PortMaster IRX multiprotocol internetwork routers provide wide area interconnectivity between Novell/IPX, TCP/IP, and mixed network environments. Interconnectivity is provided over long distances using WAN links such as digital leased lines (64K to T1/E1), ISDN, switched 56K, or Frame Relay lines.

PortMaster routers have one or more Ethernet ports, one asynchronous port for dial-up routing or as a console, and one or more synchronous ports for high-speed routing. The IRX routers (Figure 1-3) are designed to perform routing functions and not communications server functions.

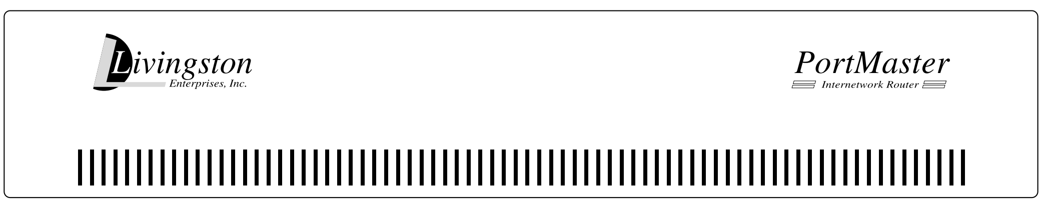

Figure 1-3 PortMaster IRX Router

FireWall IRX-211 Router

The FireWall IRX-211 router provides local networks with secure connectivity to remote networks, including the world-wide Internet. The FireWall IRX-211 provides security by allowing internetwork accessible hosts, such as ftp servers, to be segmented from the private network. This product also implements independent packet filtering and packet logging for each network segment. Packet filtering allows you to permit or deny the passage of packets to limit inbound packets while allowing local users outbound access to remote networks and Internet services.

PortMaster Office Router

The PortMaster Office Router provides a cost-effective way to connect a small office to a larger corporate office or to the Internet. The dial on-demand feature of the router allows local area networks to be economically and seamlessly connected using modems and standard telephone lines when data is ready to be transmitted.

The PortMaster Office Router, shown in Figure 1-4, consists of an Ethernet port, a console port that can also be used for an external modem and one of the following:

- PCMCIA modem port
- ISDN BRI port

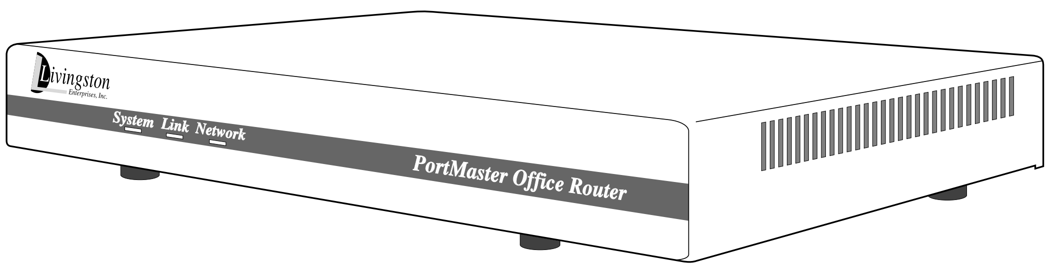

Figure 1-4 PortMaster Office Router

PortMaster Software Description

All PortMasters come standard with the PortMaster software, which includes:

- ComOS™—The communication software operating system already loaded in the FLASH RAM of each PortMaster.
- PMconsole—The optional user interface software for configuring the PortMaster. The PortMaster can also be configured through the console or a telnet session without using PMconsole. Available for Windows, SunOS, Solaris, AIX, HP/UX, and other platforms.
- `pmd` or `in.pmd`—The optional PortMaster daemon software that can be installed on UNIX hosts to allow the host to connect to printers or modems attached to a PortMaster. The daemon also allows the PortMaster to multiplex incoming users onto the host using one TCP stream instead of multiple streams like rlogin. Available for SunOS, Solaris, AIX, HP/UX, and other platforms.

- RADIUS—The RADIUS (Remote Authentication Dial In User Service) server, `radiusd`, runs as a daemon on UNIX systems, providing centralized authentication of dial-in users. The `radiusd` daemon is provided in binary and source form for SunOS, Solaris, AIX, HP/UX, and other platforms. The daemon is also provided in source form for Alpha OSF/1, Linux, BSD/OS, Unixware, and SCO. For more information see the *RADIUS Administrator's Guide*.

Software installation procedures are described in the *Administrator's Guide* for your interface software.

Software Versions

This manual documents the software releases shown in Table 1-3.

Table 1-3 Software Versions

ComOS	Upgrade Image	Platforms
3.3	pm2_3.3	PM-2, PM-2R, PM-2E, PM-2ER
3.3	pm25_3.3	PM-25
3.3L	or_3.3L	OR-M, OR-U
3.3R	irx_3.3R	IRX-111, IRX-112, IRX-114, IRX-211

If you are running a later release, check the release notes for changes to the software since the publication of this document. Additional information about software releases is available from `ftp://ftp.livingston.com/pub/livingston/release/`. Upgrade images can be installed on PortMasters using `pminstall` and are available on `ftp://ftp.livingston.com/pub/livingston/upgrades/`. Refer to Chapter 19, "Troubleshooting the PortMaster Configuration" for more information about upgrading software.

Using PortMasters

Before the PortMaster can be used to connect Wide Area Networks (WANs), you must install the hardware using the instructions in the *Hardware Installation Guide* for your system.

This guide is designed to introduce the most common configuration options available for PortMaster products. This material should be thoroughly reviewed before you configure your router. Many decisions should be made before or during the configuration process, including:

- What general configuration do you want to implement?
- Do you want to use a synchronous connection to a high speed line?
- Will your high speed line(s) be using Frame Relay, ISDN, switched 56K, or PPP?
- If you want dial on-demand routing do you want multi-line load-balancing?
- Do you want packet filtering for Internet connections?
- Do you want packet filtering for connections to other offices?
- Do you want dial in users to use SLIP, PPP, or both?
- If you use PPP, do you want PAP or CHAP authentication?
- Are you using a name service such as DNS or NIS?
- Do you have the appropriate network addresses available?
- Are you running IP, IPX, or both?
- Do you want to enable SNMP for network monitoring?
- Do you want dial in only, dial out only, or two way communications on each port?
- What characteristics do you want to assign to the dial-out locations?
- How do you want to configure dial-in users?
- Do you want to use RADIUS to authenticate dial-in users, or the internal User Table on the PortMaster?
- Do you want to use the console port for administration functions or do you want to attach an external modem to the port?

There are many other decisions that need to be made during the configuration process. This guide discusses the various configuration options and their implications.

Trade-Offs between Dial-on-Demand, Leased Line, and Frame Relay

Determining which type of communication service best meets your networking needs is not a simple matter. The differences in user requirements, telephone company charges, and equipment and maintenance costs must all be taken into account. In this section, we hope to provide an overview of the parameters that should go into this decision.

The first criteria is user requirements, which can generally be used to set the minimum level of service. For example, if your application requires less than 128Kbps of throughput, then multi-line load balancing across dial on-demand modems or ISDN may be a viable candidate. The higher your bandwidth need over 56Kbps, the more likely fractional T1 may be what you need.

Often, the next factor involved in making a decision is cost. Generally, the lowest cost service meeting user requirements is chosen. Computing cost can be very tricky, however, due to the varying rates from telecommunications providers and the differences between flat-rate monthly services and metered-usage services. Some providers charge for Frame Relay services based on the byte-count transferred, some provide Frame Relay on a flat-rate basis. ISDN services can be billed on a flat-rate basis or on a per-minute usage basis. Point-to-Point leased circuits are almost always based on a flat monthly rate.

Generally, Frame Relay is most cost-effective in areas where the application is from a single hub to multiple remote offices (point to multipoint) or a meshed network of several offices (multipoint to multipoint). In most cases, Frame Relay is more expensive than a single point-to-point leased line between two locations.

ISDN is most cost effective in situations where high-bandwidth and low latency are desirable, but the need to exchange data is widely distributed over time. If you are using on-demand ISDN, you should pay close attention to your monthly ISDN usage bills. If the usage charges start to approach leased-line costs, perhaps it is time to consider switching. If you are running an ISDN dial-in pool for multiple remote offices, then the aggregate ISDN bill should be compared to the cost of a Frame Relay network. Additionally, the top 3 to 5 ISDN bills can be compared to a smaller Frame Relay network while the rest of the offices remain on ISDN.

There are a variety of other trade-offs as well. Modems offer the highest latency and the lowest bandwidth. Next, ISDN offers better latency than modems, but still has fairly high latency compared to other technologies. The switching inherent in Frame Relay adds some latency, but less than ISDN or modems. ISDN can be used for bandwidths up to 128K or further if additional B channels are used with multi-line load balancing or multilink PPP, while Frame Relay can scale as high as T1 or E1. Point-to-point lines offer the lowest latency, and scale up to very high bandwidths. The maximum bandwidth supported by any PortMaster synchronous port is T1 (1.544 Mbps) or E1 (2.048 Mbps). However, point-to-point lines also usually come at the highest price.

Example Applications for PortMasters

The different PortMaster models have different applications depending on their hardware configuration. Table 1-4 shows each of the products and the applications for which it is best suited.

Table 1-4 Example Applications

Product	Example Applications
OR-M	For branch, small office, or home network requiring limited bandwidth connectivity using a modem several hours per day.
OR-U	For branch, small office, or home network requiring ISDN BRI connectivity.
PM-2E-10 PM-2E-20 PM-2E-30	For communications server applications requiring dial-up connectivity, Internet Service Provider access, remote access to login hosts, SLIP or PPP remote networking, telecommuting, mobile computing for sales or field personnel connections to the main network, and shared access to RS-232 devices such as modems and printers. The ISDN BRI expansion boards provide ISDN dial-in and dial-out service without a terminal adapter. Can also serve as an ISDN routing hub for high-end telecommuting or ISP services.
PM-25	Used for the same applications as the PM-2E but has higher port density and easier to manage cabling. Two PM-25s take the same rack space as one PM-2E-30, while providing 48 ports with only 6 cables.
PM-2	Any of the PM-2E applications that do not require expandability. This model provides only 10 ports.

Table 1-4 Example Applications *(Continued)*

Product	**Example Applications**
PM-2ER-10 PM-2ER-20 PM-2ER-30	For communications server applications listed for the PM-2E with a built-in T1 synchronous port that allows a high-speed connection to another site. These models are ideal for remote point of presence (POP) servers for ISPs or organizations that need to provide access to a centralized database by 20 to 60 remote terminals or modems over leased lines, Frame Relay, switched 56K, or ISDN connections. For larger POPs the IRX-111 combined with 3 or more PM-2E's is preferable.
PM-2R	Especially good for small remote offices that have a synchronous link to a central or regional hub but also require a small amount of local dial-in capacity.
IRX-111	For IP and IPX routing between an Ethernet and a synchronous line up to T1/E1 speeds using leased lines, Frame Relay, or switched 56K. Also supports ISDN with an external terminal adapter.
IRX-112	Expands the functionality of the IRX-111 by providing one port up to T1/E1 speed and one 64Kbps port.
IRX-114	Expands the functionality of the IRX-111 by providing two ports up to T1/E1, which can allow a leased line T1 connection to an ISP at the same time as a Frame Relay T1 connection to another office. Also has two 64Kbps ports.
IRX-211	This product is specifically designed for building firewalls. The IRX-211 has a T1/E1 port for Internet connectivity and two Ethernet ports: one for exposed hosts and one for protected hosts. It also has a console port for out-of-band management.

Asynchronous Applications

The following examples describe various uses for asynchronous ports.

Connections Between Offices

Office to office connections can be achieved using dial-up asynchronous connections or synchronous connections depending on your application. Examples of both are given in this guide.

Once a PortMaster is installed in each office and connected to the local Ethernet using an AUI, 10Base2, or 10BaseT connector, one or more asynchronous serial ports can be configured to dial another office or a set of offices when network traffic for the specified location exists. The two most common configurations are a “star” where multiple branch offices dial into a central hub which routes among them, and a “mesh” where every office can speak to any other office on demand. Intermediate configurations between “star” and “mesh” are also possible.

To add network bandwidth on-demand, additional ports can be configured for load-balancing. These ports can be configured to connect to a location when the network traffic exceeds a specific level. In this configuration, multiple ports are connected during times of heavy traffic thereby adding bandwidth as needed and are disconnected when traffic drops.

Connections to the Internet

An asynchronous port can be set for a continuous connection to an Internet Service Provider (ISP) by configuring it for continuous dial out. In this configuration if the dial-out line is dropped, the PortMaster automatically reestablishes the connection.

Connecting to the Internet should include packet filtering and security to ensure that access to the local network is restricted.

Logging Into Remote Hosts

Communication servers are most commonly used to allow remote users to dial into a network location and access a host with their local account. This configuration is also used by Internet Services Providers that provide many users access to shell accounts. PortMaster asynchronous ports are configured for login by dial-in users. When users dial in, they are connected with a modem, allowed to login, and then connected with a specified host for the current session.

Dial-In Network Connectivity

A PortMaster asynchronous port can provide PPP or SLIP service to a dial-in user, allowing them to route TCP/IP (and if using PPP, IPX as well) traffic across a modem to access the local network or the entire Internet. This configuration is very heavily used by Internet Service Providers and by corporations with remote users running client-server applications that require access to central hosts from home, field offices, or on the road.

Sharing Devices Across the Network

PortMaster asynchronous ports can be configured to allow network hosts access to shared devices connected directly to the PortMaster. If the network host is running the PortMaster `in.pmd` daemon, a connection can be established to a specified port on the PortMaster. Once the connection is established, the connected device such as a printer or modem, can be accessed as if it were connected directly to the host.

Ports can also be configured to be accessed by programs using TCP/IP sockets, or by telnet from the network.

Synchronous Applications

The following examples describe various uses for synchronous ports.

Routing Over Leased Lines

A synchronous port can be used to connect to synchronous leased lines from 9600 bps to T1 (1.544 Mbps) or E1 (2.048 Mbps) for continuous operation. A Digital Service Unit/Channel Service Unit (DSU/CSU) must be attached to the WAN port on the PortMaster.

Routing Over Frame Relay

Frame Relay provides connectivity using a packet-switched network. Its two advantages over a leased line network are lower cost and the ability to have multiple Private Virtual Circuits (PVCs) come into a single physical port. It is especially popular for hub and spoke network arrangements, for example having a dozen field offices with 56Kbps or fractional T1 Frame Relay connections connect to a central office using a Fractional T1 or T1 Frame Relay connection. The central office requires only one CSU/DSU and synchronous port on the router, instead of twelve.

Routing Over Switched 56K

Switched 56K can be less expensive than Frame Relay in applications where short bursts of connectivity are required but dial-up modems do not provide enough bandwidth. V.25bis dialing is used to establish a link over a switched network and the link is brought down after a specified period with no traffic.

Routing Over ISDN

Integrated Services Digital Network (ISDN) provides fast dial-up connectivity for applications where the expense of a dedicated Frame Relay or leased line connection is not called for by the amount and nature of the traffic.

Various PortMaster products support ISDN in three different ways. Any asynchronous port can be connected to an asynchronous terminal adapter (TA) which can take asynchronous data up to 115200 bps and convert it into a 64Kbps synchronous data stream. A second option is to connect a synchronous port to a 128Kbps synchronous terminal adapter using two ISDN B channels.

Additionally, some products have Basic Rate Interface (BRI) ports with integrated NT1 (a U interface) for use in countries that follow USA telephone standards. These allow you to plug an ISDN phone line directly into the router, so no terminal adapter is required, making configuration much easier. Each BRI port has 2 64Kbps synchronous B-channels plus one 16Kbps D-channel for signalling.

Configuration Overview

Your PortMaster comes with software used to install and configure the PortMaster. This section briefly describes the installation and configuration process and where to find the instructions for each step.

There are several different versions of PMconsole that can be used to configure your PortMaster, including PMconsole for Windows, PMconsole for UNIX, and the Command Line Interface. You can use one or more of these interfaces to configure your PortMaster. Your decision is usually based on the type of hosts available on your network and whether you want to use a graphical user interface (GUI). A quick reference guide to the command line syntax is included in Chapter 20, “Command Line Summary.”

To install and configure a PortMaster:

1. Understand networking concepts and how to configure the PortMaster. (*Configuration Guide*)
2. Install the PortMaster hardware and set the IP address. (*Hardware Installation Guide*)
3. Install the PMconsole software, if desired. (*PMconsole Administrator’s Guide*)
4. Configure the PortMaster global parameters. (*Configuration Guide* and *Administrator’s Guide*)

5. Configure the PortMaster Ethernet port. (*Configuration Guide* and *Administrator's Guide*)
6. Configure the asynchronous serial port(s), if available. (*Configuration Guide* and *Administrator's Guide*)
7. Configure the synchronous WAN port, if available. (*Configuration Guide* and *Administrator's Guide*)
8. If you want dial-in connections, configure the User Table, which defines the characteristics of dial-in users. (*Configuration Guide* and *Administrator's Guide*)
9. If you are using RADIUS security instead of a User Table, refer to the *RADIUS Administrator's Guide* for more information.
10. If you want dial-out connections, configure the Location Table, which defines the characteristics of dial-out connections. (*Configuration Guide* and *Administrator's Guide*)
11. If you want to use packet filters or access filters to provide additional security, configure the Filter Table, which defines input and output packet filters and access filters associated with ports, users, and locations. (*Configuration Guide* and *Administrator's Guide*)
12. Use the specific configuration information in Chapters 11 through 18 that apply to your application to complete your PortMaster configuration.

The *Configuration Guide for PortMaster Products* provides information you need to decide how to configure your PortMaster. Refer to the "Preface" for an overview of each of the chapters.

The *Administrator's Guide* for each interface provides specific information about how to use that interface to configure your PortMaster.

These guides are intended to be used together when configuring PortMasters.

Where To Go From Here

If you are already familiar with networking concepts and PortMaster products, proceed to Chapters 11 through 18 for specific configuration instructions. If you are not familiar with networking concepts or PortMaster products, proceed to Chapter 2, "Networking Concepts" and Chapter 3, "How PortMasters Work." If you need more information about networking, additional reading is listed in the References section at the end of this guide.

Networking Concepts 2

This chapter describes general network concepts that you must understand before you configure your PortMaster. If you are already familiar with the topics described in this chapter, proceed to Chapter 3, "How PortMasters Work" for information about possible configuration options.

This chapter includes the following:

- Addressing concepts for IP and IPX protocols
- A description of how netmasks are used to help define subnets
- Routing concepts including RIP
- A description of SNMP management
- A description of naming services, DNS and NIS
- A discussion of network security issues and an introduction to RADIUS

Network Addressing

PortMaster products support packet routing using both IP and IPX protocols. The Internet Protocol (IP) is a packet-based protocol used to exchange data over computer networks. IP provides addressing and control information that allows data packets to be routed across networks.

Novell Internet Packet Exchange (IPX) is another protocol used to exchange data over PC-based networks. IPX uses Novell's proprietary Service Advertisement Protocol (SAP) to advertise special services such as print and file servers.

IP Addressing

IP address descriptions are found in RFC 1166, Internet Numbers. Refer to the "References" chapter of this guide for more information. The Network Information Center (NIC) maintains and distributes the RFC documents. The NIC also assigns IP addresses and network numbers. When an organization applies to the NIC, a network number or range of addresses appropriate to the number of host devices on their network is assigned.

In the past, all IP addresses were assigned by the NIC. However, as the Internet has grown, this is no longer possible. As a result, IP addresses are now generally delegated in large blocks to Internet Service Providers (ISPs) who assign them to their customers. If you are connecting to the Internet, contact your Internet Service Provider for address assignment.

The sections that follow describe the various types of IP addresses, how addresses are given, and routing issues related to IP.

IP Address Notation

IP addresses are written as four numbers separated by dots (periods). The leading zeros are dropped in IP addresses. Each number, written in decimal, represents an 8-bit octet (sometimes informally referred to as a byte) giving each number a range of 0 through 255, inclusive. When strung together, the four octets form the 32-bit IP address. This notation is called dotted decimal.

These examples show 32-bit values expressed as IP addresses:

```
100.100.100.10
195.32.4.200 (meaning 195.032.004.200)
```

The largest possible value of a field in dotted-decimal notation is 255, which represents an octet where all of the bits are ones.

IP Address Classes

There are different classes of addresses based on the number of hosts and subnetworks required to support the hosts. As described in RFC 1166, IP addresses are 32-bit quantities divided into five classes. Each class has a different number of bits allocated to the network and host portions of the address. For this discussion, consider a network to be a collection of computers (hosts) that have the same network field values in their IP addresses.

Class A Addresses

The class A IP address format allocates the highest eight bits to the network field and sets the highest priority bit to 0 (zero). The remaining 24 bits form the host field. Only 126 class A networks can exist (0 is reserved, and 127 is used for loopback networks), but each class A network can have almost 17 million hosts. No new class A networks can be assigned at this time.

For example:

```
10.100.232.1
 /          \
Network    Host
Address    Address
```

Class B Addresses

The class B IP address format allocates the highest 16 bits to the network field and sets the two highest-order bits to 1 and 0, resulting in a range from 128 through 191, inclusive. The remaining 16 bits form the host field. More than 16,000 class B networks can exist, and each class B network can have up to 65,534 hosts. For example:

```
172.16.232.121
 /          \
Network    Host
Address    Address
```

Class C Addresses

The class C IP address format allocates the highest 24 bits to the network field and sets the three highest-order bits to 1,1, and 0, resulting in a range from 192 through 223, inclusive. The remaining eight bits form the host field. More than 2 million class C networks can exist, and each class C network can have up to 254 hosts. For example:

```
192.168.20.220
 /          \
Network    Host
Address    Address
```

Class D Addresses

The class D IP address format was designed for multicast groups, as discussed in RFC 988. In class D addresses, the four highest-order bits are set to 1,1,1,0, resulting in a range from 224 through 239, inclusive.

Class D addresses are currently used primarily for MBONE. Many routers, including those from Livingston. do not support MBONE or multicast and therefore ignore class D addresses.

Class E Addresses

The class E IP address is reserved for future use. In class E addresses, the four highest order bits are set to 1,1,1,1. Routers currently ignore class E IP addresses.

Reserved IP Addresses

Some IP addresses are reserved for special uses and cannot be used for host addresses. Table 2-1 lists ranges of IP addresses and shows which addresses are reserved, which are available to be assigned, and which are for broadcast.

Table 2-1 Reserved and Available IP Addresses

Class	Address/Range	Status
A	0.0.0.0	Reserved
	1.0.0.0 through 126.0.0.0	Available
	127.0.0.0	Loopback networks (localhost)
B	128.0.0.0	Reserved
	128.1.0.0 through 191.254.0.0	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 through 223.255.254	Available
	223.255.255.0	Reserved
D	224.0.0.0 through 239.255.255.255	Multicast group addresses
E	240.0.0.0 through 255.255.255.254	Reserved
	255.255.255.255	Broadcast

IP Address Conventions

If the bits in the host portion of an address are all 0, that address refers to the network specified in the network portion of the address. For example, the class C address 192.31.7.0 refers to a particular network. Historically this address was used as a broadcast. The current standard is to use all ones in the host portion (for example, 192.168.1.255), however, many hosts still use all zeroes. The PortMaster can be configured either way, and should be set to match the other systems on your network.

Note – Do not use an IP address with all zeros or all ones in the host portion of the address, since these are reserved as broadcast addresses.

IPX Addressing

An IPX address consists of 10 bytes (usually expressed in hexadecimal notation), which gives an IPX network host a unique identifier. IPX addresses are made up of two parts, as follows:

- Network segment address, expressed as eight hexadecimal digits

  These 4 bytes (32 bits) specify on which segment the node resides.
- Node address, expressed as dotted triplets of four-digit hexadecimal numbers

  These 6 bytes (48 bits) provide the MAC address of the node.

The two elements of the IPX address are separated by a colon. Following is an example of an IPX address:

```
        00000003:0001.8423.4567
           /            \
    Network              Node
    Segment Address      Address
```

The first eight digits represent the network segment, and the following 12 digits represent the node or MAC address of the node. All digits are expressed in hexadecimal.

Using Netmasks to Create IP Subnets

Netmasks are used to create IP subnets and thereby divide networks into smaller more manageable groups of hosts. Subnetting is a scheme for imposing a simple hierarchy on hosts on a single physical network. The usual practice is to use the first few bits in the host portion of the network address for a subnet field. The official description of subnetting is RFC 950, Internet Standard Subnetting Procedure.

Subnetting and Routing

Routers and hosts can use the subnet field for routing. The rules for routing on subnets are identical to the rules for routing on networks. However, correct routing requires all subnets of a network to be physically contiguous. In other words, the network must be set up so that it does not require traffic between any two subnets to cross another network. Also, RFC 950 implicitly requires that all subnets of a network have the same number of bits in the subnet field.

Livingston products support a special subnet mask that allows for noncontiguous subnets. However, using noncontiguous subnets is not recommended because not all routers support them.

Subnet Masks

A subnet mask identifies the subnet field of a network address. This mask is a 32-bit number written in dotted-decimal notation with all ones in the network and subnet portions of the address, and all zeros in the host portion. This scheme allows for the identification of the host portion of any address on the network.

Table 2-2 shows the subnet masks you can use to divide a class C network into subnets.

Table 2-2 Subnet Masks for a Class C Network

Subnet bits	**Host bits**	**Number of Subnets**	**Number of hosts per subnet**	**Hexadecimal netmask**	**Dotted decimal netmask**
24	8	1	254	0xffffff00	255.255.255.0
25	7	2	126	0xffffff80	255.255.255.128
26	6	4	62	0xffffffc0	255.255.255.192
27	5	8	30	0xffffffe0	255.255.255.224
28	4	16	14	0xfffffff0	255.255.255.240
29	3	32	6	0xfffffff8	255.255.255.248
30	2	64	2	0xfffffffc	255.255.255.252
32	0	256	1	0xffffffff	255.255.255.255

NetMasks

Each network on a PortMaster has an associated netmask. The single most important thing to understand about routing on a PortMaster is that each network number has ONE netmask which must be the same for all subnets; the PortMaster does not support variable length subnet masks.

Therefore if the administrator mistakenly sets different netmasks on the same network, the PortMaster has to choose one. Here are the rules the PortMaster follows to decide what netmask to use when a new interface comes up.

Anytime the PortMaster establishes a point-to-point link a host route is added. Then the following rules are applied if there is no static Netmask Table entry for the network:

1. If the netmask is 0xffffffff, it is ignored.
2. If no netmasks exist currently for this network, the new netmask specified in the interface is used.
3. If the netmask is the same as the active netmask from an interface which previously existed, everything is fine and the current netmask is used.

4. If either netmask (the new one or the active one) is 0xffffff00, this becomes the preferred netmask.
5. If the new netmask has more bits set than the active netmask, the new netmask is used, otherwise the original active netmask is retained.
6. If none of these rules apply, the default netmask for the class of address is used.

Remember, the PortMaster supports ONE netmask per network, not per subnet.

Routing Concepts

When a host sends an IP data packet where the destination host and the sending host are on the same subnet, the packet goes directly to the destination host. If the destination host and sending host are on different subnets, the packet goes to a router. Addresses make routing and packet delivery possible.

Routing and routing protocols are two different concepts. Routing specifies which hop is next for a given destination. Routing protocols describe how a router updates its routing information. The primary function of the router is to direct packets between networks, delivering them to their final destination or to another router. (A router-to-router transmission is called a hop.) A router has two or more network interfaces to different networks or subnets to allow packet transmission between networks.

To determine whether the destination host is on the same network (or subnet), the sending host compares the network portions of the destination address and its own address. If the network and subnet portion of the IP addresses are the same, the destination host is on the same network. If the network or subnet numbers are different, the destination host is on another network, and the data packet must go to a router.

The PortMaster is a router that contains a routing table. A routing table is a list of routes. A route tells a host or router the next place to send a packet to get it closer to its destination. A route consists of a destination specifier, a gateway to the destination, and a metric to determine how desirable this gateway is for reaching the destination. When a router receives a packet to be forwarded, the router looks in the packet to find the destination address, then the routing table is consulted to find a route for the specified destination. Once the route is determined, the packet is forwarded to the associated gateway. The destination in a route can be either a host, a subnet, or a network. PortMasters require one subnet mask per network but do support host routes.

Note – The PortMaster key routing concept is that each network on a PortMaster has one subnet mask.

A routing protocol is a method of exchanging routes between routers. RIP is a routing protocol described in RFC 1058, "Routing Information Protocol." The PortMaster supports RIP for routing both IP and IPX. All of the routing concepts described in this section apply to both IP and IPX packets, except that IPX has only networks, no subnets.

ARP

An Ethernet device listens for two addresses, its own MAC address and MAC broadcasts. If a host receives an ARP request and its own IP address is the one requested, it replies to the ARP requester with its own MAC address. The requester then adds the IP address and MAC translation to its own ARP cache for future use.The PortMaster ARP cache entries expire after 15 minutes. Near the end of the 15 minute interval the PortMaster sends another ARP request to refresh the entry.

Proxy ARP

Livingston products support proxy ARP. ARP is used to discover the Media Access Control (MAC) address associated with a given IP address. The PortMaster responds to ARP requests for addresses if it knows of a route to the address through another interface.

As a result, if a dial-in user is given an address on the same subnet as the PortMaster Ethernet interface, hosts on that Ethernet can ARP for the IP address of the dial-in user and the PortMaster responds to the ARP request with its own Ethernet MAC address.

Livingston's Implementation of Routing

The router gathers and maintains information in a routing table that enables the transmission of data between networks. The routing table contains an entry for each identified route and can be configured statically, maintained by the router dynamically via RIP, or both.

PortMasters determine if a packet is local or needs to be routed based on the destination IP address of the packet, and the IP address and subnet mask of the PortMaster Ethernet interface. For example, if the PortMaster Ethernet address is

192.168.1.1 and the netmask is set to 255.255.255.0, then all hosts with addresses between 192.168.1.1 and 192.168.1.254 are deemed local hosts and packets for these hosts do not require routing.

If a packet requires routing, the routing table is consulting with one of two results, if a route is found the packet is sent to the gateway specified in the route, if no route is found the packet is discarded and an ICMP unreachable packet is sent to the source of the packet. The gateway is always expected to be one hop away.

Routing can occur over Ethernet, synchronous, and asynchronous lines. RIP updates can be turned on or off for individual interfaces. Routing over asynchronous lines can provide significant savings for small offices by allowing the use of regular phone lines instead of expensive leased lines.

PortMasters can send default route information as part of normal RIP messages, if routing is turned on. Static routes can be defined and used. PortMasters support host routes, subnet routes (although all netmasks must be the same for a given network number) and network routes.

Each interface can be configured to listen to routing updates, broadcast routing updates, both, or neither.

- Broadcast—Sends RIP information to the interface.
- Listen mode—Accepts RIP information on the interface.

Routing is set on the Ethernet interface(s), hardwired network ports, in the User Table or RADIUS for dial-in users, and in the Location Table for dial-out locations. IPX routing is supported using RIP and Novell's Service Advertisement Protocol (SAP).

Note – An interface is defined as the virtual connection between a PortMaster port and the network to which it is connected. The connection can be permanent as with the Ethernet interface or network hardwired ports, or it can be temporary, as with ports used for dial-in or dial-out connections.

For more information about how the PortMaster works, refer to Chapter 3, "How PortMasters Work."

Routing Table

The PortMaster maintains a Routing Table that is divided into three parts.

- Default Gateway
  - Learned gateway, which is learned externally
  - Primary gateway, which is learned when you specify a gateway during configuration
- Host Route Table
- Network Route Table

Host and network routes are stored in hashed lookup format which fixes the lookup time regardless of the number of entries. The `show routes` command shows the default route first (if any), then host routes, then network routes, expired routes that are no longer being advertised are displayed at the end. Routes that have very recently expired are marked with an O and are advertised with a hop count of 16 in RIP (unreachable). These routes appear mixed with the other host or network routes; after they are no longer advertised they appear with the other expired routes in the last section.

Each routing table entry includes the following information:

- Destination
- Gateway
- Metric
- Flags
- Interface

When a routing table entry is needed, first the host route table is examined. If no route is found, the netmask table is queried for the netmask associated with the given IP address and a network address is calculated. The network route table is examined for that network address. If no route is found, the learned gateway is used if it exists, otherwise the primary gateway is used. If no route is found an ICMP Unreachable message is returned to the source address indicating that no route was found, and the packet is discarded.

Static routes are never overwritten with learned (dynamic) routes, but if a default gateway with a better metric than the primary gateway is learned and default routes are being listened for, the new gateway is set as the learned gateway. In addition, the learned gateway is replaced if a default gateway with a lower metric is found.

Routing table entries are aged according to the following formula. For RIP, updates are expected every 30 seconds. After 120 seconds if another route for a given destination is observed, the new route is used for the destination. After 180 seconds without an update, we make the route obsolete by setting its metric to 16. The routing timer is suspended if an on-demand interface is suspended. Routes are only valid for active interfaces. If an interface goes down, all routes that go through the interface are examined. If the specified gateway is available using another interface, the route is moved to the active interface. Otherwise the routing table entry is marked as obsolete. The routing table flags are described in Table 2-3.

Table 2-3 Routing Table Flags

Flag	**Definition**	**Description**
H	Host	Host route
N	Network	Network route
L	Local	This network or destination is directly attached. If this is a point-to-point link it can be reached by sending the packet down the link; otherwise, we can reach hosts on this network with an ARP request.
S	Static	Route was added through the static route table
D	Dynamic	The route was learned via RIP
C	Changed	Changed recently but not yet propagated via RIP
O	Obsolete	Obsolete, marked for deletion

Note – A gateway is always expected to be one hop away. The PortMaster never looks up a gateway again in the routing table.

IPX routing works the same as IP routing except there are no host routes.

Default Gateway

If you specify a default gateway, all packets to destinations not found in the routing table of the PortMaster are forwarded to the default gateway. A router with more extensive route information than the PortMaster is usually specified as the default gateway, for example, the upstream Internet Service Provider router.

Managing Network Devices Using SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that allows devices to communicate management information. SNMP has the following parts:

- An SNMP agent (provided in ComOS)
- An SNMP manager (not provided)
- A Management Information Base (MIB)

SNMP specifies the message format for exchanging information between the SNMP manager and an SNMP agent. The SNMP manager is typically part of some Network Management System (NMS).

The SNMP agent contains MIB variables that can be changed or queried by the SNMP manager. The agent gathers information from the MIB, which resides on the target device. MIB information can include device parameters and network statistical data. The agent is capable of responding to requests to get or set data from the manager.

Livingston products provide both MIB I and MIB II support as specified in RFC 1213. SNMP management can be enabled for any PortMaster.

Community Strings

Community strings allow you to control access to the MIB information on selected SNMP devices. The read and write community strings act like passwords to permit access to the SNMP agent information. The read community string must be known by any device allowed to access or read the MIB information. The default read community string is “public”. The write community string must be known by any device before information can be set on the SNMP agent. The default write community string is “private”. Community strings should be set on SNMP agents so that configuration information is not changed by unauthorized users.

Read and Write Hosts

PortMaster products allow you to control SNMP security by specifying the IP addresses of the hosts that are allowed to access SNMP information. The specification of read and write hosts allows another level of security beyond the community strings. If SNMP hosts are specified, each host wanting to access SNMP information must not only possess the correct community string, they must also be on the read/write host list. This additional level of security allows only authorized SNMP managers to access or change sensitive MIB information. Use of the default write community string (private) is strongly discouraged.

Using Naming Services and the Host Table

Naming services are used to associate IP addresses with host names. Many networks use the Domain Name System (DNS) or the Network Information Service (NIS) for mapping host names to IP addresses. Both services are used to identify and locate objects and resources on the network. The IP address of the name server must be specified during the configuration process in order to use DNS or NIS.

PortMasters allow you to specify an internal host table, which can be used in addition to DNS and NIS. The host table allows each unique IP address to be aliased to a unique name. The host table is consulted when a port set for host access prompts for the name of the host. The table is used to identify the IP address of the requested host. If the user specified host name is not found in the hosts table then NIS or DNS is consulted.

Note – The internal host table should only be used when no other host mapping facility is available. This reduces confusion and the amount of network maintenance required.

Managing Network Security

PortMaster products allow you to maintain network security using a variety of methods. Security is a general term that refers to restricting access to network devices and data. To enable security features, you must identify sensitive information, find the network access points to the sensitive information, and secure and maintain the access points.

PortMaster security methods include:

- Dial-back for remote access users
- Local passwords before connections are established
- Access control filters for host connections
- Inbound and outbound packet filtering
- IP packet filtering by protocol, source and destination address, and port
- IPX packet filtering by source and destination network, node, and socket

- SAP filtering
- PAP and CHAP authentication protocols for PPP connections
- Password security for administrative access
- Remote Authentication Dial In User Service (RADIUS) support

Each of these security methods is described in more detail later in this guide. All or some of these security methods can be configured as you configure the system-wide parameters and each interface. RADIUS is described in the next section; however, for more information about configuring RADIUS, refer to the *RADIUS Administrator's Guide*.

RADIUS

RADIUS is a protocol invented by Livingston Enterprises that provides security for distributed network environments. RADIUS provides an open and scalable client/server security system. The RADIUS server can be adapted to work with third-party security products or proprietary security systems. Any communications server or network hardware that supports the RADIUS protocol can communicate with a RADIUS server.

RADIUS consolidates all user authentication and network service access information on the authentication (RADIUS) server. The server can authenticate users against a UNIX password file, NIS databases, or a separately maintained RADIUS database. The PortMaster acts as a RADIUS client and sends authentication requests to the RADIUS server and acts on responses sent back by the server. For more information about RADIUS, refer to the *RADIUS Administrator's Guide*.

How PortMasters Work 3

This chapter provides an overview of how a PortMaster operates and describes each of the ways an asynchronous serial port on a PortMaster can be used. A detailed discussion of each use is included along with an example. The purpose of this chapter is to give you an idea of what the PortMaster capabilities are so you can choose how to configure your system. Synchronous port uses are described in Chapter 7 and Chapters 15 through 18.

The following operational information is provided:

- What happens when a PortMaster is booted
- What happens during normal PortMaster operation
- An overview of ports and interfaces
- Managing security on a PortMaster
- Understanding the port states

The following asynchronous port configurations are discussed:

- Configuring a port to allow users to login to a computer on the network using telnet, rlogin, pmd, or netdata application services.
- Configuring a port to allow computers to access shared devices on the PortMaster, such as a printer or modem.
- Configuring a port to allow outside users to dial in to the network and inside users to dial out to other networks using SLIP or PPP.
- Configuring a port for a permanent connection to a leased-line modem, async to sync converter, or Frame Relay Asynchronous Device (FRAD).

Detailed configuration information for asynchronous ports is described in Chapter 6, “Configuring an Asynchronous Port.” Usage and configuration information for synchronous ports is described in Chapter 7, “Configuring a Synchronous WAN Port.” Specific examples of different configurations are given in Chapters 11 through 18.

Understanding PortMaster Operation

This section describes what happens when a PortMaster connection is requested and initiated. Many of the terms used in this section are defined later in the guide so it may be confusing at first. However, take the time to read this section. The information contained is very useful for understanding how the PortMaster works.

Booting the PortMaster

When you turn the power on, the PortMaster runs self-diagnostics (displaying the results to port S0 if the console dip switch is up). The PortMaster then checks the status of the network dip switch.

If the network dip switch is down, the PortMaster boots from the ComOS stored in nonvolatile flash RAM. The PortMaster has 512 KB of Flash RAM divided into four banks, and 1 MB of DRAM (expandable to 4 MB or 16 MB)[1]. Flash RAM banks 0, 1, and 3 store the compressed ComOS. Bank 2 stores the saved configuration. The PortMaster uncompresses and loads the ComOS into DRAM. If a valid ComOS is not found in Flash then it attempts to boot from the network as described in the next paragraph.

If the network dip switch is up, or if a valid ComOS is not found in Flash, the PortMaster sends a RARP message to the ether0 Ethernet interface to find its IP address. If it gets a reply it then attempts to boot itself across the network using TFTP to download a netbootable ComOS image from the host that replied to the RARP. The TFTP process begins by transferring the `/tftpboot/`*`ADDRESS.TYP`* file where *ADDRESS* is the uppercase 8-character hexadecimal expression of the IP address of the PortMaster and *TYP* is the 3 character boot extension describing the model of PortMaster, as shown in Table 3-1. If `/tftpboot/`*`ADDRESS.TYP`* is not found, the PortMaster then requests `/tftpboot/GENERIC.`*`TYP`*.

Table 3-1 Boot Extensions

Boot Extension	**PortMaster Model**
`PM2`	PM-2, PM-2E, PM-2R, PM-2ER
`IRX`	IRX, any model
`P25`	PM-25
`PMO`	PortMaster Office Router, any model

1.The DRAM in the PortMaster Office Router is not expandable.

The ComOS can also be downloaded via serial cable through the console port, see “Network Booting” on page 19-12.

Once the ComOS is loaded and running, the user configuration is loaded from Flash bank 2. If no address is configured for the Ethernet interface and no address was obtained from netbooting, the PortMaster now sends a RARP message to discover its IP address. This action can be monitored by the “Install New PortMaster” option of `pminstall` on SunOS 4.1.3. If the PortMaster receives a reply to the RARP message, its IP address is set in dynamic memory.

At this point the PortMaster is fully booted with its configuration loaded into DRAM. This process takes less than a minute. After successfully booting, the Status LED will be on, blinking off once every 5 seconds. Refer to the *Hardware Installation Guide* for the location of the Status LED and for troubleshooting procedures if the LED is not behaving as described.

After the PortMaster Boots

Once the PortMaster has successfully booted, all Ethernet interfaces are started, modem initialization strings are sent to asynchronous ports that have modem table entries defined, and all network hardwired ports and continuous dial-out locations are initiated. The PortMaster then attempts to dial out to all on-demand locations that have any form of routing set for them, so that it can exchange routing information. Broadcasting and listening for routing packets is started on interfaces configured for routing.

If there are any ports configured as host devices using the PortMaster device service, TCP connections are established to the `in.pmd` PortMaster daemon running on those hosts at port 1642. The PortMaster also listens for TCP connections to any ports configured as network devices. In addition, the PortMaster listens for the PMconsole connection on TCP port 1643, for administrative telnet sessions and for SNMP requests (if configured to do so).

Less than a minute has passed since the power switch was turned on. The PortMaster is now ready to begin providing dial-in and dial-out service.

PortMaster Operation

When the PortMaster receives packets going to an on-demand location that is suspended (not currently active) it dials out to that location if a line is available. If idle timers expire on a connection, the connection is brought down, freeing the port for other uses. At regular intervals the packet queues are checked for dial-out locations configured for multi-line load balancing to see if more bandwidth is needed, and if so, the PortMaster dials out on an additional port and adds that to the existing interface.

When users dial in they are authenticated and provided with their configured service.

Ports and Interfaces

To fully understand how the PortMaster works, it is absolutely vital to understand the distinction between port and interface. A "port" refers to either a TCP or UDP port, or more often to a physical port on the PortMaster, such as S1 or W1, whether asynchronous or synchronous. The Ethernet connector is also sometimes referred to as a port. Some models also have a parallel port, P0, for connecting a printer for use as a host device or (more rarely) a network device. These are all ports.

An "interface" refers to a logical (as opposed to physical) routing construct. For example, ether0 is an interface, but also a port. S1 is a port, and if it was used for a network hardwired connection as a point-to-point link using SLIP or PPP it would have an attached interface called "ptp1". However if S1 and S2 were both used to connect to another site using multi-line load balancing, there would still be only one interface, either "ptp1" (if S1 connected first) or "ptp2" (if S2 connected first). If a user dialed into port S3 and established a SLIP or PPP connection the new interface would be called "ptp3". However, if instead of establishing a network connection the user established a telnet connection to a host, no interface would be created.

On-demand locations always have interfaces associated with them, typically starting at one higher than the number of ports. For example, if you have a 30 port PortMaster, your on-demand locations will start at ptp30 and count up from there. When there is an active connection established an on-demand interface looks like any other. When there is no active connection, the on-demand location is said to be suspended.

A synchronous port can use Frame Relay instead of PPP; Frame Relay interfaces are called "frm1" instead of "ptp1". Some models call their synchronous port W1 rather than S1 because they already have an asynchronous port S1; thus you may see interfaces called "ptpW1" or "frmW1" as well. You can even have two Frame Relay interfaces on a single Frame Relay port, assigning each PVC to one or the other.

ISDN interfaces are slightly more complicated. Some PortMaster models have ISDN BRI ports with integrated NT1, which is called a "U interface" in ISDN terminology, but that "interface" should not be confused with the kind of interface we have defined in this section. These ports are physically an RJ-45 jack, accepting an 8-pin RJ-45 connector directly from an ISDN phone line in countries following the USA telephone standards. The ISDN BRI port uses two of the wires to provide two B-channels for data and one D-channel for signalling. The two B-channels are treated as two ports for the purpose of configuration, even though they come in on one physical port. So you have one physical U interface going to two ports (say S10 and S11) which can become two interfaces “ptp10” and “ptp11” for two different users.

If you are using the command line interface, the `ifconfig` command shows you all the current interfaces, and the `show arp` *`interface`* command shows you ARP table entries for Ethernet and Frame Relay interfaces.

PortMaster Security Management

PortMaster security is controlled through the User Table or RADIUS security. When a dial-in user attempts to authenticate at the login prompt, the PortMaster uses the entry in the User Table that corresponds to the current user. This process applies to both PAP and CHAP authentication as well. If the password entered by the user does not match, the PortMaster denies access with an “Invalid Login” message. If there is no User Table entry and Port Security is off, the PortMaster passes the user on to the Host defined for that port using the selected Login Service. In this situation the specified host is expected to authenticate the user.

If Port Security is On and the user was not found in the User Table, the PortMaster queries the RADIUS server if one has been configured. If the user name is not found in the User Table, Port Security is On, and no RADIUS server is configured in the global configuration of the PortMaster, access is denied with an “Invalid Login” message. If the RADIUS server is queried and does not respond within 30 seconds (and neither does the alternate RADIUS server), access is denied with an “Invalid Login” message.

Access can also be denied if the specified Login Service is unavailable -- for example, if the PortMaster Login Service has been selected for the user but the selected host does not have the `in.pmd` PortMaster daemon installed, access is denied. Access is denied with the “Host Is Currently Unavailable” message if the host is down or otherwise not responding to the login request.

If an access filter is configured on the port and the login host for the user is not permitted by the access filter, the PortMaster refuses service with an Access Denied message. If the access override parameter is set on the port, the PortMaster asks the user to authenticate himself, even though the default access filter would deny access.

Refer to the *RADIUS Administrator’s Guide* for more information about RADIUS.

Port Status

Each of the PortMaster ports has a status at all times. Each status is described in Table 3-2.

Note – On older Livingston expansion boards (ports s10-s29) and system boards (s0-s9) the carrier signal floats high if nothing is attached; in this case the port shows a status of USERNAME. This condition is harmless. Newer boards pull carrier low if nothing is attached to the port; in this case the port status is IDLE.

Table 3-2 PortMaster Port Status

Status	Description
IDLE	The port is not in use.
USERNAME	The Login Prompt is displayed on the port.
HOSTNAME	The host: prompt is displayed on the port.
PASSWORD	The Password: prompt is displayed on the port.
CONNECTING	A connection is being established on the port.
ESTABLISHED	A connection is active on the port.
DISCONNECTING	The connection has just ended and the port is returning to the IDLE state.
INITIALIZING	The modem attached to the port is being initialized by the modem table.
COMMAND	The command line interface is being used on the port.
NO-SERVICE	An ISDN port is not receiving service from the telephone company.

Allowing Users to Log In to a Host

PortMasters can be configured to allow dial-in users to log into a specified host or be prompted for a login host. This configuration is called user login. In user login mode, after the attached modem answers and completes rate negotiation, the user is prompted for their login name. Once the user is identified as a valid user through the PortMaster internal User Table or RADIUS security, a login session is established on the host specified for the port. The User Table is described in Chapter 8, “Configuring Dial-In Users.” Figure 3-1 shows a diagram of this configuration.

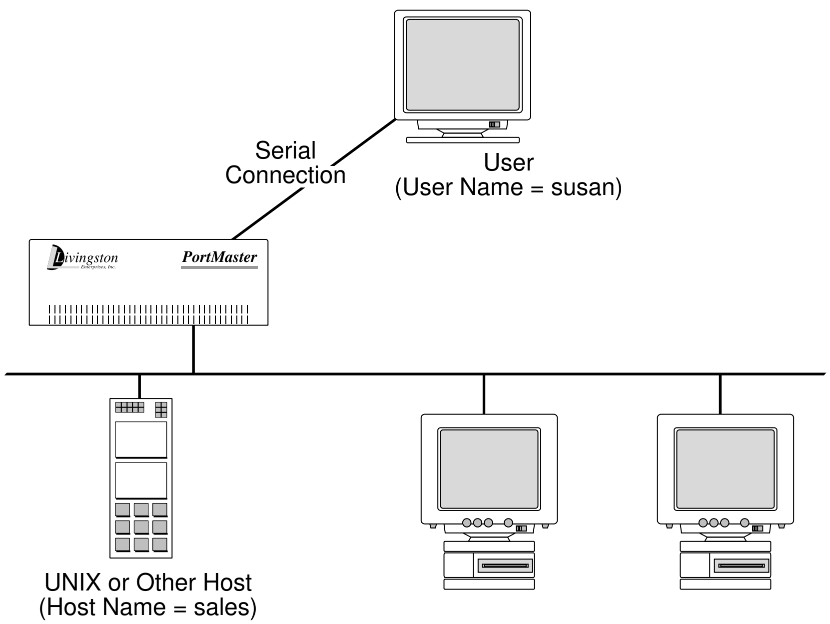

Figure 3-1 User Login Configuration

In Figure 3-1 after the user named “susan” is verified as an authorized user, susan is connected to the host named “sales,” specified as the host for this port. The port type, user login, can be selected along with the host device and network port types. Each port can be set for several different functions, giving the PortMaster configuration more flexibility. However, each port only operates in one mode at a time. For example, if a port connects a dial-in user login request, this port cannot be used for anything else until the current session is terminated. The port is then available for dial-out use or any other purpose specified when the port was configured.

Once the user login port type has been selected you have several options for the login service you want. The login service defines the method used to connect the login user to the host.

Login Services

The following login services can be selected:

- PortMaster login (`in.pmd`)
- Rlogin
- Telnet
- Netdata

PortMaster Login Service

The PortMaster login service is the most efficient and highest performance login service. This service can be used with any workstation that has the PortMaster `in.pmd` daemon software installed. PortMaster login is the default and preferred service because it allows the specified port to operate like a serial port on the host. This service also consumes fewer resources on the host by requiring only one daemon per PortMaster rather than one daemon per user.

Rlogin Login Service

Rlogin is the remote login service. This service is used primarily by UNIX workstations, although not exclusively. Generally, it is preferable to use rlogin because rlogin is able to carry certain user session parameters forward. Use rlogin in environments where it is supported by the hosts, but PortMaster service is not.

Telnet Login Service

Telnet is a terminal protocol supported by most computers using the TCP/IP protocol. Once the connection is established, keystrokes are passed from one system to the other. Telnet service should be used in networks where rlogin or PortMaster login service is unavailable.

Netdata Login Service

The netdata type of login service provides a TCP clear channel on which 8-bit data is passed without interpretation. This service can be used to connect the selected port to another serial port on a different PortMaster. Netdata is most commonly used for special applications that use a socket interface. This login service provides a direct data link from the device connected to the PortMaster port to the application. With this type of socket connection, no special option negotiation or protocol is required. Netdata is more commonly used for outgoing connection from the host application to the device attached to the PortMaster, rather than as login service. However, it can be used either way.

The default TCP port number for the netdata service is 6000, but you may specify any TCP port number from 1 to 65535.

Allowing Access to Shared Devices

One of the functions of a communications server is to provide network users access to shared devices such as printers and modems. This can be done if the port connected to the printer or modem is configured as a host device port. This configuration is also useful for tip and uucp services.

Once a port is defined as host device, a device service must be selected that defines the method used to connect the user to the specified port and device. Host device services include: PortMaster, rlogin, telnet, and netdata.

Host device ports can be accessed by establishing a pseudo-tty connection to the port from a UNIX host with the PortMaster daemon software installed. In this case, the port operates as a host-controlled device. Figure 3-2 shows a diagram of the host device configuration using the PortMaster device service and a pseudo-tty connection. This configuration is most commonly used to access shared devices such as printers.

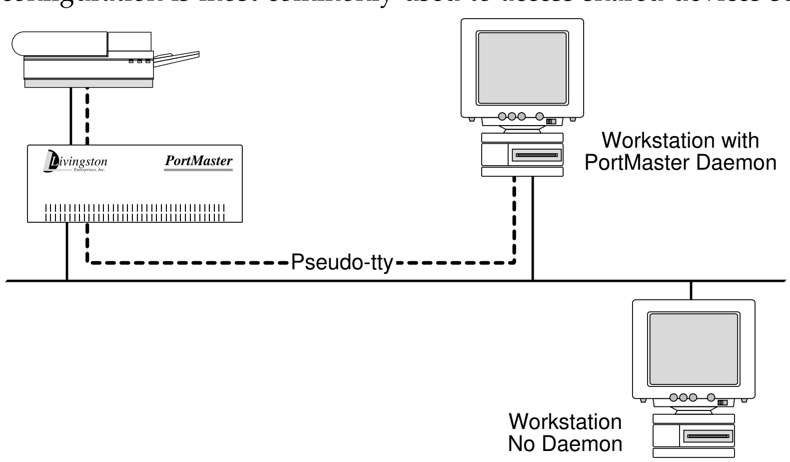

Figure 3-2 Host Device Configuration

Figure 3-3 shows a diagram of the host device configuration where the device service is set as rlogin, telnet, or netdata. In this configuration the host device name is set as `/dev/network`. This configuration is used in cases where users want to telnet or rlogin to the shared device before transferring data, such as with a modem.

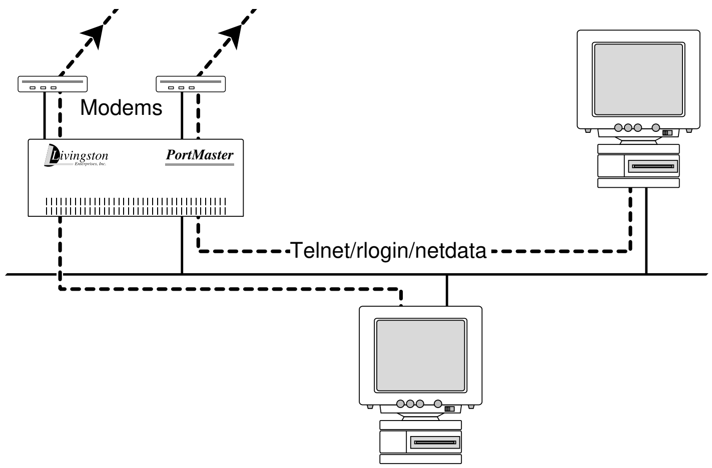

Figure 3-3 Network Device Configuration

Once the port type is set as host device, the device service must be selected and the host name entered. If the device service is set to PortMaster for pseudo-tty operation, a host name must be specified either in the port configuration or as the global default host. In addition, the PortMaster `in.pmd` daemon must be installed on the specified host.

Device Services

The device service defines the method used to connect a host to a host device port. The following device service options can be selected:

- PortMaster
- Rlogin
- Telnet
- Netdata

PortMaster Device Service

The PortMaster device service is the most efficient and highest performance service. This service can be used with any workstation that has the PortMaster `in.pmd` daemon installed. PortMaster service is the default and preferred service because it allows the specified port to operate like a serial port installed on the host.

If this service is selected, the host device name must be the name of a pseudo-tty device listed in the /dev directory of each UNIX host with access to the shared device. The standard device entries have the following ranges:

`/dev/ttyp0` through `/dev/ttypf`
`/dev/ttyq0` through `/dev/ttyqf`
`/dev/ttyr0` through `/dev/ttyrf`
and so on.

Since these tty devices can be dynamically selected for use by a variety of host programs, devices from the end of the tty list should be used for PortMaster shared devices. Most programs start their selection from the beginning of the device list, so selecting devices at the end of the list minimizes the possibility of finding a device unavailable.

This configuration is sometimes referred to as the host device configuration because the shared device you are connecting to through the PortMaster is known to the host as /dev/tty**, where ** is the specific device identifier.

Rlogin Device Service

Rlogin is the method for logging into a remote machine from a workstation. Once the login and password procedures are completed, a session is started on the host. In the case of device service, once the session is successfully established, the host applications can directly read and write data to the PortMaster serial port. No password is required for a PortMaster rlogin device service connection.

If multiple ports on the PortMaster are configured for rlogin host device service, a pool of available ports is formed automatically by the PortMaster. Once all of the available ports are occupied with hosts, new users are given a “Connection Refused” message.

In this configuration, the device name must be set to `/dev/network`.

Telnet Device Service

Telnet is a remote terminal protocol supported by most computers using TCP/IP protocols. Telnet allows the user at one site to establish a TCP connection to a login server at another site. Once the connection is established, keystrokes are passed from one system to the other. Telnet service should be used in networks where a variety of hardware devices with different operating systems must use the selected port.

In this configuration, the device name must be set to `/dev/network`.

The default TCP port number for telnet is 23; however, another TCP port can be specified on a per-port basis. All ports with a common telnet port number form a pool, similar to the rlogin pool.

Note – If you use telnet to administer the PortMaster, you should select a different TCP port number for your administrative telnet port.

Netdata Device Service

The netdata type of device service provides a TCP clear channel on which 8-bit data is passed without interpretation. This service can be used to connect to the selected port from another serial port on a different PortMaster. This configuration can provide network connections between hosts on different networks. Netdata is most commonly used for special applications that use a socket interface. This device service provides a direct data link from the application to the device connected to the PortMaster port. With the socket connection, no special option negotiation or protocol is required.

The default TCP port number for the netdata service is 6000, but you may specify another port.

In this configuration, the device name must be set to `/dev/network`.

Selecting the host device port type with the rlogin, Telnet, or netdata device service is sometimes referred to as the network device configuration because the shared device you are connecting to through the PortMaster is specified as `/dev/network`.

Allowing Network Dial-In and or Dial-Out Operation

You can configure PortMaster ports for network dial-in only operation, dial-out only operation, or both dial-in and dial-out operation. You can select dial-in and dial-out operation with the login and device operation discussed in the previous sections.

Network Dial-In Operation

Network dial-in only operation may be set on ports dedicated to answering requests from mobile or home users. In this configuration, the selected port is used to allow an authorized user to connect to the network for mail, file, and other services using Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) encapsulation. Figure 3-4 shows how the PortMaster provides network connectivity for remote users.

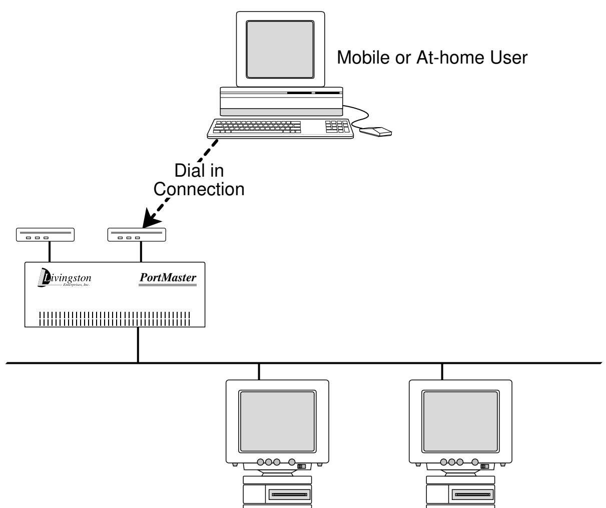

Figure 3-4 Dial-In Only Port Configuration

Network Dial-Out Operation

Network dial-out only operation may be set on ports dedicated to Internet connections or connections to another office. In this configuration, the port is used to establish communication from the PortMaster to an outside location. SLIP or PPP are used for these types of connections. Figure 3-5 shows an example of a dial-out only configuration.

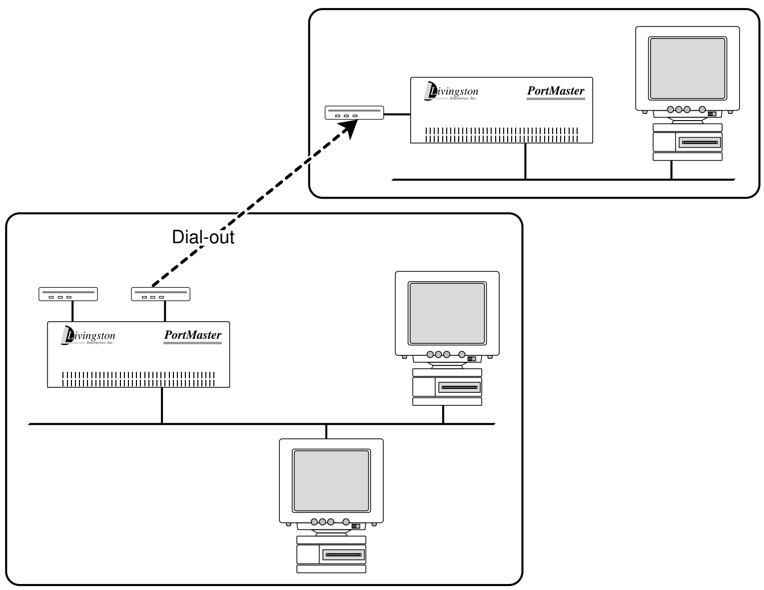

Figure 3-5 Dial-Out Only Port Configuration

Network Dial-In and Dial-Out (Two Way) Operation

Dial-in and dial-out operation on a selected port is called two way operation or dial-in & out operation. Two way operation is specified for ports where both dial-in and dial-out service are needed. Dial-in services with modems allow users to connect to the main network without the cost of leased-line connection. This method can also be used for connecting to remote sites that need only occasional telecommuting or backup connectivity.

To configure dial-in and dial-out operation, the port type must be set to network then the network type is set for dial-in & out. This configuration is explained in more detail in Chapter 6, “Configuring an Asynchronous Port.”

As mentioned in “Network Dial-In Operation” on page 3-13, SLIP and PPP are used to define the method of sending IP packets over standard asynchronous lines with a minimum line speed of 1200 baud. These encapsulation methods allow you to establish connections on an as-needed basis to reduce phone costs.

Using SLIP for Dial-In/Dial-Out Operation

The Serial Line Internet Protocol (SLIP) is an older protocol than PPP and not as robust. However, some hosts only support SLIP. The type of protocol allowed is specified for each dial-in user, dial-out location, or network hardwired port.

Note – Hardware flow control (RTS/CTS) should be used for all SLIP and PPP connections.

Using PPP for Dial-In/Dial-Out Operation

The Point-to-Point Protocol (PPP) is a method of encapsulating network layer IP protocol information on asynchronous point-to-point links. PPP is described in RFCs 1331 and 1332. Livingston’s implementation of PPP provides autodetect PPP support for the Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) on serial ports running PPP. ComOS 3.3 and later supports multilink PPP as described in RFC 1717.

PAP and CHAP Authentication

When a port is configured for PPP the PortMaster autodetects PPP. If a user dials into the port and starts sending PPP packets, the PortMaster starts LCP negotiation and asks the user to authenticate using PAP. If the user refuses PAP authentication, the PortMaster asks the user to authenticate using CHAP. If the user refuses CHAP authentication, the PortMaster hangs up.

If the user accepts PAP authentication, the user sends a PAP ID and PAP password to the PortMaster. The PortMaster treats the ID and password as if it were the user name and password.

If the user accepts CHAP authentication, the communication server sends a CHAP packet to the user. The user is "challenged" to respond. The challenge includes an ID, a random number, and either the host name of the local communications server or the name of the user. The user is required to respond with an encrypted version of the ID and a user name.

When the PortMaster receives the response, the secret is verified by looking up the user name given in the response and performing the same encryption operation. Before a connection is established the passwords must be the same on both ends of the connection. This protocol prevents other network devices from stealing the password and gaining illegal access to the network because the secret is never transmitted. A correct response is required before a network connection is established.

CHAP authentication occurs only at the time the connection is established. No verification is performed while the connection is active. Both the local communication server and the remote device must support CHAP in order to use this protocol.

To configure PAP or CHAP for PPP users, the local User Table or RADIUS must have an entry for each authorized user that includes the user name and password. The passwords on both ends of the connection must be identical or the authentication process fails.

To disallow PAP authentication and only accept CHAP, use the `set pap off` command.

Establishing a Permanent Asynchronous Connection

A permanent network connection can be established. In this configuration, no modem dialing or authentication protocol is required. This configuration is designed for connections to modems configured for leased-line operation, async to sync converters, or Frame Relay Asynchronous Devices and can use SLIP or PPP with IP and IPX. Livingston calls this configuration Hardwired where the Port Type parameter is set to Network and the Network Type parameter is set to Hardwired.

Note – When the network type is Hardwired the port type must be network only. This configures a continuous uninterrupted connection on this port.

An example of a Hardwired port is shown in Figure 3-6.

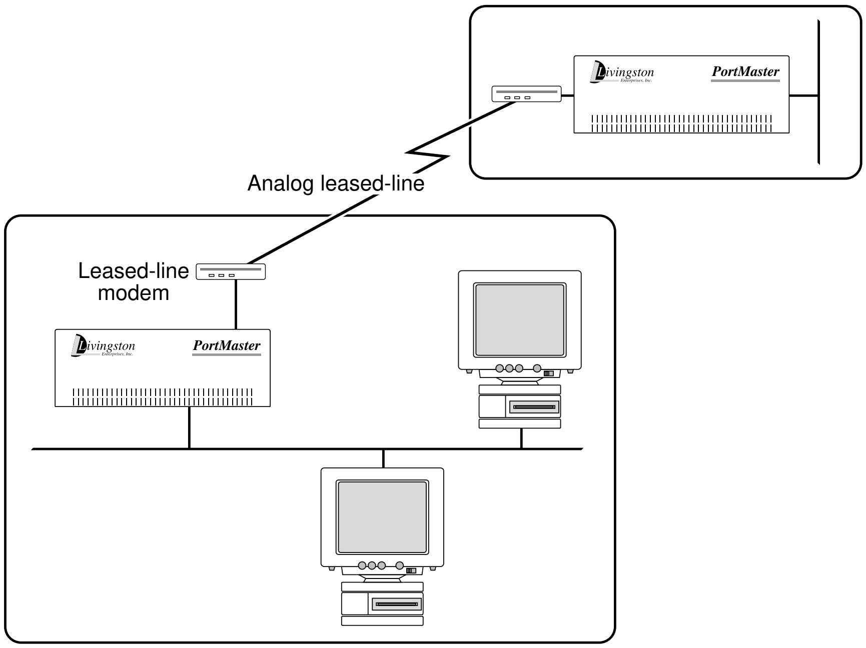

Figure 3-6 Hardwired Port Configuration

Hardwired connections on asynchronous ports provide the continuous connection advantage of a synchronous port (at lower bandwidth) without the cost of T1-line connection.

Once the port is set for a hardwired connection, additional parameters specifically related to this type of connection must be set. These parameters include Protocol, TCP Header Compression, Maximum Transmission Unit (MTU), routing, and assigning an IPX network to the line if you are using the IPX protocol.

Configuring a PortMaster 4

This chapter describes the steps required to configure a PortMaster. These steps are not dependent on which user interface you are using to configure your system. The *Administrator's Guide* for your user interface describes how to set each option. The purpose of this chapter is to review the overall steps required to configure a PortMaster and describe the global parameters.

Each of the possible global parameters are described in this chapter; however, you must only configure the parameters required for the configuration you want. Example configurations are described in Chapters 11 through 18.

This chapter includes the following topics:

- Configuration tips
- Overview of how to configure a PortMaster
- Configuring global (system-wide) parameters
- Setting static routes

Configuration Tips

PortMaster configuration can be confusing because networking parameters can be set for a port, a user, or a location. Use the following tips to determine how to configure your PortMaster:

- If you are configuring a network hardwired port, configure the networking parameters on the port.
- If you configure one or more ports for dial-out operation, configure the networking parameters for the dial-out locations using the Location Table.
- If you configure one or more ports for dial-in operation, configure the networking parameters for the dial-in users using the User Table.
- If you configure a network dialback user, configure the dialback location in the Location Table and refer to the location name in the User Table.

Overview of PortMaster Configuration Steps

The exact PortMaster configuration steps depend upon the hardware you are installing and your network configuration. However, the general configuration steps are the same for all PortMaster products, as follows:

- Connect the hardware as your configuration requires.
- Attach a terminal to the console port and boot the system.
- Log in to the system as the administrator and configure the system address.
- You can now disconnect the console and use the graphical user interface, PMconsole, to configure your system, or continue your configuration using the command line interface.
- Install the PMconsole software on a workstation anywhere on your network.
- Run PMconsole and log in to the new PortMaster using its host name or address, and a password, if set.
- Open the Edit Global parameters window and configure the PortMaster global parameters.

  Each of the PortMaster global parameters is described later in this chapter.
- Open the Edit Ethernet parameters window and configure the Ethernet, IP and IPX protocol parameters for your network.

  Each of the PortMaster Ethernet parameters are described in detail in Chapter 5, "Configuring the Ethernet Interface."
- Select the first asynchronous port and open the edit port window, then configure the asynchronous port parameters. The modem parameters are also set at the same time.

  Each of the PortMaster asynchronous port parameters are described in detail in Chapter 6, "Configuring an Asynchronous Port" along with modem configuration parameters.
- Repeat the port configuration for each asynchronous port or use the clone feature of PMconsole to configure additional ports.
- Select the first synchronous port, if available, and open the edit port window. Then configure the synchronous port parameters to allow for a leased line, ISDN, Frame Relay, or switched 56K connection.

  Each of the PortMaster synchronous port parameters are described in detail in Chapter 7, "Configuring a Synchronous WAN Port."

- Repeat the port configuration for each synchronous port, if more than one is available.
- If you are not using RADIUS, open the User Table and enter each authorized user for your network along with their user type, password, and other configuration information.

  Each of the User Table parameters are described in detail in Chapter 8, "Configuring Dial-In Users."
- Open the Location Table and enter each of the authorized dial-out destinations for your network along with location parameters. If you are configuring a synchronous interface for an ISDN connection, enter your ISDN dial script in the Location Table.

  Each of the Location Table parameters are described in detail in Chapter 9, "Configuring Dial-Out Locations."
- Open the Filter Table and specify filter rules for your network configuration. Once the filters are created, they can be assigned as input or output filters for the Ethernet interface, various users, locations, or hardwired ports.

  Filters are described in detail in Chapter 10, "Configuring Filters."

Once all of the configuration parameters are set, your PortMaster is ready to provide communication service and routing for your network.

Setting Global Parameters

Global parameters are used to set system-wide variables such as the system name, the default gateway, and SNMP monitoring. All parameters can be set using the PMconsole graphical user interface, using commands entered through the system console port, or using administrative telnet. This guide provides general information about each of the parameters and their options.

Figure 4-1 shows an example of the PMconsole global configuration window. The actual window you will see depends on the version of PMconsole you choose for configuring your PortMaster. The instructions for opening and using this window are in the *Administrator's Guide* for your user interface.

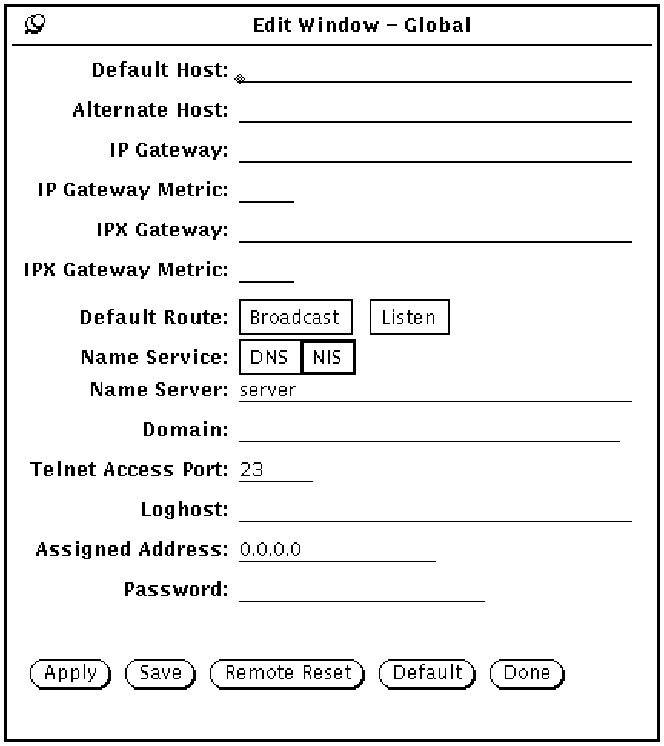

Figure 4-1 Global Configuration Window—X Windows GUI

For specific information about how to configure your system using PMconsole, refer to the *Administrator's Guide* for your graphical user interface.

The following sections describe each of the global parameters and the available options.

Setting the System Name

The system name parameter defines the name of the PortMaster that is used for SNMP queries, IPX protocol routing, and CHAP authentication. Enter a name that is valid for your network. In some versions of PMconsole this value is entered in the SNMP Table window, not the Global parameter window.

Setting the System Password

The password parameter is an ASCII printable string of up to 16 characters used to access the PortMaster administration features. The password must be entered twice when setting it using PMconsole to ensure that it is entered correctly. The password can only be changed by the administrator.

Setting the Default Gateway

The Default Gateway parameter identifies the default IP gateway address, which is the address of the router of last resort. The default gateway is used when no other route is found. The address is entered in dotted-decimal notation.

For IPX networks, the name of the default gateway is entered for the IPX gateway. This gateway is used for networks with no RIP gateways.

The IP and IPX gateway metric parameters can be set between 1 and 15 and indicate the hop count associated with the gateway route. The hop count value is used if the PortMaster is set to listen for default routes from other routers.

Refer to Chapter 2, “Networking Concepts,” for more information about address formats and routing.

Default Routing

As described in Chapter 2, “Networking Concepts,” PortMaster products can automatically send and accept route information as part of RIP messages if routing is turned on. If default routing is on, default routes are sent and accepted, as part of the RIP messages.

When Broadcast is selected for the Default Route parameter the PortMaster advertises itself as a default route in its RIP messages, if a default route is set. When Listen is selected, the PortMaster accepts default route entries in RIP packets from other routers. Both options can be selected at the same time to enable the sending and acceptance of default routing information. If neither option is selected, default route information is not sent with RIP information and the PortMaster ignores all default route entries it receives from other routers.

Using a Name Service

The PortMaster can work with network name services such as NIS or DNS. Chapter 2, "Networking Concepts" describes these name services. The Name Service parameter is set to the name service, if any, used on your network.

Once the name service is set you must set the Name Server parameter to the address of your NIS or DNS server and enter the domain name of your network into the Domain parameter.

The PortMaster stores all information by address not name. As a result, configuring the name server is only useful if you are using the command line interface for administration or if you prompt a login user for a host. If you are not using either of these features, you do not need to set the Name Service, Name Server, or Domain parameters.

Using Telnet for Administration Tasks

The telnet access port can be set to any number between 0 and 65535. The telnet port allows the administrator to access and maintain the PortMaster using a telnet connection to this TCP port. If zero (0) is used telnet administration is disabled. The default value is port 23. Up to four administrative telnet sessions at a time can be used.

If the console parameter is set from a telnet session, the current connection becomes the console. This feature is useful for administrators who log in to a port using telnet and need to access the console for debugging purposes.

Setting System Logging

PortMaster products allow you to log authentication information to a log file for network accounting purposes. Information is logged to the `auth.info` facility of syslog at the host entered as the Loghost parameter. In addition, packet filter rules with the log keyword are logged to the `auth.notice` facility. Logging is performed by the `syslogd` daemon if the following entry is made in your `/etc/syslog.conf` file:

```
auth.info       /var/log/authlog
```

Consult the `syslogd(8)` and `/etc/syslog.conf(5)` man pages on your loghost for more information on system logging.

RADIUS accounting provides a better form of logging usage information. Refer to the *RADIUS Administrator's Guide* for more information.

Dynamically Assigning IP Addresses

IP addresses can be assigned dynamically to network dial-in users using PPP or SLIP to access the network. By assigning addresses as needed, a smaller pool of addresses is required than if every user had his own address. Once a connection is closed the address goes back in the pool and can be reused. The value of the Assigned Address parameter is the first address in the sequence of addresses available for temporary assignment. The PortMaster allocates one address into the pool of addresses for each port configured for network dial in.

Setting SNMP Monitoring

SNMP monitoring as described in Chapter 2, "Networking Concepts," is used to set and collect information on SNMP-capable devices. This feature is most often used to monitor network statistics such as error rate and utilization. Livingston supports MIB-II variables and ships configuration files compatible with various network management packages along with the PMconsole software.

If the SNMP Status parameter is on, the PortMaster accepts SNMP queries. If this parameter is off, all SNMP queries are ignored.

Chapter 2, "Networking Concepts," describes community strings, which are used for SNMP security. The Read Community parameter must have the value of the read community string for your network. In addition, you can specify the Read host or hosts allowed to respond to SNMP get queries on your network. The same is true for the Write Community and Write Hosts parameters. You can specify a list of hosts that can perform SNMP sets, you can allow access for all hosts (not recommended), or you can allow access for no hosts refusing all SNMP get queries.

Configuring the Host Table

Each host attached to an IP network is assigned a unique IP address. PortMasters support a local Host Table to map hostnames to IP addresses. If your network lacks a computer that can perform hostname resolution, the PortMaster allows entries in a local Host Table. Hostnames are only used by the PortMaster for the convenience of the administrator when using the command line interface, and for hostnames entered by users at the host prompt.

To avoid confusion and reduce administrative overhead, Livingston recommends using Domain Name Service (DNS) or Network Information Service (NIS) for hostname resolution rather than using the local Host Table. The PortMaster always checks the local Host Table before using DNS or NIS. For information on setting the NIS or DNS name server and domain, refer to "Using a Name Service" on page 4-6.

Setting Static Routes

Static routes are used to provide routing information when the Routing Information Protocol (RIP) is not running. RIP may not be running for several reasons:

- Network administrators may choose not to run RIP
- Hosts or networks connected to the PortMaster may not be able to run RIP

Static routes are maintained in the Route Table accessed using the Tables menu. Two static route tables are maintained, one for IP and one for IPX. A static route contains the following items:

- Destination
- Gateway
- Metric
- Ticks (IPX routes only)

Refer to Chapter 2, "Networking Concepts" for more information about routing and static routes.

Setting Route Destinations

The route destination is set to the host or network for which the PortMaster will be routing.

Setting Gateway

The route gateway is the address of a locally attached router where packets should be sent for forwarding to the destination. The gateway can never be set to the address of the PortMaster.

For IPX networks, the gateway parameter is set to a hexadecimal address that represents the network number and the node address separated by a colon. For example, 00000002:A0B1C2D3E4F5.

Setting the Metric

The metric in RIP is the number of gateways, hops, a packet must cross to reach its destination. The metric represents the cost of sending the packet through the above gateway to the specified destination.

The Ticks parameter is used on IPX networks to represent the time it takes to send the packet to its destination. Ticks are measured in 50ms increments.

Once all of the global parameters are set you should configure the Ethernet interface as described in Chapter 5, "Configuring the Ethernet Interface."

Setting the Netmask Table

The Netmask Table is provided to allow routes to remain uncollapsed on network boundaries in cases where its necessary to break a network into discontiguous subnets. The PortMaster normally collapses routes on network boundaries as suggested in RFC 1058. However, in certain circumstances where you do not want to do that, the Netmask Table is available.

For example, if the address of ether0 is 172.16.1.1 with a 255.255.255.0 netmask (a class B subnetted on 24 bits) and the destination of ptp1 is 192.168.9.65 with a 255.255.255.240 netmask (a class C subnetted on 28 bits) and routing broadcast is on, the PortMaster's routing broadcast on ether0 claims a route to the entire 192.168.9.0 network. Additionally, the broadcast on ptp1 claims a route to 172.16.0.0, which is entirely proper.

Sometimes, however, you want the PortMaster to collapse routes to some bit boundary, other than the network boundary. In this case, you can use the Netmask Table; however, RIP only supports host and network routes, since it has no provision to include a netmask. Therefore, if you set a static netmask in the Netmask Table, the PortMaster collapses the route to that boundary instead, and broadcasts a host route with that value. Other PortMasters with the same static Netmask Table entry turn the host route back into a subnet route when they receive the RIP packet. This work-around only works if all of the products involved are from Livingston, with two exceptions: 1) If you use a netmask table entry of 255.255.255.255 then the routes are broadcast as host routes and really are host routes, so other routers can use them. Keep in mind, not all routers accept host routes. 2) If the other router has the ability to turn host routes into subnet routes through some mechanism of its own.

The most common use for the static Netmask Table is to split a single class C network into 8 30-host subnets for use in assigned pools. This allows each PortMaster to broadcast a route to the subnet instead of claiming a route to the entire class C. An example of that usage is provided below.

The next most common use for the static Netmask Table is to allow dial-in users to use specified IP addresses across multiple PortMasters, in situations where Assigned IP addresses are not sufficient. This can result in very large Routing Tables and is not recommended except where no other alternative is possible.

The Netmask Table can only be accessed using the command line interface. To add a static netmask, use the `add netmask <network> <netmask>` command. To delete a static netmask, use the `delete netmask <network>` command. The `show table netmask` command shows both dynamic netmasks and static netmasks, marking them accordingly.

Caution – Do not use the static Netmask Table unless you thoroughly understand and need its function. In most circumstances it is NOT necessary. Very large routing updates can result from too much use of the NetMask Table, resulting in adverse effects on performance.

The following Netmask Table example assumes the following:

- You have 20 PortMasters (or anywhere between 8 and 250 PortMasters)
- You assign all the user addresses from the dynamic address assignment pools on the PortMasters
- You are using 27-bit subnets of these three class C networks 192.168.207.0, 192.168.208.0, and 192.168.209.0
- You are using the 192.168.206.0 network for your Ethernet
- All PortMasters involved must be running ComOS 3.1.2 or later
- Proxy ARP is convenient for 7 or fewer PortMasters, but should be avoided as you scale up. Instead, use your 192.168.206.0 network for the Ethernet and divide your other networks up among the PortMasters.
- Each network should provide 30 addresses for the assigned pool of each of 8 PortMasters.

In this example, use the following commands on all of the PortMasters:

```
Command> set ether0 address 192.168.206.X (for some value of X)
Command> set gateway 192.168.206.Y (where Y points at your gateway)
Command> add netmask 192.168.207.0 255.255.255.224
Command> add netmask 192.168.208.0 255.255.255.224
Command> add netmask 192.168.209.0 255.255.255.224
Command> set ether0 routing on
Command> save all
```

The Netmask Table collapses routes on the boundaries specified, so if on one PortMaster you have an assigned pool starting at 192.168.207.33, instead of broadcasting a route to the 192.168.207.0 network the PortMaster would broadcast that it has a host route to 192.168.207.32. The other PortMasters will see that route, look in their own Netmask Table, and convert it back into a subnet route to 192.168.207.33 through 192.168.207.62.

If your gateway out from the Ethernet is not a Livingston product the netmask table is not supported. However, you can set a static route on the gateway for each of the three destination networks for your assigned pools (192.168.207.0, 192.168.208.0, and 192.168.209.0), pointing at one of the PortMasters. The identified PortMaster then forwards packets to the proper PortMaster. If you are using an IRX running ComOS 3.2R or later as your gateway, you could set the Netmask Table on the router also. This allows you to listen to RIP messages from the PortMasters and route directly to each of them.

Configuring the Ethernet Interface 5

This chapter describes how to configure the PortMaster Ethernet interface. All of the possible parameters are reviewed along with explanations of each option. Use the information in this chapter along with the specific configuration information described in Chapters 11 through 18 to configure the PortMaster for your application.

This chapter includes the following topics:

- Setting general Ethernet parameters
- Setting IP protocol parameters
- Setting IPX protocol parameters

Connecting the Hardware

On most PortMaster models you have the choice of several different Ethernet hardware connections:

- Twisted pair Ethernet (10BaseT) using an RJ-45 connector
- Thin Ethernet (10Base2) using a built-in BNC connector or a transceiver with an AUI cable

  The PortMaster Office Router does not have a BNC connector.
- Thick Ethernet (10Base5) using a transceiver and an AUI cable with a DB-15 connector

Connect your network to the Ethernet port that best suits your installation. Use the DIP switches to select the connector type. Refer to your *Hardware Installation Guide* for more information.

General Ethernet Parameters

The Ethernet parameters described in this section allow you to configure your Ethernet interface. In addition to specifying the protocol type (IP, IPX, or both) and address, you must specify any routing and filtering you want on the Ethernet interface.

This subsection describes the general Ethernet parameters that apply to your network regardless of the protocol you use. Figure 5-1 shows an example of the Ethernet configuration window. The actual window you will see depends on the version of PMconsole you choose for configuring your PortMaster.

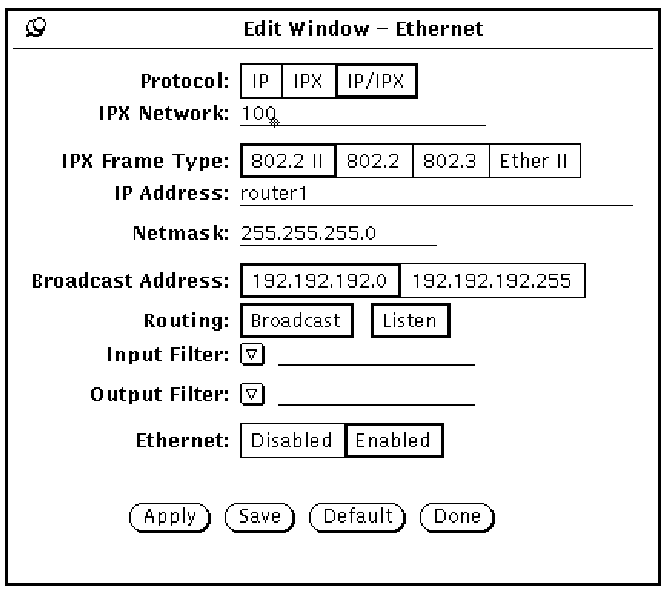

Figure 5-1 Ethernet Configuration Window—X Windows GUI

For specific information about how to configure your system using PMconsole, refer to the *PMconsole Administrator's Guide* for your user interface.

Configuring Routing

As described in Chapter 2, “Networking Concepts,” PortMaster products automatically send and accept route information as RIP messages if routing is turned on.

Select Broadcast for the Routing parameter to broadcast routing packets on the local Ethernet. When Listen is selected, the PortMaster accepts routing packets from other routers on the local Ethernet. Both options can be selected at the same time to enable the sending and acceptance of routing information. If neither option is selected, route information is not sent and the PortMaster ignores all route messages from other routers on the local Ethernet.

Setting Input and Output Filters

Input and output filters can be created and attached to the Ethernet interface. Filters allow you to restrict network traffic. If an input filter is set, all packets received from the Ethernet interface are evaluated against the rule set for the attached filter. Only packets allowed by the filter are passed through the PortMaster. If an output filter is set, only packets allowed by the filter are sent to the interface. For more information about filters, see Chapter 10, “Configuring Filters.”

Ethernet IP Parameters

PortMaster products support both the IP and IPX protocols. When you select a protocol for the Ethernet port, values for the parameters appropriate for the selected protocol must be entered.

This subsection describes the IP parameters, which must be entered if you select IP or IP/IPX protocol support.

Setting the IP Address

The IP address parameter is the same address set during the installation process. When the PortMaster is installed, its IP address is set using the console port. From then on configuration can be done across the network using either PMconsole or administrative telnet.

Note – If you change the IP address of the Ethernet interface, you must reboot the PortMaster for the change to take effect.

Setting the Netmask

Netmasks are used to divide networks into subnets as described in Chapter 2, "Networking Concepts." The default netmask is 255.255.255.0. If you use a different netmask on your network, enter the subnet mask that describes how your network addresses are divided between the network portion and the host portion.

Note – Only one netmask per network is permitted.

Setting the Broadcast Address

The Broadcast Address parameter defines the IP address used as the local broadcast address. The RIP routing protocol uses this address to send information to other hosts on the local Ethernet network. The actual broadcast address is constructed from the IP address of the Ethernet port and the netmask. The two valid values are high, where the host part of the address is all ones (such as 192.168.1.255) or low, where the host part of the address is all zeros (such as 192.168.1.0). The current standard is broadcast high but some hosts still use broadcast address low, including hosts running SunOS 4.x (Solaris 1.x) and earlier.

The value of the Broadcast Address parameter must match the broadcast address set for other hosts on your local Ethernet segment.

Enabling IP Traffic

The Ethernet must be enabled on all PortMasters attached directly to a local Ethernet. When enabled, IP traffic is sent and received through the PortMaster Ethernet port. This parameter should only be disabled if the PortMaster is not attached to a local Ethernet network.

Ethernet IPX Parameters

IPX parameter values must be entered if the IPX or IP/IPX protocols are selected. IPX routing is enabled when either or both Broadcast and Listen are selected for the Routing parameter.

Setting the IPX Network Address

The IPX Network or IPXNet parameter is the IPX network of your local Ethernet segment. The IPX network of the interface is entered in HEX format, described in Chapter 2, "Networking Concepts."

Setting the IPX Frame Type

The IPX frame type must be identified and set to the value used on the local IPX network. The frame type identifies the encapsulation method used on your IPX interfaces. The IPX protocol can be implemented using one of three different IPX encapsulation and frame types, as shown in Table 5-1:

Table 5-1 Novell IPX Encapsulation and Frame Types

IPX Frame Type	Description
Ethernet_802.3	This encapsulation consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. This is the default encapsulation used by Novell NetWare Version 3.11.
Ethernet_II	This encapsulation uses Novell's Ethernet_II and is sometimes used for networks that handle both TCP/IP and IPX traffic.
Ethernet_802.2	This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by Novell NetWare Version 4.0.
Ethernet_802.2_II	This encapsulation is not commonly used.

The decision of encapsulation method and frame type was made at the time your Novell IPX network servers were installed. The PortMaster IPX Frame Type parameter must match the frame type set for your network. Contact your Novell NetWare administrator for information about the frame type used on your network.

Enabling NetBIOS Broadcast Packet Propagation

NetBIOS over IPX uses type 20 broadcast packets propagated to all networks to get information about the named nodes on the network. NetBIOS uses a broadcast mechanism to get this information, because it does not implement a network layer. Before forwarding the packets, the PortMaster performs loop detection as described by the IPX Router Specification available from Novell.

Full NetBIOS protocol compliance requires that the PortMaster be set to propagate and forward type 20 broadcast packets across your IPX network router. When the NetBIOS parameter is on, the PortMaster broadcasts type 20 packets. When the NetBIOS parameter is off, the type 20 packets are not broadcast across the router. The default is off.

Note – The NetBIOS parameter can only be enabled from the command line interface by typing:

```
set NETBIOS on
```

Configuring an Asynchronous Port 6

This chapter describes the steps required to configure a PortMaster asynchronous port. These steps are not dependent on which user interface you are using to configure your system. The *Administrator's Guide* for your user interface describes how to set each option. The purpose of this chapter is to review each of the port parameters and its options.

All of the possible port parameters are described in this chapter; however, you only need to set the parameters required for the configuration you want. Specific configurations are described in Chapters 11 through 18.

This chapter includes the following topics:

- Introduction to port configuration
- Setting ports for login users
- Setting ports to access host devices
- Setting ports for network dial in and dial out users
- Setting ports for dedicated network connections
- Setting general port parameters
- Configuring modems and setting modem parameters

Introduction

A single PortMaster port can be configured for several different types of operation. For example, a port set for login users can also be set to access host devices; this is called TwoWay operation. The port set for TwoWay operation is now available for both login users and users who need to access shared devices. In this configuration the port can be used for two purposes: one now and another one later.

Each of the asynchronous ports is configured using port parameters that can be set through the PMconsole graphical user interface. An example of the asynchronous port configuration window is shown in Figure 6-1. The actual window you will see depends on the version of PMconsole you choose for configuring your PortMaster.

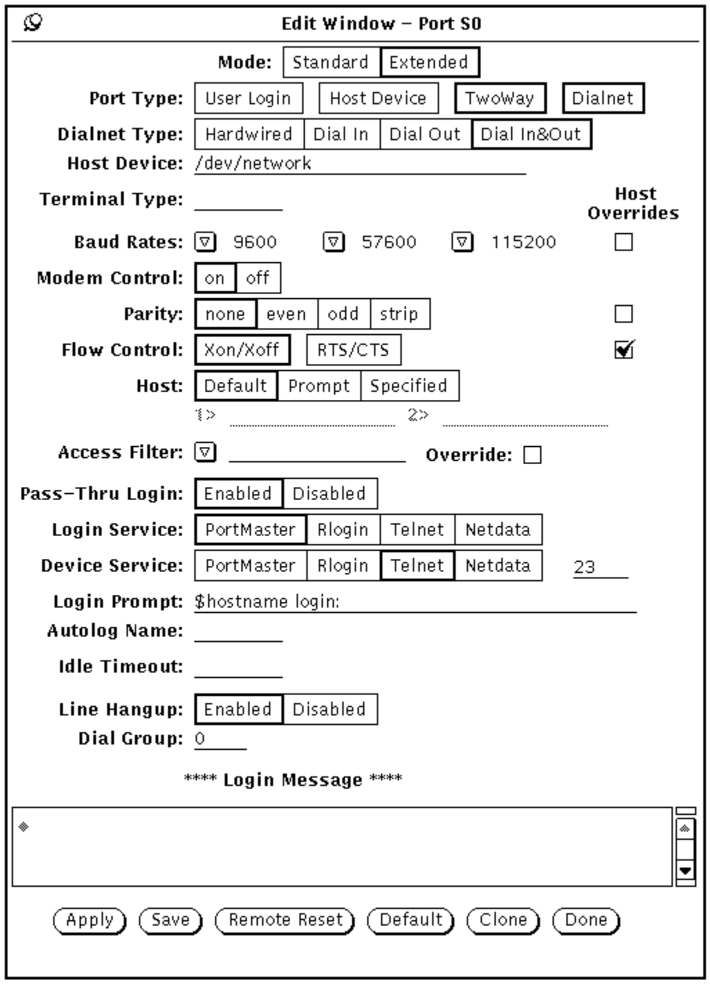

Figure 6-1 Asynchronous Port Window S0—X Windows GUI

All of the available parameters are described in this chapter.

Setting the Asynchronous Port Type

Chapter 3, "How PortMasters Work" describes each of the ways an asynchronous port can be used. This section describes each of the specific parameters used to configure the port.

Setting a Port for Login Users

Setting the Port Type parameter to User Login allows users to be authenticated using the internal User Table or RADIUS and then be transferred to a login session on the host specified for this port. The User Login Port Type can be selected with any of the other Port Type options except for Network Hardwired. For more information about user authentication, refer to Chapter 2, "Networking Concepts." For more information about setting security on ports, see "Setting Port Security" on page 6-12.

Setting the Login Service

Once the Port Type User Login is selected, you can set the Login Service parameter. The Login Service specifies how login sessions are established. Four types of Login Service are available as described in Table 6-1.

Table 6-1 Types of Login Service

Login Service	**Function**
PortMaster	PortMaster is the default login service and can be used to access any host that has the PortMaster `in.pmd` daemon installed. This type of login service is preferred because it makes the PortMaster port operate as if it was a serial port attached to the host. This service is the most cost effective in terms of host resources.
Rlogin	Rlogin uses the rlogin protocol to establish a login session to the specified host. This login method is used on mixed UNIX networks where it is impractical to use the PortMaster login service.
Telnet	Telnet is supported on most TCP/IP hosts. This login service should be selected when the PortMaster and rlogin protocols are not available. The default port number is 23, but other ports can be entered.

Table 6-1 Types of Login Service *(Continued)*

Login Service	Function
Netdata	Netdata creates a virtual connection between the PortMaster port and another serial port on another PortMaster or between the PortMaster port and a host. This login service creates a clear channel TCP connection. To connect to another PortMaster port using netdata, that port must be configured as a Host Device with Device Service Netdata using the same TCP port number. The default netdata port is 6000; however, other ports can be used. This effectively allows any TCP/IP network to be used as an RS-232 cable, without distance limitations. However, with some serial communications protocols, such as FAX, there are potential latency issues.

Specifying the Login Host

The Host parameter is used to specify how the login host is determined for the selected port. There are three ways to determine the login host as described in Table 6-2.

Table 6-2 Login Host Options

Host Option	Description
Default	The host used for this port is the Default or Alternate Host specified in the global parameters.
Prompt	The user is given the opportunity to enter a valid host name or IP address instead of the standard login prompt.
Specified	You set a primary and up to three alternate hosts for this port. This allows you to assign specific ports to specific hosts.

Specifying the Terminal Type

The Terminal Type parameter can be entered if the Port Type is set to User Login or TwoWay and the Login Service is set to PortMaster, rlogin, or telnet. The terminal type is passed as an environment variable when a connection is established with a host. The Terminal Type should be a valid entry on the host you are logging into.

Setting a Port for Access to Shared Devices

Host Device must be set as the Port Type for any port that you want to act as a host controlled device on a workstation. This configuration allows users to connect through the PortMaster port to shared devices such as printers or modems. The type of device available depends on the type of Device Service selected.

In addition, the host device configuration only works if the Host Device parameter is set to the correct value. Table 6-3 shows the options for the Device Service and Host Device parameters when the Port Type is set to Host Device.

Table 6-3 Types of Device Service

Device Service	**Host Device Value**	**Function**
PortMaster	/dev/tty** where ** is the specific device identifier	PortMaster is the default device service. This type of device service is preferred because it makes the PortMaster port operate as if it was a serial port physically attached to a UNIX host such as a printer or modem. However, the PortMaster `in.pmd` daemon must be installed on the host for this device service to be used.
Rlogin	/dev/network	A host can use the UNIX `rlogin` command to establish a connection to the port. Once the rlogin session is established, the host application can read and write data directly to the serial port. If multiple ports on the PortMaster are configured to use this service, a pool of ports is created.
Telnet	/dev/network	Telnet is supported on most TCP/IP hosts. This service should be selected in mixed hardware and operating system networks. Once the telnet session is established, the host application can read and write data to the port. The default TCP port number is 23, but other ports can be entered. If multiple ports on the PortMaster are configured to use this device service at the same TCP port, a pool of ports is created.

Table 6-3 Types of Device Service *(Continued)*

Device Service	**Host Device Value**	**Function**
Netdata	/dev/network	Netdata allows a clear channel TCP or SPX connection from a network host to the PortMaster port. This device service is used with customized applications that use a socket interface and need a direct data link to a serial device. The advantage of this configuration is that no option or protocol negotiation is required to establish the session. The host application can begin reading and writing data to the PortMaster immediately. The default netdata port is 6000; however, other ports can be used. If multiple ports on the PortMaster are configured to use this device service at the same TCP or SPX port, a pool of ports is created.

Setting Override Parameters

If the Port Type parameter is set to Host Device, you can specify that the host device can override certain port parameters. The override parameters are Baud Rate, Parity, Databits, and Flow Control. These parameters can be changed by the host using an `ioctl()` system call. All overrides are turned off by default. If you want to allow a host to override a parameter, turn override for the parameter on.

Setting Two Way Port Type

If the Port Type parameter is set to Two Way, the port operates in both User Login and Host Device modes. User Login mode is used if carrier is detected on pin 8 of the RS-232 connector (DCD). Otherwise, the port can be accessed as a host device on the computer. This configuration allows network users access to PortMaster modems on an as-needed basis.

The Host Device parameter must be set according to the Device Service selected as described in Table 6-1. In this configuration, the Login Service must also be specified.

Setting a Port for Network Use

Any port where you want to allow network dial-in or dial-out access must have its Port Type set to Network. Network makes the port available for connections to and from remote sites using modems and the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP). Once you have selected the Port Type as Network, you must specify one of four Network Types as described in Table 6-4.

Table 6-4 Network Types

Type	**Description**
Hardwired	This network type allows you to establish a dedicated network connection between two sites without modem dialing or authentication. In this mode the port immediately begins running the specified protocol. If the port is set for Hardwired it cannot be used for any other purpose. Hardwired connections are discussed in more detail in "Setting a Port for a Dedicated Connection" on page 6-8.
Dial In	This network type allows the port to accept dial-in network connections only. The dial-in user is required to enter a user name and password before the connection is established. Authorized users are managed through the User Table described in Chapter 8, "Configuring Dial-In Users" or using RADIUS. PPP users wishing to authenticate with PAP or CHAP can start sending PPP packets. When the packets are received the PortMaster autodetects PPP and requests PAP or CHAP authentication. Refer to "PAP and CHAP Authentication" on page 3-15.
Dial Out	This network type allows dial out to establish connections with remote locations. Dial-out network destinations are managed through the Location Table described in Chapter 9, "Configuring Dial-Out Locations."
Dial In & Out	This network type allows the port to accept dial-in users and use dial-out locations.

Setting Dial Group

The Dial Group parameter is used to assign ports to modem pools for use by dial-out locations. A group number is assigned to each location in the Location Table. For example, you create a dial-out location called “home” and specify that the Dial Group for “home” is 2. When you configure each port, you may assign the port to a dial group. Any idle port in Dial Group 2 can be used to dial the destination “home,” other ports can not. In order for modem pools to work, each port must be assigned to a Dial Group and each destination must specify a Dial Group. Valid dial groups are numbered 0 to 99. The default dial group is 0 (zero).

Setting a Port for a Dedicated Connection

A port can be configured for a dedicated network connection by setting the Port Type parameter to Network and the Network Type to Hardwired. If the port is hardwired, it can not perform any of the other port functions described in this chapter.

When the Network Type is set to Hardwired, the port configuration window is changed to include parameters that must be set only on hardwired ports. These parameters are described in the following subsections and only apply to network hardwired ports.

Setting the Protocol

The network protocol for the hardwired port can be set for PPP packet encapsulation or SLIP encapsulation as described in Chapter 3, “How PortMasters Work.” If you want to use the Point-to-Point Protocol you have your choice of the following options:

- PPP with IP packet routing
- PPP with IPX packet routing
- PPP with both IP and IPX packet routing

You should select a protocol that is compatible with the rest of your network configuration.

Setting the Maximum Transmission Unit (MTU)

The Maximum Transmission Unit or MTU defines the largest frame or packet that can be sent through this port. If a packet exceeds the specified MTU it is automatically fragmented if IP or discarded if IPX. PPP connections can have an MTU set from 100-1500 octets. SLIP connections can have an MTU set from 100-1006 octets. The remote host can negotiate smaller MTUs if necessary.

The MTU is typically set to the maximum allowed for the protocol being used, either 1500 or 1006. However, smaller MTU values can improve performance if you are using multiline load-balancing or for enhanced interactive performance.

Setting the Destination IP Address

The IP address or host name of the machine on the other end of the hardwired connection must be entered for the IP Destination parameter.

For PPP, the IP Destination parameter can be set to Negotiated. This allows the PortMaster to learn the IP address of the system on the other end of the connection using PPP IPCP address negotiation.

Setting the Destination Netmask

The Netmask parameter defines the netmask of the system on the other end of the hardwired connection.

Setting the IPX Network Number

IPX traffic can be passed through a port if you assign an IPX network number to the hardwired network connection. The IPX Network parameter is the IPX network for the connection and must be a unique IPX network number not used anywhere else on your network.

IPX routing differs from IP in that the serial link itself must have a network, as shown in Figure 6-2. In IP routing, the serial link can have a network or be unnumbered, which is more common. In this case, the device at each end of the link uses its Ethernet IP address for its end of the serial link.

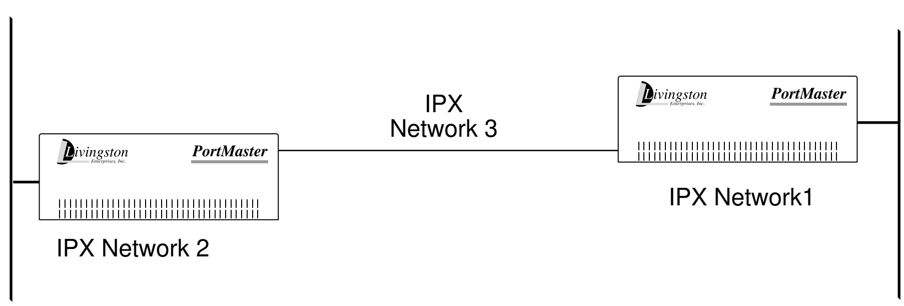

Figure 6-2 IPX Network Address Requirements

Enabling Routing

As described in Chapter 2, "Networking Concepts," PortMaster products automatically send and accept route information as part of RIP messages if routing is turned on. If you select Broadcast for the Routing parameter, routing packets are sent to the system at the other end of the hardwired connection. When Listen is selected, the PortMaster accepts routing packets from the device connected to the hardwired port. Both options can be selected at the same time to enable the sending and acceptance of routing information. If neither option is selected, RIP is turned off and the PortMaster ignores all route messages received on the interface.

Setting TCP Header Compression

Compression of TCP/IP headers can increase the performance of interactive TCP sessions over asynchronous lines. Livingston implements Van Jacobson TCP/IP header compression.

Compression should not be used with multi-line load-balancing, but may be used with multi-link PPP.

Compression must be enabled on both ends of the connection if you are using SLIP. With SLIP, TCP packets are not passed if only one side of the connection has compression enabled. For PPP connections, the PortMaster supports both bidirectional and unidirectional compression. Refer to RFC 1144 for more information about header compression.

Setting the PPP Async Map

The PPP protocol supports the escaping of nonprinting ASCII characters found in the datastream. Escaping means that specified characters are not sent through the connection but are instead replaced by a special set of characters. These special characters are interpreted by the remote system as the original character. The PPP Async Map is a bitmap of characters that should be escaped. The default PPP Async Map is 00000000. If the remote host requires a PPP async map, the PortMaster accepts the request for the map.

Setting Input and Output Filters

Input and output packet filters can be attached to a network hardwired port. Filters allow you to monitor and restrict network traffic. If an input filter is attached, all packets received from the interface are evaluated against the rule set for the attached filter. Only packets permitted by the filter are passed through the PortMaster. If an output filter is attached, packets going to the interface are evaluated against the rule set in the filter and only packets permitted by the filter are sent to the interface. For more information about filters, see Chapter 10, "Configuring Filters."

Setting General Port Parameters

The general port parameters are set for every asynchronous port regardless of the port type and configuration you have selected.

Displaying Extended Port Information

The PortMaster can display port information in brief or extended modes. The extended mode provides more information than the brief mode. To display all of the information available, set the Extended parameter on. In some versions of PMconsole the Extended parameter is on all the time.

Setting the Login Prompt

You can customize the login prompt displayed to users on a per port basis. Any valid ASCII characters can be used. If the string "$hostname" is included in the login prompt, the host name set for this port is substituted for the string. "$hostname login:" is the default Login Prompt. Double quotes and control characters may not be used inside the login prompt.

Setting the Login Message

The PortMaster allows you to specify a message for each port, up to 240 characters long, that is displayed to the user prior to login. To insert a new line use a caret (^). Do not include double quotes within the message.

Setting an Optional Access Filter

An access filter can provide additional login security. To enable access security, the Access Filter parameter must be defined as described in Chapter 10, "Configuring Filters." Access filters work as follows:

- The user specifies a host
- The host address is compared against the access filter
- If the address is permitted by the filter, the connection is established

- If the address is not permitted, the connection is denied unless Access Override is enabled

The Access Override parameter is used as follows if access is denied:

- Access is denied by the access filter
- The user is prompted for a username and password
- The user is verified by the User Table or RADIUS
- The access filter defined for this user is used to determine if the user has permission to access the specified host

Setting Port Security

Port Security requires that each username be found in the User Table or in the RADIUS database. If Port Security is enabled, each user that logs in must have their username verified before they are allowed to connect to the specified host.

If Security is turned off, any user not found in the User Table is passed through to the host for authentication. If you are using RADIUS authentication, Security must be on.

Allowing Users to Connect Directly to a Host

The Autolog parameter allows users to be connected with the specified host without seeing the login prompt. The Autolog parameter is automatically substituted for the login prompt response and the host session is started.

Setting a Port as the Console

The console parameter allows you to set any asynchronous port to be the console for administrative functions. If you use the `save console` command, the port remains the console even after the current session is ended.

Setting the Port Idle Time

The Idle Timeout parameter specifies how long the PortMaster should wait with no input or output activity before it resets the port. Versions of the ComOS prior to and including version 3.0.3 only monitor input activity.

This parameter is defined in minutes and can be set from 0 to 240 minutes. To disable the idle timer, set the Idle Timeout parameter to 0. If the idle time is set to 1, the login, password, and host prompts time out in 5 minutes but users already logged in are not affected. If the idle time is set to 2 or higher, the login password and host prompts time out in 5 minutes. Once the user is logged in, the timeout value is used to determine the idle time allowed. RIP, SAP, and keepalive packets are not considered traffic for the purpose of the idle timer.

Configuring Modems and Modem Parameters

Modems are connected to PortMasters using an RS-232 cable. The PortMaster is a DTE device, so a straight through cable is used to connect modems. The RS-232 input and output signals and pins are shown in Table 6-5. Straight-through cables used with modems use pins 2, 3, 4, 5, 6, 7, 8, and 20.

A null-modem cable is used to connect a terminal (DTE) to a console port. A null-modem cable crosses pins 2 and 3, and 4 and 5, pin 7 is straight-through, and pins 6 and 8 are connected to pin 20.

Table 6-5 Modem Cable Pinout

Pin Number	**Description**	**Direction**
2	Transmit Data (TXD)	Output
3	Receive Data (RCD)	Input
4	Request to Send (RTS)	Output
5	Clear to Send (CTS)	Input
6	Data Set Ready (DSR)	Input
7	Signal Ground	
8	Data Carrier Detect (DCD)	Input
20	Data Terminal Ready (DTR)	Output

Note – If you do not use hardware flow control (RTS/CTS) you do not need pins 4 and 5. If you do not use modem control, you do not need pins 6, 8, and 20. Both RTS/CTS and modem control are strongly recommended for PPP and SLIP use.

Dial-up modems that operate over normal telephone lines at speeds of 28,800 bits per second or higher are now available. These modems do not operate at a guaranteed throughput, but rather at a speed dependent on the quality of the line, the effectiveness of data compression, and other variables. These modems use hardware flow control to stop the data from the host by raising and lowering the CTS signal.

PortMasters support hardware flow control using the RTS output signal and the CTS input signal, which is also used by the normal modem handshake.

Modems should be configured to do the following:

- Raise DCD when a call comes in
- Reset itself when DTR is dropped
- Lock the DTE speed
- Use hardware flow control (RTS/CTS)

Automatic Modem Configuration

PortMasters contain a user configurable modem table that describes most common modems, their preferred speed, and initialization string. The modem table is used to automate the modem configuration process. Once you specify the name of the modem and the attached port, the PortMaster automatically configures the modem for you provided the modem is in the factory default state when it is initialized.

For ports that have never been configured, the PortMaster automatically sets the port for hardware flow control, the correct speed, and modem control when the port is reset after a modem type is specified.

Example modem table entries are shown in Table 6-6.

To view your modem table, type:

```
Command> show table modem
```

Table 6-6 Example Modem Table Entries

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
acura-v32	Hayes Acura V.32bis	38400	AT&F&C1&D3&K3&Q5E0Q1S0=1&W
hayes	Hayes Compatible	38400	AT&F&C1&D3&k3&Q5X0E0S0=1&W

Table 6-6 Example Modem Table Entries *(Continued)*

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
p-optima-v32	Hayes Optima V.32bis PCMCIA	115200	AT&F&C1&D3S0=1&W&W1
p-optima-v34	Hayes Optima V.34 PCMCIA	115200	AT&F&C1&D3&K3&Q5E0Q1S0=1&W
intel144e	Intel 144e V.32bis	38400	AT&FE0Q1&C1S21=56\X1S0=1S7=30S11=50&W
p-intel-v32	Intel V.32bis PCMCIA	115200	AT&F&D3S0=1&W&W1
mt1432ba	MultiTech MT1432BA	38400	AT&F&D3&W0
mt224	MultiTech MT224	38400	AT&F$SB38400$R1E0Q1V1&W0
p-multi-v34	MultiTech MT2834LT V.34 PCMCIA	115200	AT&F&E1&E4&C1&D3&R1$SB115200S0=1&W
p-ppi-v34	PPI ProClass V.34 PCMCIA	115200	AT&F&C1&D3&K3S0=1&W&W1
ppi-v32	Practical Peripherals SX/SA V.32bis	38400	AT&FE0S0=1Q1&C1&D2&W
p-premax-v32	Premax V.32bis PCMCIA	115200	AT&F&D3S0=1&W&W1
usr-v32	USR Courier/ Sportster V.32bis	57600	AT&F1S0=1&W
p-usr-v32	USR Courier/ Sportster V.32bis PCMCIA	57600	AT&F1S0=1&W
usr-v34	USR Courier/ Sportster V.34	115200	AT&F1S0=1&W
p-usr-v34	USR Courier/ Sportster V.34 PCMCIA	115200	AT&F1S0=1&W

Modems can be added to the modem table by typing:

```
Command> add modem name_short "name_long" speed "init_string"
```

For example, to add a USRobotics modem to the modem table, type:

```
Command> add modem usr-v34 "USRobotics V.34" 115200 "AT&F1S0=1&W\r^OK"
```

To automatically configure and attach a modem to a port, type:

```
Command> set port# modem name_short
Modem type for port# changed from modem_name to name_short
Command> reset port#
```

This command configures the modem attached to the port specified. For example:

```
Command> set s1 modem usr-v34
Modem type for s1 changed from to usr-v34
Command> reset s1
```

To configure all of the ports for the same modem type, use `all` instead of *port#* in the previous example. After the modem is attached to the port, set the other modem configuration parameters described in “Configuring Modem Parameters” on page 6-16.

To configure the modem *not* to answer when users dial-in, set `S0=0` in the initialization string.. To avoid writing the initialization to the NVRAM in the modem each time the port is reset, leave off the `&W` at the end of the initialization string.

Configuring Modem Parameters

The modem parameters described in this subsection are set for each port and should match the configuration on the attached modem.

Setting the Port Speed

The speed of a port is defined as the baud rate. The PortMaster allows you to specify three different baud rates for each port and one baud rate for host device ports. Port speeds are sequentially matched from the first baud rate through the third baud rate.

For example, when a connection with this port is established, the PortMaster uses the first baud rate value to try to synchronize the connection speed. If no synchronization is possible the PortMaster tries to synchronize speeds using the second baud rate value. If this fails, the third baud rate value is used. Each of the speeds can be set from 300 bps to 115200 bps. The default speed is 9600 bps.

Modern modems and terminals should always be set to run at a fixed rate. To define a fixed rate, lock the DTE rate by setting all three baud rate fields to the same value.

Setting Modem Control

The Modem Control parameter should be set on if you want to make use of the DCD signal for modem connections. When Modem Control is on, the PortMaster uses the condition of the carrier detect line to determine whether or not the line is in use. Modem control must be on for PortMaster outbound traffic. If modem control is off the PortMaster assumes the carrier detect line is always high. As a result, the PortMaster cannot attach to the modem for outbound traffic because it sees the line as busy.

Setting Parity

The Parity parameter must be set to match the parity on the attached device. The parity default value is none and must be used for ports configured for network dial in or dial out operation. Table 6-7 describes each of the parity options.

Table 6-7 Parity Parameter Options

Option	Description
None	Assumes 8 databits, 1 stop bit, and no parity bit.
Even	Assumes 7 databits, 1 stop bit, and even parity.
Odd	Assumes 7 databits, 1 stop bit, and odd parity.
Strip	Assumes 8 databits, 1 stop bit and the parity bit is stripped from the datastream when it is received by the PortMaster.

Setting the Flow Control

The PortMaster supports either software flow control or hardware flow control. Software flow control uses the ASCII control characters DC1 and DC3 to communicate with the attached device and start and stop the flow of data. Software flow control is set by selecting the Xon/Xoff option for the Flow Control parameter.

Hardware flow control allows the PortMaster to receive data from the attached device by raising the Request to Send (RTS) signal on pin 4 of the RS-232 connector. The PortMaster only sends information to the attached device when the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised. Hardware flow control is set by selecting the RTS/CTS option for the Flow Control parameter.

Note – Always use hardware flow control if it is available. Do not use both hardware and software flow control on the same port.

Hanging Up a Line

The Line Hangup parameter specifies whether or not the DTR signal should be dropped and the modem hung up after a session is terminated. If Line Hangup is enabled and the session is terminated, DTR is held low signalling the modem to disconnect. If Line Hangup is disabled, the DTR signal does not drop and the user session terminates.

Note – Resetting the port administratively always drops DTR.

DTR Idle

The DTR Idle parameter is used when you want to connect a PortMaster to a BBS or other host allowing bidirectional communications. This parameter changes the behavior of the port to better accommodate connecting the PortMaster to BBS systems or other legacy hosts that do not support TCP/IP but do have serial ports.

This type of connection requires that you connect a null modem cable to the PortMaster port and to your host. For more information about null modem cables, refer to your *Hardware Installation Guide*.

Note – The PortMaster ignores DSR. Some PCs may require DSR high, but do not tie DSR to DTR.

The DTR Idle parameter can only be set using the command line interface. Use the following commands to configure this feature on port S1.

```
Command> set telnet 24
Command> set s1 dtr_idle off
Command> set s1 modem on
Command> set s1 twoway /dev/network
Command> set s1 service_device telnet
Command> reset s1
Command> save all
```

The first command changes your telnet administration port. This is not necessary if you set the S1 port service_device telnet to some port other than 23. Table 6-8 describes the port transitions resulting from this configuration.

Table 6-8 DTR_Idle Transitions

Transitions	**Explanation**
No DTR from BBS	• S1 IDLE • PortMaster refuses telnet
DTR asserted by BBS	• S1 IDLE • DTR from PortMaster is deasserted • PortMaster accepts telnet for S1 at TCP port 23
Telnet session begins	• S1 changes to ESTABLISHED • DTR from PortMaster is asserted
User drops telnet session from the network side	• S1 changes to IDLE • PortMaster resets the port, dropping DTR • BBS loses Carrier Detect, terminates user (BBS can now either drop DTR or not)
BBS drops the user by deasserting DTR for 100 msec or longer	• S1 changes to IDLE • Telnet session is closed by the PortMaster

Configuring a Synchronous WAN Port 7

This chapter describes the steps required to configure a PortMaster synchronous Wide Area Network (WAN) port. These steps are not dependent on which user interface you are using to configure your system. The *Administrator's Guide* for your user interface describes how to set each option. The purpose of this chapter is to review each of the port parameters and its options.

All of the possible port parameters are described in this chapter; however, you only need to set the parameters required for the configuration you want. Specific synchronous port configurations are described in Chapters 15 through 18.

This chapter includes the following topics:

- Introduction to WAN port configuration options
- Description of leased line connections
- Description of Frame Relay connections
- Description of ISDN and switched 56Kbps line connections
- Setting general port parameters

Introduction to WAN Port Configurations

Synchronous WAN ports are usually used for high-speed dedicated connections between two remote local area networks (LAN). Once a connection is established between two remote sites, a wide area network (WAN) is achieved. Synchronous WAN connections can be achieved using dedicated leased lines, Frame Relay connections, switched 56K lines, or ISDN lines. Connections can be achieved from 9600 bps to 2.048 Mbps (E1). PortMasters support any of these connection types using one or more synchronous ports.

All of the WAN port connections are similar and are represented in Figure 7-1. For most applications a dedicated line connects two PortMaster routers, each located on a separate remote network.

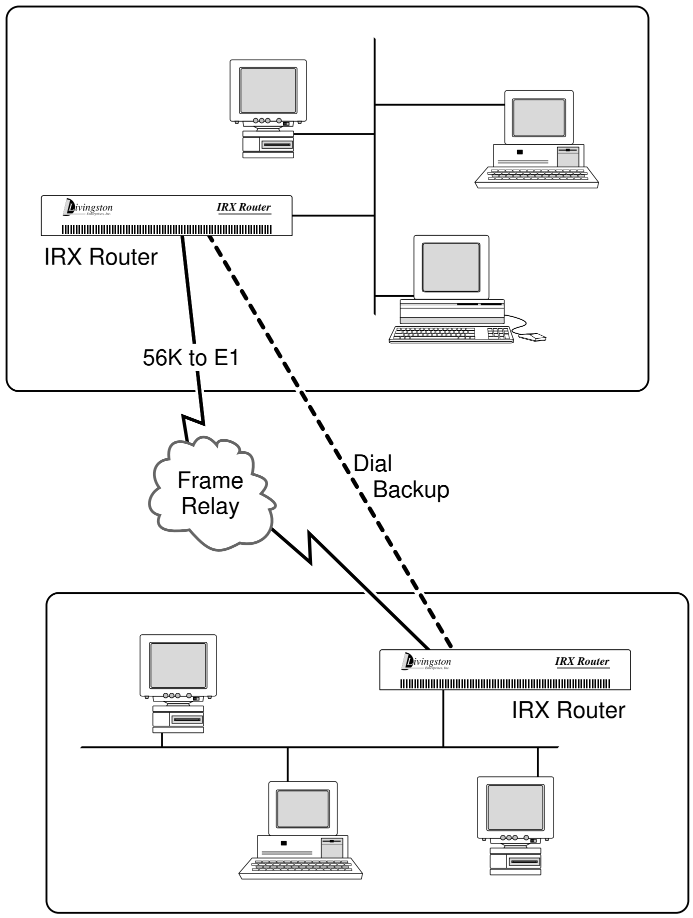

Figure 7-1 Synchronous WAN Connection

Once you have determined the type of synchronous connection to use between your remote locations, the synchronous port on each end of the connection must be configured. An example of the synchronous port configuration window from PMconsole for X Windows is shown in Figure 7-2. The actual window you see depends on the version of PMconsole used. You can also configure the port using the command line interface.

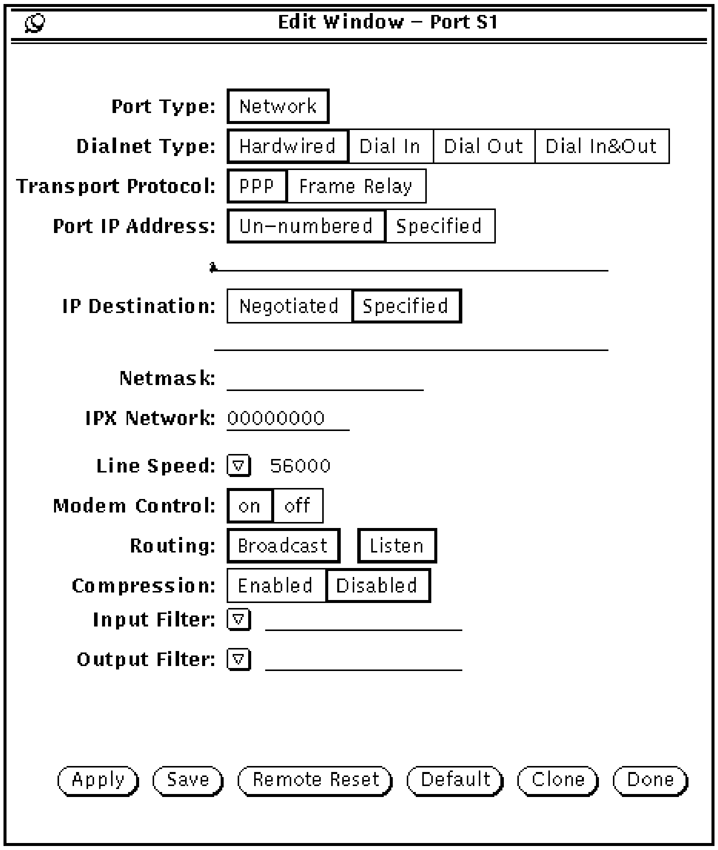

Figure 7-2 Synchronous Port Window S1—X Windows GUI

All of the available parameters are described in this chapter.

Leased Line Connections

Leased line connections use leased or dedicated lines to establish a permanent connection between two routers. Once the connection is established it remains available on a continuous basis whether there is network traffic between the two locations or not. Leased lines provide dedicated high-speed connections but often run at only 5 to 20% of their capacity during non-peak hours. Leased line connections require a Digital Service Unit/Channel Service Unit (DSU/CSU) connected between the router and the dedicated line. The DSU/CSU takes digital data in the format used by the router and translates it into the digital format used by the leased line.

PortMaster synchronous ports support leased-line connections from 9600 bps to T1 (1.544Mbps) or E1 (2.048Mbps) speeds. Synchronous ports used for leased line connections are configured for PPP operation and can have input and output filters for network security.

For more information about configuring the PortMaster for leased line connections, refer to Chapter 15, "Synchronous Leased Line Connections."

Frame Relay Connections

Frame Relay can provide low-cost high-speed WAN connectivity. Frame Relay is a packet-based interface standard for the transport of protocol-oriented data. Frame Relay uses the traditional silence between transmissions by encapsulating protocol-oriented data in discrete units of information (generic packets) and transmitting them across statistically multiplexed paths as bandwidth becomes available, thereby effectively transmitting more data over a given bandwidth.

The statistically multiplexed paths are called virtual circuits. Frame Relay does not allocate bandwidth to a given path until actual data needs to be transmitted. As a result, the bandwidth within the network is dynamically allocated on a packet-by-packet basis. During peak load periods, Frame Relay devices can buffer or store the data for later transmission.

Frame Relay also reduces much of the protocol processing currently performed by networks thereby reducing much of the transmission latency attributed to protocol processing. Instead, the endpoint devices, PC's and workstations, take on the responsibility for guaranteeing the error-free end-to-end transfer of frames. The protocol processing is now left to higher layers inherent in the transported data. Frame Relay allows the communication bandwidth to be shared among multiple users creating bandwidth allocation on demand. In a properly configured Frame Relay environment, the incidence of errors or lost packets is extremely low even though the assurance of reliable communication is left to higher layer protocols.

Each frame contains header information that is used to determine the routing of the data to the specified destination, as well as a Data Link Channel Identifier (DLCI), which defines the conversation that owns the frame. As a result, each endpoint can communicate with multiple destinations via a single access link to the network. Frame Relay traffic receives full bandwidth for short transaction bursts, instead of fixed amounts of dedicated bandwidth. In other words, a single Frame Relay interface can contain many individual conversations, each with its own DLCI, and each using as much bandwidth as is available at a given time.

Before ordering your Frame Relay circuit or network from your telecommunications provider, there are several terms that should be clearly understood because the way that Frame Relay does statistical multiplexing can be confusing. Many Frame Relay terms are defined briefly in the glossary. A more detailed description can be found in "Frame Relay Terms" on page 16-1.

A virtual circuit is defined by the DLCI and can be either permanent (PVC) or switched (SVC), established by a user who specifies the destination. PVCs and SVCs are defined by their endpoints. The actual path between the two endpoints may vary from time to time and is determined by the network administrator or service provider. The Frame Relay implementation on PortMasters support PVCs but not SVCs.

Special management frames with unique DLCIs are passed between the network and the Frame Relay devices. These frames are used to monitor the link status and pass information about the status of PVCs and DLCIs. These frames are defined as the Local Management Interface (LMI) and are used to provide information about the permanent virtual circuits.

PortMasters support Frame Relay on synchronous lines as described in RFC 1490. If you are configuring your system for Frame Relay, additional information about DLCIs and LMI must be provided at configuration time. The Frame Relay specific parameters are described in "Frame Relay Parameters" on page 7-11 and in Chapter 16, "Synchronous Frame Relay Connections."

You can find more information about Frame Relay by accessing the Frame Relay Forum home page on the world-wide web at `http://frame-relay.indiana.edu/`.

Switched 56K and V.25bis Dialing Connections

PortMasters support dial on-demand switched 56K connections using synchronous ports and the PPP protocol. Switched 56K connections require an external CSU/DSU and can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the Location Table for dial-out connections and a dial-in user must be specified in the User Table for dial-in connections.

PAP or CHAP is available for dial-in authentication when a router dials into your PortMaster. CHAP is available for dial-out authentication.

ISDN Connections

PortMasters support Integrated Services Digital Network (ISDN) connections on synchronous ports. Like leased lines, ISDN lines are provided by the local telephone company and can provide speeds of 64Kbps on each B-channel, which can be three times faster than a traditional connection using a modem and an ordinary telephone line.

ISDN lines can be configured for Basic Rate Interface (BRI), which provides two B-channels used for voice or data and one D-channel used for signaling. ISDN lines can also be configured for Primary Rate Interface (PRI), which provides 23 B-channels and one D-channel.

ISDN is most commonly used to provide low-cost connectivity between sites that cannot justify the cost of a dedicated high-speed leased line. However, ISDN connections provide more bandwidth than asynchronous dial-up connections can, as well as quicker call completion (approximately 1 second instead of 45 seconds).

PortMasters require an external terminal adapter (TA) to connect from the PortMaster synchronous port to the ISDN link. For TAs that do not have auto-dial or for administrators who want to manually connect with the TA, PortMasters support V.25bis dialing. The dial script is configured as a destination in the Location Table described in Chapter 9, "Configuring Dial-Out Locations." For more information about configuring the PortMaster for ISDN with an external terminal adapter and V.25bis dialing, refer to Chapter 17, "Synchronous V.25bis Dial-Up Connections."

PortMasters are also available with a built-in BRI port with integrated NT1, providing a U interface for ISDN connectivity. The BRI ports do not require an external terminal adapter. For more information about configuring the PortMaster for ISDN connections, refer to Chapter 18, "ISDN Connections." The U interface works in the USA and other countries that follow US telephone standards.

Setting WAN Port Parameters

The WAN port parameters described in this section are set for every synchronous port regardless of the connection type and configuration you have selected. However, the Network Type parameter determines which other parameters should be set.

Displaying Extended Port Information

The PortMaster can display port information in brief or extended modes. The extended mode provides more information than the brief mode. To display all of the information available, set the Extended parameter on. Some version of PMconsole always use the Extended display mode.

Port Type

The Port Type parameter is always set to Network for synchronous ports.

Setting the Network Type

You must specify one of four Network Types as described in Table 7-1.

Table 7-1 Network Types

Type	Description
Hardwired	This network type allows you to establish a dedicated network connection between two sites without modem dialing or authentication. In this mode the port immediately begins running the specified protocol. If the port is set for Hardwired it cannot be used for any other purpose. A hardwired connection must be used for a leased line or Frame Relay connection.
Dial In	This network type allows the port to accept dial-in network connections, for use with switched 56K or ISDN connections. The dial-in user is required to enter a user name and password before the connection is established. Authorized users are managed through the User Table described in Chapter 8, "Configuring Dial-In Users" or using RADIUS. PPP users wishing to authenticate with PAP or CHAP can start sending PPP packets. When the packets are received the PortMaster autodetects PPP and requests PAP or CHAP authentication. Refer to "PAP and CHAP Authentication" on page 3-15.

Table 7-1 Network Types *(Continued)*

Type	Description
Dial Out	This network type allows dial out to establish connections with remote locations. Dial-out network destinations are managed through the Location Table described in Chapter 9, "Configuring Dial-Out Locations." This network type can be used for ISDN and switched 56K connections.
Dial In & Out (TwoWay)	This network type allows the port to accept dial-in users and use dial-out locations. This network type can be used for ISDN and switched 56K connections.

Setting the Transport Protocol

The transport protocol for synchronous connections can be set to PPP for leased line, switched 56K, and ISDN connections, or to Frame Relay for a Frame Relay connection. If Frame Relay is selected, additional Frame Relay specific parameters are displayed. The Frame Relay specific parameters are described in "Frame Relay Parameters" on page 7-11.

Setting the Port IP Address

The Port IP Address parameter can be set to Unnumbered or Specified. If Specified is selected, an IP address for the port must be entered. The Unnumbered option is used if you have selected the PPP protocol for leased line or ISDN connections. This option prevents the assignment of an IP address directly to the port; instead the Ethernet address of the router is assigned to the port. Fewer networks or subnets are needed as a result.

The Specified option must be used if you are using Frame Relay on this port and is optional for leased lines. Be sure to enter the IP address of the synchronous port when this option is used.

Setting the Destination IP Address

The destination IP address or host name of the machine on the other end of the connection is used for leased line connections only. The IP Destination parameter can also be set to Negotiated. This allows the PortMaster to learn the IP address of the system on the other end of the connection using PPP IPCP address negotiation.

Do not set a destination IP address for Frame Relay connections. Instead, use the DLCI list to link IP addresses to DLCIs or use LMI or Annex-D and inverse ARP to discover Frame Relay addresses dynamically. For network dial-in or dial-out connections, do not set a destination IP address for the port. Instead, the destination address is set in the User Table or RADIUS for dial-in, or in the Location Table for dial-out.

Setting the Netmask

Netmasks are used to divide networks into subnets as described in Chapter 2, "Networking Concepts." The default netmask is 255.255.255.0. If you use a different netmask on your network, enter the subnet mask that describes how your network addresses are divided between the network portion and the host portion. This parameter is set for leased line or Frame Relay connections.

Setting the IPX Network Number

The IPX Network or IPXNet parameter is the IPX network of the serial link. The IPX network of the interface is entered in HEX format, described in Chapter 2, "Networking Concepts." This parameter is set only for leased line connections.

Setting the Port Speed

Although you can select a speed between 9600 and E1, the actual line speed is set by the external clock on the device to which the PortMaster is connected or by the carrier. The line speed can be set for reference, but the value is a comment only.

Setting Modem Control

The Modem Control parameter defaults to off for synchronous connections. With modem control set off, the PortMaster assumes the carrier detect line is always high.

This parameter should be set on only if you want to make use of the DCD signal from the attached device. When Modem Control is on, the PortMaster uses the condition of the carrier detect line to determine whether or not the line is in use.

Modem control is usually off for leased line or Frame Relay connections but can be turned on if the CSU/DSU is configured accordingly. This parameter is usually on for network dial-in or dial-out configurations.

Enabling Routing

As described in Chapter 2, "Networking Concepts," PortMaster products automatically send and accept route information as part of RIP messages if routing is turned on. If you select Broadcast for the Routing parameter, routing packets are sent to the system at the other end of the WAN connection. When Listen is selected, the PortMaster accepts routing packets from the WAN port. Both options can be selected at the same time to enable the sending and acceptance of RIP information. If neither option is selected, RIP is turned off and the PortMaster ignores all route messages received on the interface.

The Routing parameter is only set on the port for network hardwired connections such as leased line or Frame Relay. Routing is set in the User Table for dial-in connections and in the Location Table for dial-out connections.

Setting TCP Header Compression

Van Jacobson TCP/IP header compression improves performance on asynchronous line but degrades performance on high-speed synchronous lines. Therefore, compression should be turned off on synchronous ports.

Setting Input and Output Filters

Input and output packet filters can be attached to a synchronous port for leased lines or Frame Relay. Filters allow you to monitor and restrict network traffic. If an input filter is attached, all packets received from the interface are evaluated against the rule set for the attached filter. Only packets permitted by the filter are passed through the PortMaster. If an output filter is attached, packets going to the interface are evaluated against the rule set in the filter and only packets permitted by the filter are sent out of the interface. For more information about filters, see Chapter 10, "Configuring Filters."

Set filters in the User Table or RADIUS for dial-in connections and in the Location Table for dial-out connections.

Setting Dial Group

The Dial Group parameter is used to assign synchronous ports to modem pools for use by V.25bis dial-out locations. A group number is assigned to each location in the Location Table. For example, you create a dial-out location called "home" and specify that the Dial Group for "home" is 2. When you configure each V.25bis synchronous port, you may assign the port to a dial group. Any idle port in Dial Group 2 can be used to dial the destination "home," other ports can not. In order for modem pools to work, each port must be assigned to a Dial Group and each destination must specify a Dial Group. Valid dial groups are numbered 0 to 99. The default dial group is 0 (zero).

Frame Relay Parameters

The following WAN port parameters apply only to Frame Relay interfaces.

Automatically Learning the DLCI List

The LMI parameter specifies whether or not the PortMaster accepts Local Management Interface (LMI) frames from the attached Frame Relay switch. If LMI is enabled on the switch, the PortMaster LMI parameter should be enabled. The default keepalive value of 10 seconds is inserted automatically. Enabling LMI causes the DLCI list to be completed automatically. The LMI parameter on the PortMaster can be enabled by setting the LMI keepalive timer. If the switch uses a different keepalive timer interval than the default, be sure the keepalive timer on the PortMaster matches that of the attached Frame Relay switch.

The PortMaster also accepts Annex-D keepalives. Currently, Annex-D keepalives can be configured using the command line interface only, not PMconsole. Contact your Frame Relay carrier to determine which keepalive they are using, LMI or Annex-D; both may be referred to as LMI.

Listing DLCI's for Frame Relay Access

If LMI or Annex-D is not used, you must enter the DLCI list manually. The DLCI list is a list of DLCIs that are accessible through the Frame Relay network by this interface. The PortMaster uses inverse ARP to learn the IP addresses of routers attached to the permanent virtual circuits represented by the specified DLCIs, if those routers support inverse ARP.

The DLCI list can be provided by your Frame Relay carrier, or if LMI is enabled the list is learned dynamically. For dynamically learned lists, 32 PVCs are allowed. Only 16 PVCs can be specified if the DLCI and IP address are entered. If you specify only DLCIs, you can list 24. When the PVC and IP address are specified, the PortMaster statistically configures these entries into its ARP table.

For information on Frame Relay subinterfaces see "Frame Relay Subinterface" on page 16-10.

Configuring Dial-In Users 8

This chapter describes how to configure PortMaster users. These steps are not dependent on which user interface you are using to configure your system. The *Administrator's Guide* for your user interface describes how to set each option. The purpose of this chapter is to review each of the user parameters that must be set and the options for each.

All of the possible user parameters are described in this chapter; however, you only need to configure the parameters required for your application. Specific configurations are described in Chapters 11 through 18.

This chapter includes the following topics:

- A description of the different types of users
- How to configure network users
- How to configure login users
- How to configure dialback users

Note – If you have many users or many PortMasters, you should use RADIUS for user authentication rather than the User Table. Refer to the *RADIUS Administrator's Guide* for information about configuring RADIUS.

Description of Users

User parameters define the nature and behavior of dial-in users. The User Table contains entries for each defined dial-in user along with the characteristics for the user.

PortMaster products allow you to configure four different types of users:

- Network User—Normal
- Network User—Dialback
- Login User—Normal
- Login User—Dialback

The User Table provides login security for users to establish login sessions or network dial-in connections. If you want to allow a network dial-in connection from another router, the router must have an entry in the User Table.

Description of Network Users

Network users are defined as users who dial into an asynchronous serial, synchronous serial, or ISDN port on the PortMaster and send network packets using PPP (or SLIP on asynchronous ports). This type of connection can be used for dial-in users or other routers who need to access and transfer data from the network. This type of user is defined when network packets must be sent through the connection.

Description of Login Users

Login users are defined as users who connect to an asynchronous serial or ISDN port on the PortMaster and establish a connection to a host. A login user can only send and receive characters through the connection. This type of connection is useful for users who need to access an account on a host running TCP/IP.

Description of Normal and Dialback Users

For each of the user types described above, you can choose whether the connection should be established immediately when the user logs into the PortMaster (Normal) or if the PortMaster closes the connection and dials the user back to establish a connection (Dialback). Dialback is used for enhanced network security or to simplify telephone charging.

When a normal user logs in, a connection with the network is established immediately. If the user is a network user, a PPP or SLIP session is started. If the user is a login user, a connection is established to the specified host.

When a dialback login user logs in, the user is disconnected and the PortMaster dials back the user using a predefined telephone number, then establishes a session to the specified host.

When a dialback network user logs in, the user is disconnected and the PortMaster dials out to the location specified for that user and establishes a PPP or SLIP session. The PortMaster always dials back using the same port on which the user dialed in. For more information about configuring locations, refer to Chapter 9, "Configuring Dial-Out Locations."

Configuring Users

All users are configured using the User Table unless you are using RADIUS. The User Table maintains the characteristics of login users and inbound network connections. This table can be accessed through the Table menu in the PMconsole graphical user interface. An example of the User Table window is shown in Figure 8-1. The window that you see depends on the version of PMconsole you are using.

If you are using RADIUS, refer to the *RADIUS Administrator's Guide* for more information about configuring dial-in users.

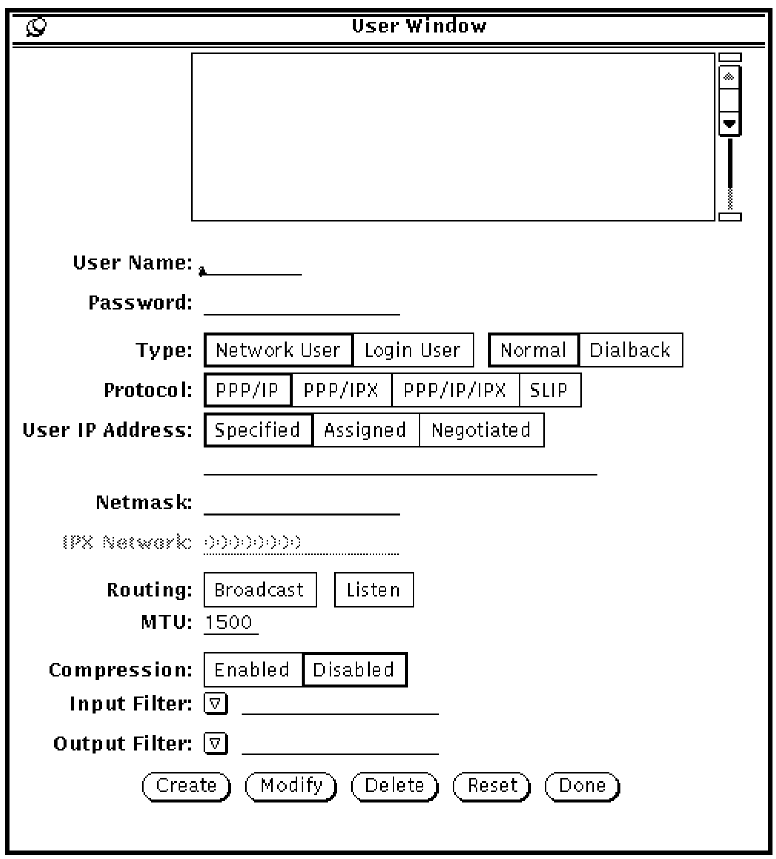

Figure 8-1 User Table Window—X Windows GUI

The parameters to be configured differ for network and login users. All of the parameters are described in the following sections.

For network dial-in connections from other routers, each remote router must be defined as a user on the PortMaster.

Configuring Network Users

Network users are allowed to establish PPP or SLIP connections to the network. These connections require a certain amount of configuration that is different from login users. This section describes each of the parameters that must be entered to configure network users.

Once you have selected the network user, select Normal or Dialback.

Configuring Normal Network Users

Normal network users establish PPP or SLIP connections with the network as soon as they have been authenticated.

Creating a New User

A new user is created when you enter a user name and password. The user name is a string of up to 8 printable non-space ASCII characters. (RADIUS supports user names up to 63 characters long.) The password for the user is a string of up to 16 printable ASCII characters, for both the User Table and RADIUS.

Setting the Protocol

The network protocol for the network user can be set for PPP packet encapsulation or SLIP encapsulation as described in Chapter 3, “How PortMasters Work.” If you want to use the Point-to-Point Protocol you have your choice of the following options:

- PPP with IP packet routing
- PPP with IPX packet routing
- PPP with both IP and IPX packet routing

You should select a protocol that is compatible with the rest of your network configuration and the user’s capabilities.

Setting the User IP Address

The User IP address parameter defines the IP address or host name of the remote host or router. Table 8-1 describes three different ways that the user IP address can be determined.

Table 8-1 User IP Address Options

IP Address Type	Description
Specified	This option allows you to define a specific IP address for the remote computer or router. This method for assigning an IP address to a user is most commonly used for routers that establish a connection with the PortMaster.
Assigned	This option allows the PortMaster to assign a temporary IP address that is used for the current session only. The address used comes from a pool of addresses set up during global configuration. This method for assigning IP addresses to users is most commonly used when there are a large number of users who are authorized to dial in.
Negotiated	This option is only used for PPP sessions. Here, the PortMaster learns the IP address of the remote host using IPCP negotiation.

Setting the Netmask

The Netmask parameter defines the netmask of the user's system on the remote end of the connection.

Setting the IPX Network Number

You must assign a unique IPX number to the network connection between the remote user device and the PortMaster, if you are using the IPX protocol for this user.

Enabling Routing

Users can have routing associated with them. This is used for connections such as dial on-demand routing where the remote router dials in to the local PortMaster.

PortMaster products automatically send and accept route information as part of RIP messages if routing is turned on. If routing Broadcast is on, RIP packets are sent to the host on the other end of the connection. When Listen is selected, the PortMaster accepts routing packets from the host or router. Both options can be selected at the same time to enable the sending and acceptance of routing information. If neither option is selected, RIP is disabled and the PortMaster ignores all routing packets received on the interface.

Setting the MTU

The Maximum Transmission Unit or MTU defines the largest frame or packet that can be sent on this connection. If an IP packet exceeds the specified MTU it is fragmented. An IPX packet that exceeds the specified MTU is dropped. PPP connections can have an MTU set from 100-1500 octets. SLIP connections can have an MTU set from 100-1006 octets. PPP can negotiate smaller MTUs when requested by the calling party.

The MTU is typically set to the maximum allowed for the protocol being used, either 1500 or 1006. However, smaller MTU values can improve performance for interactive sessions. If you are using IPX, the MTU should be set to at least 600.

Setting TCP Header Compression

Compression of TCP/IP headers can increase the performance of interactive TCP sessions if it is supported by devices on both ends of the connection. Livingston implements Van Jacobson TCP/IP header compression on asynchronous ports.

Compression should not be used with multi-line load-balancing, but may be used with multi-link PPP.

Compression must be enabled or disabled the same way on both ends of the connection if you are using SLIP. For PPP connections, the PortMaster supports both bidirectional and unidirectional compression. Refer to RFC 1144 for more information about header compression.

Setting Filters

Input and output packet filters can be attached to each network user. If an input filter is attached to a user, when the user dials in and establishes a connection, all packets received from the interface are evaluated against the rule set for the attached filter and only packets allowed by the filter are passed on. If an output filter is attached to a user, only packets allowed by the filter are sent out on the interface. For more information about filters, see Chapter 10, "Configuring Filters."

Configuring Dialback Network Users

When the network user type Dialback is selected, the Location parameter must be set. The Location parameter identifies the name of a dialback location defined in the Location Table. The PortMaster hangs up on the user and dials out to the specified location to establish a network connection.

Normal network users do not need Location Table entries. Dialback network users always require Location Table entries. Therefore, dialback network users must have their parameters set in the Location Table, not the User Table.

Configuring Login Users

Login users are allowed to establish PortMaster (`in.pmd`), rlogin, telnet, or netdata (TCP clear) connections with specified hosts. These connections require a different configuration than network users. Therefore, the parameters listed on the Users Table differ for network and login users. This section describes each of the parameters that must be entered to configure login users.

Once you have selected the Login User type for this user, select Normal or Dialback.

Configuring Normal Login Users

Normal login users establish connections with hosts using one of the login services described in Chapter 6, "Configuring an Asynchronous Port."

Creating a New Login User

A new login user is created when you enter a user name and password. The User Name parameter is used at the login prompt and can be up to 8 printable non-space ASCII characters. (RADIUS supports user names up to 63 characters long.) The password for the user can be up to 16 printable ASCII characters.

Setting the Login Host

The Login Host parameter defines the host to which the user is connected. The Login Host can be defined in one of three ways. Table 8-2 shows each of the host options.

Table 8-2 Login Host Options

Host Option	**Description**
Default	This option allows the user to login to the default or alternate host specified for this port.
Prompt	This option allows the user to select a host at the time the login session is established. The user must enter the IP address or host name.
Specified	This option allows the user to connect only to the host specifically named in the Host parameter field. A valid host name or IP address must be added to this field after the Specified option is selected. This configuration is used when you want to allow a user to access a specific host. For example, this configuration could be used to allow the user “susan” to always be connected with the host “sales.”

Setting an Optional Access Filter

An access filter can be associated with users to restrict which hosts they can log into. Access filters work as follows:

- The user logs in and specifies a host
- The host address is compared against the access filter
- If the address is permitted by the filter, the connection is established
- If the address is not permitted, the connection is denied

Setting the Login Service Type

All login users must have an associated login service that determines the nature of their connection with the host. Four types of Login Service are available as described in Table 8-3.

Table 8-3 Types of Login Service

Login Service	Function
PortMaster	PortMaster is the default login service and can be used to access any host that has the PortMaster `in.pmd` daemon installed. This type of login service is preferred because it makes the PortMaster port operate as if it was a serial port attached to the host.
Rlogin	Rlogin uses the rlogin protocol to establish a login session to the specified host. This login service is used on mixed UNIX networks where it is impractical to use the PortMaster login service.
Telnet	Telnet is supported on most TCP/IP hosts. This login service should be selected when the PortMaster and rlogin protocols are not available. The default TCP port number is 23, but another number can be entered.
Netdata	Netdata creates a virtual connection between the PortMaster port and another serial port on another PortMaster or between the PortMaster port and a host. This login service creates a clear channel TCP connection. To connect to another PortMaster port using netdata, that port must be configured as a Host Device with a Device Service Netdata using the same TCP port number. The default netdata TCP port is 6000; however, any number between 1 and 65535 can be used.

Configuring Dialback Login Users

When the Login User type Dialback is selected, the Telephone Number parameter is displayed and must be set. Telephone Number identifies the number that the PortMaster should dial to establish a connection with this user. The Login User dialback feature can only be used with modems that support the Hayes AT command set. The PortMaster always dials back using the same port on which the user dialed in.

Configuring Dial-Out Locations 9

This chapter describes how to configure network dial-out destinations using the Location Table. The parameters described in this chapter are not dependent on which user interface you are using to configure your system. The *Administrator's Guide* for your user interface describes how to set each option. The purpose of this chapter is to review each of the Location Table parameters and the options for each.

All of the possible location parameters are described in this chapter; however, you only need to configure the parameters required for your application. Specific configurations are described in Chapters 11 through 18.

Note – The Location Table is not used for dialing out with tip or UUCP. For information on these applications, refer to Chapter 14, "Configuring the PortMaster to Access Shared Devices."

This chapter includes the following topics:

- Overview of managing locations
- How to set dial-out on-demand locations
- How to set continuous dial-out locations
- How to set manual dial-out locations
- Setting general location parameters
- Setting multi-line load-balancing parameters
- Setting multilink PPP (MP) parameters
- Defining asynchronous and V.25bis chat scripts
- Testing your location configurations

Overview of Location Management

The Location Table is used to define each dial-out destination and the characteristics of the connection. The Location Table controls dial-out network connections in much the same way the User Table controls dial-in network connections.

The Location Table can be accessed through the Table menu in PMconsole. Figure 9-1 shows an example of a Location Window. The window you see will vary depending on the version of PMconsole you are using to configure your PortMaster. The Location Table can also be configured using the command line interface.

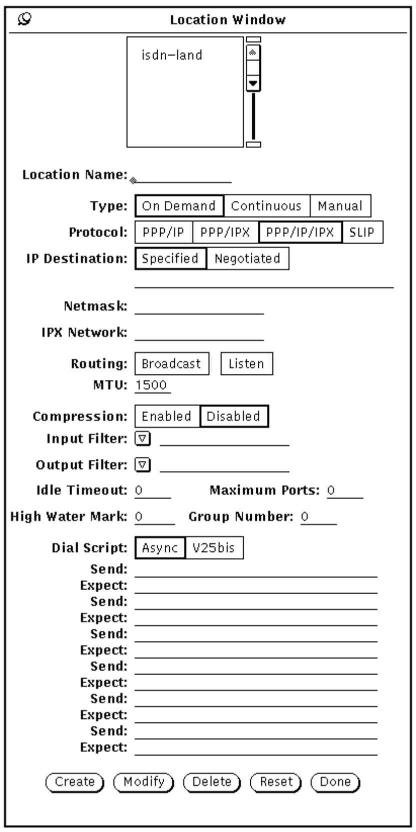

Figure 9-1 Location Window—X Windows GUI

A unique dial-out location must be created for each remote host or router you want to access. Location Table entries are identified by a unique Location Name parameter, which can be any 12-character name used to identify the remote location.

Once you have created a new location by giving it a unique name, you must define how the connection with the location will be initiated. Connections can be initiated as shown in Table 9-1. Before you change from one connection type to another, verify that the connection is not active.

Table 9-1 Initiating Dial-Out Connections

Connection Type	Description
On Demand	This type of connection with the specified location is started when packets for the remote location are queued by the PortMaster.
Continuous	This type of dial-out connection with the specified location is always active. If the telephone connection is dropped the PortMaster initiates a new connection with the location after a one minute waiting period.
Manual	This type of connection with the specified location is started when the administrator requests a connection. This configuration can be used by the administrator to test a connection. This type of connection can also be used for network dialback users.

Setting On-Demand Dial-Out Locations

On-demand dial-out connections to selected locations can save money because the telephone line is only used when there is traffic that needs to be transmitted. The dial on-demand configuration can also be used as a backup for other types of connections such as those using high-speed synchronous lines. Dial-out on-demand is usually used with the Idle Time parameter so that the connection is closed when no longer needed.

When configuring an on-demand location be careful not to have the on-demand location be the route to the Loghost, RADIUS server, RADIUS Accounting server, or any Host for a port using the PortMaster login or device service, unless you are very careful to understand the effect of these services upon dial on-demand.

If Routing for an on-demand location is set to On, Listen or Broadcast, the PortMaster will dial out to that location when it boots, to update routing information. It hangs up when the idle timer expires since RIP traffic does not reset the idle timer.

To set a location to support a dial on-demand connection, set the Type parameter to On-Demand.

Setting Continuous Dial-Out Locations

A continuous dial-out connection can be established with a location whose Location Type is set to Continuous. In this configuration, the PortMaster dials out after it boots and establishes a network connection to the specified location. If the connection is dropped for any reason, the PortMaster dials out again and re-establishes the connection after a one minute wait.

To set a location to support a continuous connection, set the Type parameter to Continuous.

Setting Manual Dial-Out Locations

Locations can be set for manual dialing while you are configuring them or if you want the connection to be established only when requested by the administrator or a network dialback user. Use manual dial-out to test the connection before changing it to a continuous or on-demand location. To set a location to support a manual connection, set the Type parameter to Manual.

Note – When switching a location from Manual to On Demand, verify that the dial-out connection has been closed and that the serial port is reset before updating the location table.

Setting Location Table Parameters

The parameters described in this section allow you to configure dial-out locations. Many of these same parameters are set for network users. Remember, the User Table controls dial-in connections and the Location Table controls dial-out connections.

Setting the Protocol for a Location

The network protocol for a dial-out location can be set for PPP packet encapsulation or SLIP encapsulation as described in Chapter 3, “How PortMasters Work.” If you want to use the Point-to-Point Protocol you have your choice of the following options:

- PPP with IP packet routing
- PPP with IPX packet routing
- PPP with both IP and IPX packet routing
- Frame

You should select a protocol that is compatible with the remote location. For more information about setting the location protocol parameter to Frame for a Frame Relay subinterface, see "Frame Relay Subinterface" on page 16-10.

Setting the Destination IP Address

The IP Destination parameter defines the IP address or host name of the remote host or router. For SLIP connections and locations set for on-demand dialing, the IP Destination parameter must be set to Specified and the IP address for the remote system must be entered.

For PPP connections to locations set for continuous or manual operation, the IP address of the destination can be specified or negotiated. If set to negotiated, the PortMaster learns the IP address of the remote system during PPP IPCP negotiation. Negotiated addresses cannot be used with SLIP connections or on-demand locations.

Setting the Destination Netmask

The Netmask parameter is the netmask of the host or network on the remote end of the connection.

Note – PortMasters do not support variable length subnet masks. All subnets of the same network must have the same netmask.

Setting the IPX Network Number

You must assign a unique IPX network number to the network connection between the remote host and the PortMaster, if you are using the IPX protocol. The IPX Network parameter is the IPX network for the serial connection and must be different than any other IPX network number used on your network.

Enabling Routing

Locations can have routing associated with them. This is used for connections such as dial on-demand routing where the remote router is defined as a location on the local PortMaster.

PortMaster products send and accept route information as part of RIP messages if routing is turned on. If you select Broadcast for the Routing parameter, RIP packets are sent to the host on the other end of the connection. When Listen is selected, the PortMaster accepts RIP packets from the remote host or router. Both options can be selected at the same time to enable the sending and acceptance of routing information. If neither option is selected, RIP is disabled on the interface and the PortMaster ignores all routing messages from this location.

If you are using RIP, the destination address for the connection must match the source address of the RIP packets received from the remote router.

Setting the MTU

The Maximum Transmission Unit or MTU defines the largest frame or packet that can be sent to this location. If an IP packet exceeds the specified MTU it is automatically fragmented. An IPX packet that exceeds the specified MTU is automatically dropped. PPP connections can have an MTU set from 100-1500 octets. SLIP connections can have an MTU set from 100-1006 octets. With PPP, the PortMaster can negotiate smaller MTUs when requested during PPP negotiation.

The MTU is typically set to the maximum allowed for the protocol being used, either 1500 or 1006. However, smaller MTU values can improve performance for interactive sessions. If you are using IPX, the MTU should be set to at least 600.

Setting TCP Header Compression

Compression of TCP/IP headers can increase the performance of interactive TCP sessions if the devices on both ends of the connection support compression. PortMasters support Van Jacobson TCP/IP header compression on asynchronous ports.

Compression should not be used with multi-line load-balancing, but may be used with multilink PPP.

Compression must be enabled or disabled on both ends of the connection if you are using SLIP. For PPP connections, PortMasters support both bidirectional and unidirectional compression. Refer to RFC 1144 for more information about header compression.

Setting Filters

Input and output filters can be attached to each location. If an input filter is attached to a location, when the PortMaster dials out and establishes a connection to the location, all packets received from the interface are evaluated against the rule set for the attached filter and only packets allowed by the filter are accepted. If an output filter is attached to a location, only packets allowed by the filter are passed out to the interface. For more information about filters, see Chapter 10, “Configuring Filters.”

Setting the Idle Time

The Idle Time parameter can be set for manual or on-demand locations. This parameter defines the number of minutes the line can be idle, with no network traffic to or from the remote site, before the PortMaster disconnects the telephone connection and hangs up the line. The Idle Time can be set from 2 to 240 minutes. If a setting of 0 or 1 is used, no idle time out occurs. The idle timer is not reset by RIP, keepalive, or SAP packets.

Note – Idle times for dial-in connections are set on each port. Idle times for dial-out connections are set in the Location Table.

Setting the Dial Group

Each location must be assigned to a Dial Group, as described in Chapter 6, “Configuring an Asynchronous Port” and Chapter 7, “Configuring a Synchronous WAN Port.” Only ports in this Dial Group are available to dial out to this location. This parameter is used to allocate ports for specific locations. Special modems that are only compatible with this location can be assigned to a special group for this location.

The Dial Group parameter associated with a location works with the Dial Group parameter specified for each port. For example, you create a dial out location called “home” and specify that the Dial Group for “home” is 2. When you configure each port you can assign the port to a Dial Group. Only ports assigned to group 2 will be used to dial the location “home,” while other ports will not. Dial Groups are numbered 0 to 99.

Setting Multi-line Load-balancing

Several asynchronous ports can be set to connect to a single location in order to distribute heavy traffic loads. This is called multi-line load-balancing. A threshold or high-water mark for a location can be defined to trigger the PortMaster to bring up an additional connection to the location when the amount of data specified by the high-water mark is queued. The PortMaster examines the queue several times a minute to determine if the high-water mark has been reached.

Load balancing is useful for on-demand routing because as the load exceeds what can be handled by one port, additional connections with the location are initiated. As the load drops the additional connections can be closed by the idle timer.

Load balancing can save you money because you do not need to configure your network to handle the maximum load between locations. Periods of heavy traffic can be handled by additional ports on an as-needed basis. At other times, the additional ports can be used for other purposes.

When multiple ports are in use, each packet is queued on the port with the least amount of traffic in the queue. Ports with very different speeds should not be combined for load balancing purposes. The overall throughput for a given number of ports will be approximately equal to the number of ports, multiplied by the throughput of the slowest port.

Note – TCP header compression cannot be used with multi-line load-balancing.

The following parameters are used to configure load-balancing and define when additional lines to this location are dialed.

Setting the Maximum Number of Dial-Out Ports

The Maximum Ports parameter defines the number of dial-out ports that can be used to dial and establish a connection with this location. This parameter creates a pool of ports that can be used to establish a connection with this location at the same time.

If the maximum number of ports is set to 0, no connection with this location is established. If the Maximum Ports parameter is set to any number greater than 1, the High Water Mark parameter is used to determine when additional connections are established with this location.

When more than one line is open to a given location, the PortMaster balances the load across each line. The value of the Idle Timeout parameter is used to determine when to disconnect unneeded lines.

Setting the High Water Mark

The High Water Mark parameter determines when an additional line to this location should be established. The High Water Mark specifies the number of bytes of queued network traffic needed to open an additional connection. The PortMaster examines the queue several times a minute to determine if the high-water mark has been reached.

If you set a very small threshold number, the PortMaster will quickly use all of the ports specified by the Maximum Ports parameter. When you are deciding on a threshold, keep in mind that interactive traffic from login users queues a relatively small number of bytes, only several hundred. However, network users doing file transfers can queue several thousand bytes of traffic. These activities should be considered before you set your dial-out threshold.

This value is only used when the Maximum Port parameter is greater than 1.

Setting Multilink PPP

ComOS 3.3 and later supports Multilink PPP (MP) as described in RFC 1717. To use Multilink PPP instead of Multi-line Load Balancing, set the Multilink parameter in the location table entry ON, and set Maximum Ports to the number of ports you wish to use for MP.

Defining and Using Chat Scripts

Chat scripts are strings of text used to send commands to modems or V.25bis dialers for dialing out and logging into remote systems. Each chat script is defined for a dial-out location and consists of send and expect strings.

PortMaster chat scripts should be written for placing a call and logging into the machine at the remote location for which the script is intended. The dial script can also be used for authentication at the remote site. Each dial script contains a series of send and expect strings. The send string is sent from the PortMaster to the modem and thus the remote host. The expect string is received by the PortMaster from the modem or remote host and used to verify that the previous send string was properly received. If the expect string is correct, the PortMaster sends the next send string.

Send strings can be up to 30 printable ASCII characters. In addition, the special characters shown in Table 9-2 are available.

Table 9-2 Chat Script Special Characters

Character	Description
“”	Expect or send nothing
\r	Sends a carriage return character
\n	Sends a line feed character
\0XX	Sends the octal digit specified by XX
\\	Sends a single backslash character

All chat script send strings must end with a carriage return (\r) character, except V.25bis script send strings.

A valid expect string needs to only check for the last word in the received string. For example, if the remote system is prompting for a login ID, it may issue the following string:

```
Please enter your login:
```

“ogin:” is a valid expect string for this prompt. The last expect string in a chat script should be a string that indicates that the remote system is ready to receive network packets. You must be familiar with the remote system prompts in order to determine what the final expect string should be. If you are connecting to another PortMaster and establishing a PPP or SLIP connection, the final expect string should be PPP or ~ for PPP connections and SLIP for SLIP connections.

Chat scripts for remote locations are specified using the Location Table. No quotes are needed for any of the send and expect strings if you are using PMconsole.

Asynchronous Chat Script Examples

Table 9-3 is an example of a dial script that establishes a connection between two PortMasters that have modems supporting the AT dial command syntax.

Table 9-3 Example Chat Script

String Type	String	Description
Send	ATDT18005551212\r	Dials the number specified
Expect	CONNECT	Expect the modem to connect
Send	\r	Sends a carriage return to prompt the next transmission
Expect	ogin:	Expect a prompt for your user name that ends with the characters "login:" or "Login:"
Send	my_login\r	Sends the actual user name for your location, known to the remote system
Expect	ssword:	Expect a prompt for your password that ends with the characters "ssword:"
Send	my_password\r	Sends the actual password, known to the remote site, associated with your user name
Expect	PPP	Expect the remote system to start the PPP connection

If you are using CHAP with PPP, you only need the first send and expect string shown in Table 9-3. The rest of the authentication takes place using CHAP and does not need to be scripted. For more information about CHAP, refer to Chapter 3, "How PortMasters Work."

Table 9-4 shows other chat script send and expect strings and their meanings.

Table 9-4 Other Chat Script Send and Expect Strings

String Type	String	Description
Send	AT Z\r	Sends the AT Z command to the modem
Expect	OK	Expect OK
Send	ATDT18005551212\r	Sends the dial command and dial number to the modem
Expect	=DCD=	Waits for Carrier Detect
Expect	~	Expect first character of PPP negotiation
Send	=PAP=*user*/*password*	Authenticate using PAP with ID *user* and password *password*

Any strings that define the traffic between two systems can be incorporated into dial scripts.

V.25bis Chat Script Example

A V.25bis chat script should be used instead of an asynchronous chat script if you are dialing out on a synchronous port attached to a switched 56K or an ISDN terminal adapter. V.25bis dialing can also be used on ISDN BRI ports. Table 9-4 shows an example of a V.25bis chat script.

Note – There is no carriage return after the phone number. PPP authentication can be done with CHAP, or with PAP by using the =PAP= Send string in ComOS 3.3 or later..

Table 9-5 V.25bis Chat Script Send and Expect Strings

String Type	String	Description
Send	CRN15105552222	Sends the dial command and dial number to the terminal adapter
Expect	=DCD=	Waits for Carrier Detect

Testing Your Location Configuration

When you are configuring a location, it is useful to set the location to manual so that you can test the configuration before resetting the location to on-demand or continuous. In order to test the configuration, you must actually initiate a connection with the remote location using the Dialer Window from the View menu of PMconsole or the dial command from the command line. Watch the connection process to ensure that your chat script and other location specific parameters are configured correctly.

When your location is configured correctly, change the location type from Manual to Continuous or On Demand.

Note – When switching a location from Manual to On Demand, verify that the dial out connection has been closed and that the serial port is reset before updating the Location Table.

Configuring Filters 10

This chapter describes how to configure input and output filters. IP, IPX and SAP rules are reviewed and filter examples are given.

This chapter includes the following topics:

- An overview of packet filters and how they are organized and created
- A description of IP, IPX, and SAP filter rules
- Filtering FTP packets
- How filters are used to limit network access

Each of the topics in this chapter include examples of filters used to accomplish the goal described.

Overview of Filters

Packet filters are used to increase security on your network. Filters are especially useful for restricting information that is passed across organizational and corporate boundaries. Filters can be used to limit certain kinds of internetwork communications by permitting or denying the passage of packets through network interfaces or ports. By designing appropriate filters, you can control access to specific hosts, networks, and network services.

Packet filtering requires the analysis of the header information contained in each packet sent or received through an interface. The header information is evaluated against a set of rules, which allow the packet to pass freely through the interface or cause the packet to be discarded without being forwarded. If a packet is not permitted by a filter, an appropriate ICMP unreachable or TCP Reset message is returned to the originator. This process reduces network traffic and provides more immediate feedback to the user attempting the unauthorized access.

Filters can also be used for packet selection, such as when using a packet trace to debug a connection. The packets permitted by the ptrace filter are displayed, while packets not permitted by the filter are not displayed. For more information about ptrace, see “Tracing Packets” on page 19-8.

The packet filtering mechanism is designed with four objectives:

- Reliability
- Predictability
- Flexibility
- Efficiency

The features listed in Table 10-1 help achieve these objectives.

Table 10-1 Features of PortMaster Filtering

Feature	**Description**
Input and Output Filters	Each user, each location, and each network hardwired port can be assigned both an input packet filter and an output packet filter. Having both input and output filters can decrease the number of rules needed and can provide better tuning of your security policy.
Source and Destination Address Filtering	You can create filters that evaluate both the source and destination addresses of a packet against a rule list. The number of significant bits used in IP address comparisons can be set, allowing filtering by a specific host, subnet, network number, or a group of hosts whose addresses are within a given bit-aligned boundary.
Protocol Filtering	Packets of certain protocols can be permitted or denied by a filter, including IPX, SAP, TCP, UDP, and ICMP packets.
Source and Destination Port Filtering	You can create filters that use the source and destination port numbers to control access to certain network services. This includes evaluation based upon whether the port number is less than, equal to, or greater than a specified value.
Established Session Filtering	You can create filters that use the status of TCP connections as part of the rule set. This can allow network users to open connections to external networks without allowing external users access to the local network.

Table 10-1 Features of PortMaster Filtering *(Continued)*

Feature	Description
Number of Rules	Each filter can have any number of rules, limited only by the memory available within the PortMaster.
Simple Rule Creation	You can create filters that only include as much information as is necessary to describe the rule. For example, if the rule is not based on specific source and destination addresses, they can be omitted from the rule.
In-line Rule Processing	Rules are processed in the order they are specified in the rule set. This eliminates ambiguity about how a packet is handled. The first rule that matches the packet is applied. If the rule is defined as permit, the packet is allowed to pass. If the rule is defined as deny, the packet is discarded. If there are any rules in the filter and the packet does not match any of the rules, the packet is discarded.

Filter Organization

Filters are maintained in a Filter Table in the PortMaster nonvolatile configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter has a name of up to 16 characters.

Each packet filter can contain three sets of rules: IP, IPX, and SAP. Within each set, the rules are numbered starting at one. Newly created packet filters do not contain any rules.

An empty set of rules is equivalent to the permit rule. If there are one or more rules in the set, any packet not explicitly permitted by a rule is denied at the end of the rule set.

IP and IPX packet filters are attached to users, locations, or network hardwired ports as either input or output filters. SAP filters are only attached as output filters. For asynchronous interfaces, the packet filter is enabled when the port transitions to the established state. The Ethernet interface filter is enabled as soon as the name of the input or output filter is attached to the interface.

All packets passing into an interface with an input filter are evaluated against the rules in the filter. As soon as a packet matches a rule, the action specified by that rule is taken. If no rules match the specific packet, the packet is denied and is discarded. Whenever an IP packet is discarded, the PortMaster generates an ICMP Host Unreachable message back to the originator. For interfaces with output filters attached, all packets going out of the interface are evaluated against the filter rules and only those packets permitted by the filter are allowed to pass out of the interface.

Filter Creation

Filters are created using the Filter Table available with any of the PMconsole interfaces to the PortMaster or from the command line. To create a filter, open the Filter Table by selecting Filters from the Tables menu. Figure 10-1 shows an example of the Filter Window. The window you see depends on the version of PMconsole you are using to configure your PortMaster.

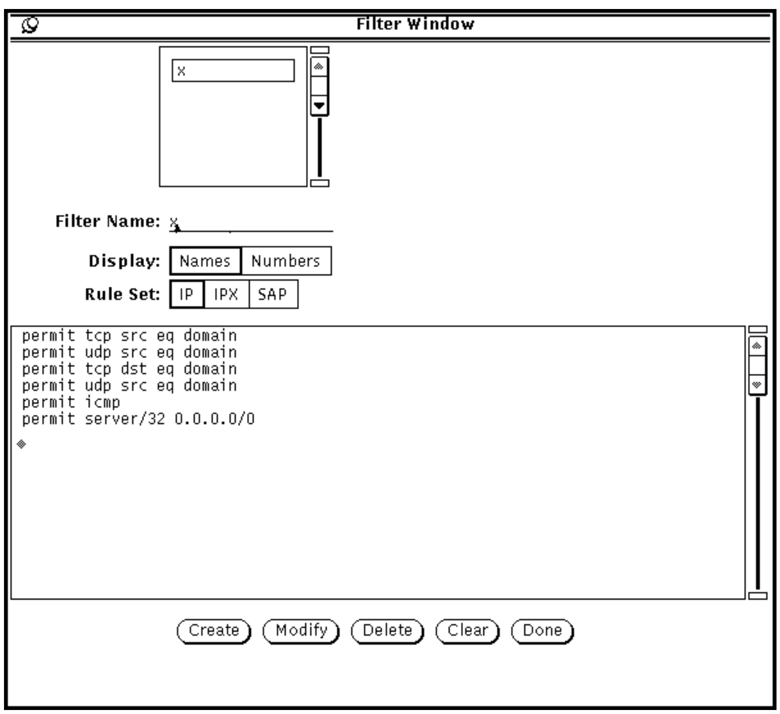

Figure 10-1 Filter Table Window—X Windows GUI

Setting Filters

Filters are constructed by creating the filter and then adding rules that permit or deny certain types of packets. Packets are evaluated in the same order as the rules are listed. Therefore, the packets representing the highest volume of traffic should be specified early in the list of rules, where possible.

Filters can be attached to Ethernet interfaces, hardwired serial ports, users, and locations. Ethernet filters are used to control the types of packets that are allowed to pass through the local Ethernet port. Filters are set on asynchronous ports configured for hardwired operation when security with another network is an issue.

User filters are attached to users configured for dial-in SLIP or PPP access. When a user makes a PPP or SLIP connection the designated filters are attached to the interface used.

Location filters are attached to dial-out locations using SLIP or PPP connections. When the connection is established to a remote site the designated filters are attached to the interface used.

You can attach filters for incoming packets or for outgoing packets or both. It is usually more effective to filter incoming packets for two reasons:

- You know which interface the packet is coming in on
- You can protect the PortMaster itself

Setting IP Filters

IP rules are specified using the following syntax:

```
action [[source_addr/mask dest_addr/mask] protocol [option]] [log]
```

Each of the criteria and its options are shown in Table 10-2.

Table 10-2 Description of IP Rule Syntax

Criteria	Options	Description
action	permit	Permits the packet to pass through the interface.
	deny	Stops the packet from passing through the interface. The packet is dropped and an ICMP Host Unreachable message is sent to the source address.
source_addr/ mask		Specifies the comparison with the source IP address of the packet. The number of high-order bits of the source IP address is determined by the mask. Common mask values are: 0—To match all packets with any source address 16—Looks only at network number of class B IP addresses 24—Looks only at network number of class C IP addresses 32—Looks at the entire IP address
dest_addr/ mask		Specifies the comparison with the destination IP address contained in the packet. The number of high-order bits of the destination IP address is determined by the mask.
protocol	TCP	Specifies that the filter looks for TCP packets. This type of rule supports filtering on source and destination port numbers as well as the established state of the connection.
	UDP	Specifies that the filter looks for UDP packets. This type of rule supports filtering on source and destination port numbers.
	ICMP	Specifies that the filter looks for ICMP packets. This rule supports filtering on the type of ICMP message. The only option for this rule is: `[type icmp_message_type]` A comparison is made with the ICMP message type contained in the packet. ICMP message types are defined in RFC 1700, “Assigned Numbers.”

Table 10-2 Description of IP Rule Syntax *(Continued)*

Criteria	Options	Description
option		The options depend on the protocol specified. The TCP options are described in Table 10-3. The UDP options are described in Table 10-4. The ICMP option is described in the ICMP option above.
log		If this rule is matched a syslog message is sent to the loghost with `auth.notice` facility and priority.

The syntax for TCP options is shown below and the options are explained in Table 10-3:

```
[src eq|gt|lt port_number] [dst eq|gt|lt port_number] [estab]
```

Table 10-3 TCP Rule Options

Option	Description
src	Compare the port number in the filter with the TCP source port number
dst	Compare the port number in the filter with the TCP destination port number
eq	The port number in the packet should be tested to see if it is equal to the port number specified in the rule
gt	The port number in the packet should be tested to see if it is greater than the port number specified in the rule
lt	The port number in the packet should be tested to see if it is less than the port number specified in the rule
estab	Determine if the packet is for an established TCP network connection. Packets being sent to start new TCP connections do not match this rule.

The syntax for UDP options is shown below and the options are explained in Table 10-4:

```
[src eq|gt|lt port_number] [dst eq|gt|lt port_number]
```

Table 10-4 UDP Rule Options

Option	**Description**
src	Compare the port number in the filter with the UDP source port number
dst	Compare the port number in the filter with the UDP destination port number
eq	The port number in the packet should be tested to see if it is equal to the port number specified in the rule
gt	The port number in the packet should be tested to see if it is greater than the port number specified in the rule
lt	The port number in the packet should be tested to see if it is less than the port number specified in the rule

Table 10-5 lists common TCP and UDP services. A more complete list is available in RFC 1700, "Assigned Numbers." If you are configuring filters with PMconsole, you can use the service name or number for the port, as found in the `/etc/services` file on most hosts. If you are configuring filters from the command line interface, you must use the port number, not the name.

Table 10-5 TCP and UDP Port Services

Service	**Port**	**Type**	**Description**
ftp-data	20	tcp	File Transfer (Default Data)
ftp	21	tcp	File Transfer (Control)
telnet	23	tcp	Telnet
smtp	25	tcp	Simple Mail Transfer (email)
nicname	43	tcp	Who Is
nicname	43	udp	Who Is

Table 10-5 TCP and UDP Port Services *(Continued)*

Service	**Port**	**Type**	**Description**
domain	53	tcp	Domain Name Server
domain	53	udp	Domain Name Server
tftp	69	udp	Trivial File Transfer
gopher	70	tcp	Gopher
gopher	70	udp	Gopher
finger	79	tcp	Finger
finger	79	udp	Finger
www-http	80	tcp	World Wide Web HTTP
kerberos	88	tcp	Kerberos
kerberos	88	udp	Kerberos
pop3	110	tcp	Post Office Protocol - Version 3
sunrpc	111	tcp	SUN Remote Procedure Call
sunrpc	111	udp	SUN Remote Procedure Call
auth	113	tcp	Authentication Service
auth	113	udp	Authentication Service
nntp	119	tcp	Network News Transfer Protocol
ntp	123	tcp	Network Time Protocol
ntp	123	udp	Network Time Protocol
snmp	161	tcp	SNMP
snmp	161	udp	SNMP
snmptrap	162	tcp	SNMPTRAP
snmptrap	162	udp	SNMPTRAP
imap3	220	tcp	Interactive Mail Access Protocol v3
imap3	220	udp	Interactive Mail Access Protocol v3
exec	512	tcp	remote process execution
login	513	tcp	remote login

Table 10-5 TCP and UDP Port Services *(Continued)*

Service	**Port**	**Type**	**Description**
who	513	udp	remote who (rwhod)
cmd	514	tcp	remote command (rsh)
syslog	514	udp	System Log Facility
printer	515	tcp	lpd spooler
talk	517	tcp	terminal to terminal chat
talk	517	udp	terminal to terminal chat
ntalk	518	tcp	newer version of terminal to terminal chat
ntalk	518	udp	newer version of terminal to terminal chat
router	520	udp	RIP
uucp	540	tcp	UNIX to UNIX Copy
uucp	540	udp	UNIX to UNIX Copy
uucp-rlogin	541	tcp	a different variant of UUCP/TCP
uucp-rlogin	541	udp	a different variant of UUCP/IP
klogin	543	tcp	Kerberized login
klogin	543	udp	Kerberized login
pmd	1642	tcp	PortMaster daemon in.pmd
pmconsole	1643	tcp	PortMaster Console Protocol
radius	1645	udp	Remote Authentication Dial In User Service
radacct	1646	udp	RADIUS Accounting

Setting IPX Filters

IPX rules are specified using the following syntax:

```
action [keyword value] [keyword value] ...
```

Each of the valid keywords are shown in Table 10-6.

Table 10-6 Description of IPX Rule Syntax

Option/Keyword	Description
action	The two options for action are permit and deny. Permit allows the packet to pass freely through the interface. Deny stops the packet from passing through the interface.
srcnet	Compares the stated value with the source IPX network address of the packet. This value must be in hexadecimal format.
dstnet	Compares the stated value with the destination IPX network address in the packet. This value must be in hexadecimal format.
srchost	Compares the stated value with the source IPX node address in the packet. This value must be in hexadecimal format.
dsthost	Compares the stated value with the destination IPX node address in the packet. This value must be in hexadecimal format.
srcsocket	Compares the stated value with the source IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid values for the second keyword are: eq, lt, or gt. The value follows the second keyword.
dstsocket	Compares the stated value with the destination IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid values for the the second keyword are: eq, lt, or gt. The value follows the second keyword.

Setting SAP Filters

SAP can be filtered on output. SAP rules are specified using the following syntax:

```
action [keyword value] [keyword value] ...
```

Each of the valid keywords are shown in Table 10-7.

Table 10-7 Description of SAP Rule Syntax

Option/Keyword	**Description**
action	The two options for action are permit and deny. Permit allows the SAP entry to be broadcast in SAP packets. Deny stops the SAP entry from being sent in SAP broadcasts.
server	Compares the value with the name of the server which is advertising its service. The server value is case-sensitive.
network	Compares the stated value with IPX network address of the server. This value must be in hexadecimal format.
host	Compares the stated value with the IPX node address of the server. This value must be in hexadecimal format.
socket	Compares the stated value with the IPX socket number of the server. A second keyword indicating the type of comparison must be specified. Valid values for the second keyword are: eq, lt, or gt. The value follows the second keyword.

Filtering FTP Packets

Filters can be used to either permit or deny FTP packets. It is important to understand how this protocol works before you develop FTP filters.

File Transfer Protocol (FTP) uses TCP port 21 as a control channel, but it transfers data on another channel initiated by the FTP server from TCP port 20 (FTP-data). Therefore, if you want to allow your internal hosts to FTP outward, you must allow external hosts to open an incoming connection from TCP port 20 to a destination port above 1023. Allowing this type of access to your network can be very risky if you are running RPC or X Windows on the host from which you are FTPing. As a result, many sites use FTP proxies or passive FTP, neither of which is discussed in this guide.

However, *Firewalls and Internet Security: Repelling the Wily Hacker* by Cheswick and Bellovin (Addison-Wesley 1994, ISBN 0-201-63357-4) and *Building Internet Firewalls* by Chapman and Zwicky (O'Reilly & Associates 1995, ISBN 1-56592-124-0) are good references.

Likewise, if you want to allow external hosts to connect to your FTP server and transfer files, you must allow incoming connections to TCP port 21 on your FTP server and allow outgoing connections from TCP port 20 of your FTP server.

In the following examples, ftp.edu.com is the name of your FTP server and proxy.edu.com is the name of the host from which you allow outgoing FTP.

```
internet.in filter
permit tcp 0.0.0.0/0 proxy.edu.com/32 src eq 20 dst gt 1023
permit tcp 0.0.0.0/0 proxy.edu.com/32 src eq 21 estab
permit tcp 0.0.0.0/0 ftp.edu.com/32 dst eq 21
permit tcp 0.0.0.0/0 ftp.edu.com/32 src gt 1023 dst eq 20 estab
```

```
internet.out filter
permit tcp proxy.edu.com/32 0.0.0.0/0 dst eq 21
permit tcp proxy.edu.com/32 0.0.0.0/0 src gt 1023 dst eq 20 estab
permit tcp ftp.edu.com/32 0.0.0.0/0 src eq 20 dst gt 1023
permit tcp ftp.edu.com/32 0.0.0.0/0 src eq 21 dst gt 1023 estab
```

If you allow any internal host to FTP outwards, replace proxy.edu.com/32 with 0.0.0.0/0 or your *network_number*/24. Take appropriate precautions to reduce the risk this configuration creates.

Note – This configuration is not recommended if you run any of the following protocols on any of the hosts from which you allow ftp access: NFS, X, RPC, or any other service that listens on ports above 1023.

Filter Examples

Filters are very flexible; therefore, it is very important that you evaluate the types of traffic that a specific filter permits or denies through an interface before attaching the filter. If possible, filters should be tested from both sides of the filtering interface to verify that the filter is operating as you intended. The `log` keyword is very useful when testing and refining filters.

Note – Any packet that is not explicitly permitted by a filter is denied, except for the special case of a filter with no rules, which permits everything.

Simple Filter Example

The filter is written as follows:

```
permit udp dst eq domain
permit tcp dst eq smtp
permit icmp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit tcp src eq ftp-data dst gt 1023
```

Table 10-8 shows the description of the filter.

Table 10-8 Description of Simple Filter

Rule	Description
1	Permits Domain Name Service (DNS) UDP packets from any host to any host.
2	Permits SMTP (mail) packets.
3	Permits ICMP packets, including ping packets.
4	Permits FTP from any host but only to the host ftp.edu.com.
5	Permits FTP data to return to the requesting host. This rule is required to provide a reverse channel for the data portion of FTP.

Filter for Internet Connection on a Hardwired Port

The filter in this example is designed as an input filter for a hardwired network interface set up to connect to the Internet. If this filter were used for dial on-demand connections it should be attached to the appropriate user and location. The filter is written as follows:

```
deny 192.168.1.0/24 0.0.0.0/0 log
permit tcp estab
permit 0.0.0.0/0 mail.edu.com/32 tcp dst eq smtp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit tcp 0.0.0.0/0 www.edu.com/32 dst eq www-http
permit tcp src eq ftp-data dst gt 1023
permit udp dst eq domain
permit tcp dst eq domain
permit icmp
```

Table 10-9 describes the filter.

Table 10-9 Description of Internet Filter

Rule	Description
1	Deny any incoming packets from your own network (192.168.1.0). This blocks IP spoofing attacks. Log the header information using syslog.
2	Permits already established TCP connections.
3	Permits SMTP connections to the mail server mail.edu.com.
4	Permits FTP to the host ftp.edu.com.
5	Permits www (http) access to the host www.edu.com.
6	Permits FTP data channel.
7	Permits Domain Name Service.
8	Permits Domain Name Service zone transfers. (You may wish to restrict this rule to allow only connections to your name servers.)
9	Permits ICMP packets.

Domain Name Server is Outside Your Local Net

If the DNS name server for your domain is outside your local net you should add the following rule to your input filter:

```
permit udp src eq domain
```

This permits DNS replies into your local net. You should then add the following output filter described in Table 10-10 to the interface:

```
deny 0.0.0.0/0 192.168.1.0/24 log
permit tcp
permit udp src eq domain
permit udp dst eq domain
permit gw.edu.com/32 rt.isp.net/32 udp dst eq 520
permit icmp
```

Table 10-10 Description of External DNS Output Filter

Rule	Description
1	Denies any outgoing packets to your own network (192.168.1.0) and makes a log.
2	Permit any TCP connection.
3	Permit Domain Name Service replies from your network.
4	Permit Domain Name Service queries from your network.
5	Permits outgoing RIP packets from the PortMaster (gw.edu.com) to the router (rt.isp.net) at the other end of the serial link.
6	Permit ICMP packets.

Note – Since the PortMaster does not apply filter rules to its own UDP and ICMP packets, rule 5 is not necessary. However, if you are broadcasting routing through this interface it is a good idea to include this rule in case PortMaster behavior is changed in the future.

Filter to Listen to RIP Information

To permit incoming RIP packets, add the following rule to your input filter:

```
permit rt.isp.net/32 gw.edu.com/32 udp dst eq 520
```

Filter to Allow Auth Queries

To allow auth queries used by some mailers and FTP servers, add the following rule to your input filter:

```
permit tcp dst eq 113
```

For more information about these types of queries, refer to RFC 1413.

Limiting Access to Specified Hosts

Security on your network can be increased if you limit the authorized activities for certain hosts. For example, you can limit the DNS and SMTP interchange with the Internet to a single well-secured host on your network. All Internet hosts would then access this single server for those services. If you have several name servers or mail servers, you can use additional rules to allow access to these servers.

To allow some other network (172.16.12.0) to have complete access to your network, add the following rule:

```
permit 172.16.12.0/24 192.168.1.0/24
```

Caution – Beware of associative trust. If 192.168.1 trusts 172.16.12 and 172.16.12 trusts 10.5.137, then 192.168.1 trusts 10.5.137 whether 192.168.1 knows it or not.

Restrictive Internet Filter

This filter is an example of an input filter for a network hardwired port. If you use dial on-demand you should add this filter to the appropriate Location Table entry.

This example allows any kind of outgoing connection from the Internet server but blocks all incoming traffic to any host but your designated Internet server. This filter allows incoming SMTP, NNTP, DNS, FTP, and ICMP traffic to the Internet server and blocks all other traffic.

Note – Unless you have the latest versions of `ftpd`, `httpd`, and `sendmail` you may be vulnerable to attacks through these ports. Check the latest CERT advisories, available on `ftp.cert.org`, for existing vulnerabilities.

In the following example, the name `server` should be replaced by the IP address or host name of your Internet server.

```
deny 192.168.1.0/24 0.0.0.0/0 log
permit 0.0.0.0/0 server/32 tcp estab
permit 0.0.0.0/0 server/32 tcp dst eq ftp
permit 0.0.0.0/0 server/32 tcp src eq ftp-data dst gt 1023
permit 0.0.0.0/0 server/32 tcp dst eq nntp
permit 0.0.0.0/0 server/32 tcp dst eq smtp
permit 0.0.0.0/0 server/32 tcp dst eq www-http
permit 0.0.0.0/0 server/32 udp dst eq domain
permit 0.0.0.0/0 server/32 tcp dst eq domain
permit 0.0.0.0/0 server/32 icmp
```

Table 10-11 describes the filter.

Table 10-11 Description of Restrictive Internet Filter

Rule	**Description**
1	Denies any incoming packets from your own network (192.168.1.0) and makes a log.
2	Permits packets from any established TCP connection to the Internet server.
3	Permits FTP from any one to the Internet server.

Table 10-11 Description of Restrictive Internet Filter

Rule	Description
4	Permits FTP data back channel.
5	Permits incoming NNTP (news) to the Internet server.
6	Permits incoming SMTP (mail) to the Internet server.
7	Permits www (http) requests to the Internet server.
8	Permits Domain Name Service queries to the Internet server.
9	Permits DNS zone transfers from the Internet server.
10	Permits ICMP to the Internet server. You can further limit ICMP to types 0, 3, 8, and 11 using four rules instead of one. See *RFC 1700* for the list of ICMP packet types.

To log all blocked packets add the following rule to the end of your filter:

```
deny log
```

Access Filters

Access filters allow you to limit access to a specified host or group of hosts. Interactive users, those using telnet and rlogin, can be allowed to select a host for their sessions. However, you may want to limit their access to specific hosts or networks. An access control filter allows you to designate a limited set of hosts or networks accessible by the user when they are presented with the “Host:” prompt.

Connecting a Branch Office to the Main Office 11

This chapter describes how to use the PortMaster to connect your office to another office using a dial on-demand configuration. This type of connection is designed to take the place of a costly dedicated line between the two locations, where the amount and duration of traffic does not justify a leased line or Frame Relay connection.

The following topics are described:

- Overview of the configuration
- Description of hardware configuration
- Description of software configuration on the PortMaster in the branch office
- Description of the software configuration on the PortMaster in the main office
- Testing the configuration
- How to setup multi-line load-balancing
- Using ISDN for on-demand connections

Overview of Main Office Connection Configuration

The configuration described in this chapter can be implemented with any PortMaster, however, the PortMaster Office Router is used in this example.

The PortMaster Office Router is designed to provide cost-effective connectivity between small remote (branch) offices and larger headquarters (main) offices. These types of connections are typically established on an as-needed basis. For most applications it is not cost-effective to maintain a continuous connection when a connection can be established to transfer network traffic when necessary. These types of connections are usually handled by a dial on-demand link.

A dial on-demand link establishes a connection with the specified location when network traffic is queued. The PortMaster Office Router OR-M is designed to support a dial on-demand connection with another office using the PCMCIA modem port, designated S1. Figure 11-1 shows an example of this configuration. The console port, S0, can be used as a console or an external modem can be connected to provide an additional dial on-demand port for multi-line load-balancing during peak traffic periods.

The PortMaster Office Router-ISDN (OR-U) has an ISDN BRI port designated S1/S2 instead of a PCMCIA modem port. The ISDN port can be used for ISDN dial on-demand connections.

The example in this chapter uses the PCMCIA asynchronous modem port on the OR-M. To use the ISDN port on the OR-U, see "Using ISDN for On-Demand Connections" on page 11-14.

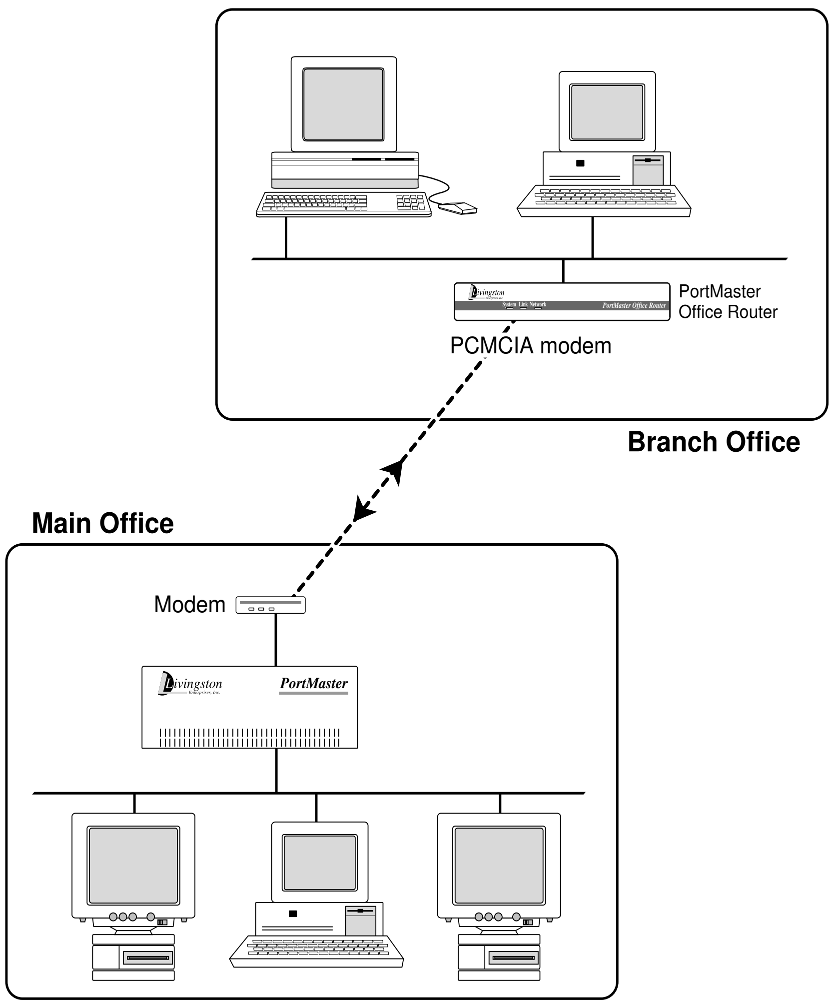

Figure 11-1 Office to Office Dial On-Demand Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster Office Router located in a branch office with a PortMaster of some type in a main office. This connection is initiated on an on-demand basis whenever traffic for the other office is queued at either end. The on-demand connection is configured for dial-in and dial-out operation using the PCMCIA port, S1. The variables shown in Table 11-1 are used in this example. Change variable values to actual values that reflect your network.

Table 11-1 Example Configuration Variables

Variable Description	**Value for this Example**
Name of router in the branch office	branch
IP address of router in the branch office	192.168.200.1
Network type and number	Class C 192.168.200.0
IPX network of router in the branch office	000000F3
IPX Frame Type	IEEE 802.2 on Ethernet
Name of PortMaster router in the main office	hq
IP address of router hq in the main office	192.168.1.1
Network type and number of router hq in the main office	Class C, 192.168.1.0
IPX network of router in the main office	000000F1
IPX network for the serial link	000000F2
Idle Timeout	5 minutes

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the "Troubleshooting" chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch(es) appropriately.**
3. **Connect the power cable.**

4. **Insert the PCMCIA modem card into the PCMCIA slot marked S1.**
5. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.
6. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.
7. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.
8. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
9. **Press [Return] at the password prompt.**
10. **Set the password on the PortMaster by typing:**

```
Command> set password password
```

   This step is optional but highly recommended.

11. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

12. **Set the netmask and broadcast values if necessary.**
13. **Save the address to the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

14. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:

```
Command> quit
```

Configuring the Software on the Router in the Branch Office

In order to use the PMconsole graphical user interface to configure the Office Router, you must install the software on a UNIX workstation or a Microsoft Windows compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 11-2. These values only apply to this example; use values appropriate for your network.

Table 11-2 Global Parameter Values

Parameter	Value
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Sysname	branch

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 11-3.

Table 11-3 Ethernet Parameter Values

Parameter	**Value**
Protocol	PPP/IP/IPX
IPX Network	000000F3
IPX Frame Type	802.2
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the PCMCIA Serial Port Parameters

The PCMCIA modem port on the PortMaster Office Router is designated S1. Configure the port parameters with the values shown in Table 11-4. The PCMCIA modem must be installed in order to configure port S1.

Table 11-4 PCMCIA (s1) Port Parameter Values

Parameter	**Value**
Port Type	Network
Network Type	Dial In&Out (or twoway for command line)
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise. Use the highest DTE speed supported by your modem.
Speed 2	Same as speed 1

Table 11-4 PCMCIA (s1) Port Parameter Values *(Continued)*

Parameter	Value
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Idle Timeout	5 minutes
Dial Group	1

All the other parameters should be left at their default values. For more information about asynchronous ports and configuring your modem, refer to Chapter 6, "Configuring an Asynchronous Port."

Defining a Dial-In User

A user account must be set up on the router in the branch office so the PortMaster in the main office can dial in when traffic is queued at the main office. The new user hq should be configured with the parameter values shown in Table 11-5.

Table 11-5 User Table Parameter Values for User hq

Parameter	Value
User Name	hq
Password	anypasswd (The password must match the password used in the dial script set on the PortMaster in the main office for location branch.) Do not use the same password used for the administrative !root login.
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)

Table 11-5 User Table Parameter Values for User hq *(Continued)*

Parameter	Value
MTU	1500
Compression	On (Unless using multi-line load-balancing.)

For more information about configuring User Table parameters, refer to Chapter 8, "Configuring Dial-In Users."

Defining a Dial-Out Location

A location entry on the PortMaster Office Router in the branch office must be created for the location identified as hq. This allows the Office Router in the branch office to call the PortMaster in the main office when network traffic is queued. The new location hq should be configured with the parameter values shown in Table 11-6.

Table 11-6 Location Table Parameter Values for Location hq

Parameter	Value
Location Name	hq
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP/IP/IPX
IP Destination	Specified 192.168.1.1 (Allows the PortMaster to know when to dial after the Type is switched to On-Demand later.)
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (Unless using multi-line load-balancing.)
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)

Table 11-6 Location Table Parameter Values for Location hq *(Continued)*

Parameter	Value
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	1
Send and Expect Pairs	Send: ATDT5551212\r Expect: CONNECT Send: \r Expect: ogin: Send: branch\r Expect: ssword: Send: anypasswd\r Expect: PPP

For more information about configuring Location Table parameters, refer to Chapter 9, "Configuring Dial-Out Locations."

After the port, user, and location parameters are entered, the port should be reset to make the new configuration active.

Configuring the Software on the PortMaster in the Main Office

In our example, the remote machine is the PortMaster in the main office. To configure this PortMaster to dial the branch office when there is any traffic queued, you must configure the main office exactly the same as the branch office except that the names and addresses are reversed as described in the following subsections.

Setting the Port Parameters

For all ports that you want enabled for dial-in and out to branch, enter the values shown for the parameters in Table 11-7.

Table 11-7 Dial-Out Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Dial In&Out (or twoway for command line)

Table 11-7 Dial-Out Port Parameter Values *(Continued)*

Parameter	**Value**
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual advises otherwise
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Idle Timeout	5 minutes (If you are also using the PortMaster in the main office for user dial in, you want to set this parameter higher or off.)
Dial Group	1

Defining a Dial-In User

A user account must be set up on the PortMaster in the main office so the router in the branch office can dial in when traffic is queued. The new user branch should be configured with the parameter values shown in Table 11-8.

Table 11-8 User Table Parameter Values for User branch

Parameter	**Value**
User Name	branch
Password	anypasswd (The password must match the password used in the dial script set on the PortMaster in the branch office for location hq.) Do not use the same password used for the administrative !root login.
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F2

Table 11-8 User Table Parameter Values for User branch *(Continued)*

Parameter	**Value**
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (Unless using multi-line load-balancing.)

Defining a Dial-Out Location

A location entry on the PortMaster in the main office must be created for the location identified as branch. This allows the PortMaster in the main office to call the PortMaster in the branch office when network traffic is queued. The new location branch should be configured with the parameter values shown in Table 11-9.

Table 11-9 Location Table Parameter Values for Location branch

Parameter	**Value**
Location Name	branch
Type	Manual (The location is set for manual dialing until configuration has been tested. After verification, the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F2
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On (If you are not using multi-line load-balancing.)
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0

Table 11-9 Location Table Parameter Values for Location branch *(Continued)*

Parameter	Value
Send and Expect Pairs	Send: ATDT5551020\r Expect: CONNECT Send: \r Expect: ogin: Send: hq\r Expect: ssword: Send: anypasswd\r Expect: PPP

Reset the port to make the new settings active.

Testing the Setup

The configuration should be tested before either of the locations are set for On-Demand dialing. To test the configuration, follow these steps:

1. **Use the Dialer to connect from branch to hq.**

   If you are using PMconsole, select Dialer from the View menu. Set the Watch Dialer parameter to Yes. If you are using the command line interface, type the following:

```
Command> set console
Command> set debug 0x55
Command> dial hq
```

2. **Monitor the dial and connect sequence between the two locations.**
3. **If everything connects as expected, reset the port on the Office Router in the branch office and change the location Type parameter to On Demand.**

   To reset the port, click the reset button on the Port window or type `reset s1` at the command prompt.

4. **If there is a problem, reset the port on the Office Router in the branch office and change the dial script or other parameters. Dial the main office again. Repeat this procedure until the connection is made correctly.**
5. **Repeat steps 1 through 4, dialing from the main office to the branch office.**

Setting the Console Port for Multi-line Load-balancing

Multi-line load-balancing is used to add additional lines when network traffic is heavy. If more than one line to the same location is established, the PortMaster balances the traffic among the lines. To configure the Office Router for multi-line load-balancing, an external modem must be attached to the console port.

Note – TCP/IP header compression cannot be used with multi-line load-balancing.

In this example the console port is being configured for use as another serial port. Once you set this configuration, the port is no longer used for the system console. Figure 11-2 diagrams the multi-line load-balancing configuration.

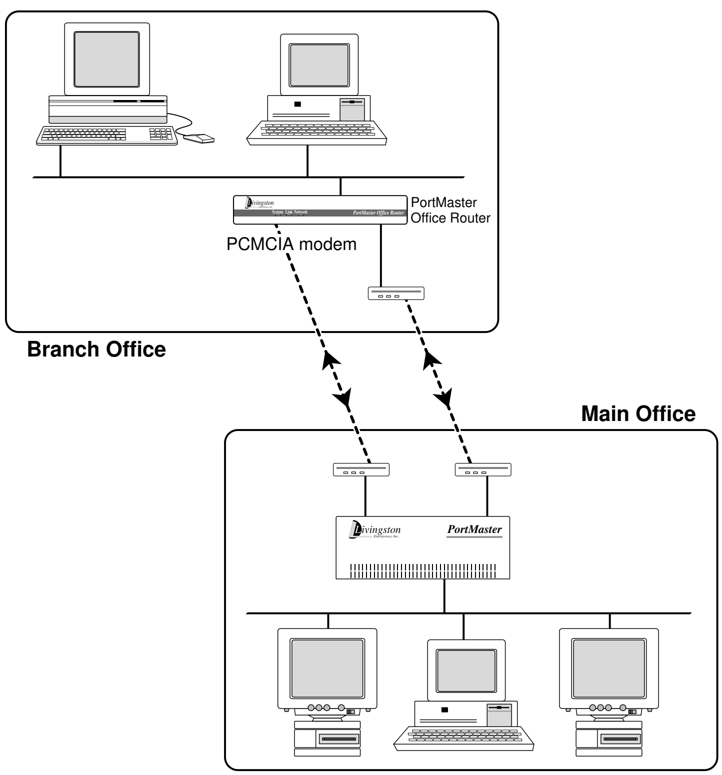

Figure 11-2 Multi-line Load-Balancing

To enable multi-line load-balancing, you must configure the S0 port using the same parameters as shown for the PCMCIA port in Table 11-4. When you configure the location hq on the router in the branch office use the parameter values shown in Table 11-10.

Table 11-10 Location (hq) Parameter Values for Load-Balancing

Parameter	**Value**
Maximum Ports	2
High Water Mark	100 bytes

The value of the High Water Mark parameter depends on the type of traffic and how many queued bytes of traffic you want before the second line is used.

Using ISDN for On-Demand Connections

Using the ISDN BRI port on the PortMaster Office Router-ISDN (OR-U) is very similar to using the PCMCIA port on the OR-M, except you must do the following:

- Configure the ISDN switch type as a global parameter
- Set the SPID on the port
- Do not set the port speed, flow control, or modem control
- Use a V.25bis dialing script in the Location Table setup

For more information about ISDN connections, see Chapter 18, "ISDN Connections" and for information about V.25bis dialing scripts, see Chapter 9, "Configuring Dial-Out Locations."

Connecting Your Office to the Internet 12

This chapter describes how to configure the PortMaster to establish a continuous connection to an Internet Service Provider (ISP). This creates a gateway from your office to the Internet using a dial-out connection through one of the serial ports on your PortMaster. Internet connections can also be set for on-demand operation. For more information about on-demand connections, refer to Chapter 9, “Configuring Dial-Out Locations” and Chapter 11, “Connecting a Branch Office to the Main Office.”

The following topics are discussed:

- Overview of establishing continuous connections
- Setting a dial out Internet connection using a modem port
- Setting a hardwired connection to the Internet using a modem port
- Setting packet filtering

Overview of the Continuous Internet Configuration

Continuous connections from serial ports are used to establish a constant link with another location over a dial up telephone line. In the configurations described in this chapter, the PortMaster is configured for a continuous dial-up connection with an Internet Service Provider (ISP) using dial-up or dedicated lines. Figure 12-1 shows an example of this configuration.

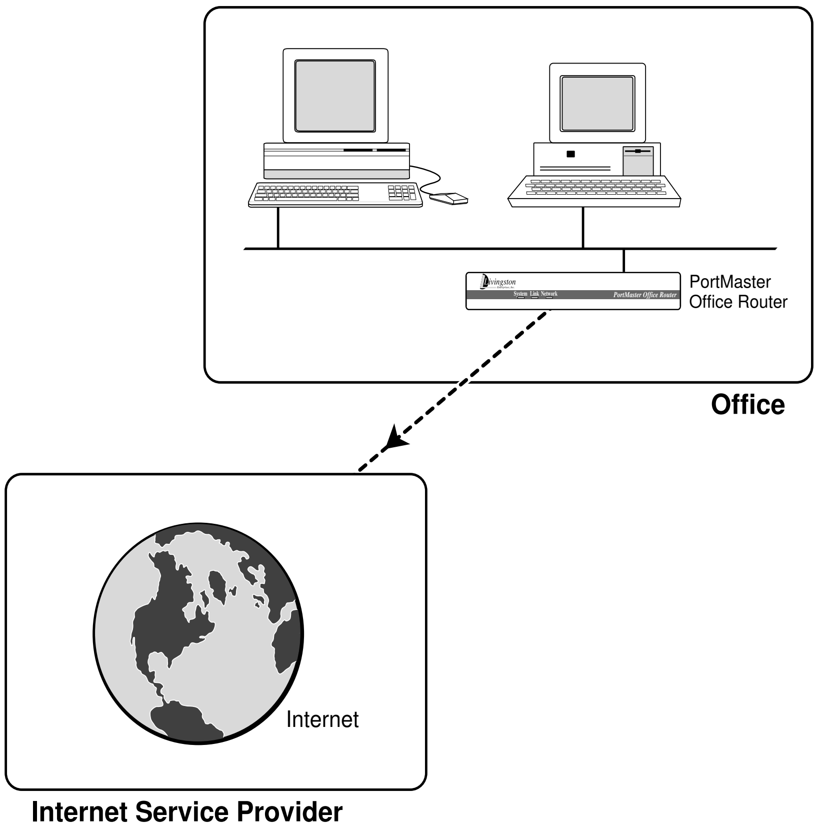

Figure 12-1 Continuous Internet Connection

Description of the Example Configuration

The example described in this chapter connects a PortMaster located in an office with an Internet Service Provider (ISP). If you use a continuous dial-out link from the S1 serial port, one Location Table entry is needed for the ISP. If you use a network hardwired port, no entries are needed in the Location Table.

A continuous dial-out connection starts as soon as the PortMaster boots and is redialed whenever the telephone connection is dropped. The network hardwired configuration is typically used if you are using a leased analog line or an asynchronous to synchronous converter. Both of these configurations are described in this chapter. For this example, IPX packets are not transmitted to or from the Internet Service Provider.

The connection to the ISP can also be configured for dial on-demand operation, as described in Chapter 11, “Connecting a Branch Office to the Main Office.” However, dial on-demand ISP connections do not allow Internet users access to your site when the dial-up connection is not established.

Note – Network connections using synchronous ports are described in Chapters 15 through 18.

The examples shown use the variables listed in Table 12-1. Change these values to reflect your network.

Table 12-1 Example Configuration Variables

Variable Description	Value for this Example
Name of router in office	office
IP address of router in office	192.168.200.1
Network type and number	Class C 192.168.200.0
Timeout for hang up	0 minutes (never hang up)
Network protocol	PPP
IP address of the ISP	192.168.5.6
Name of the ISP	isp

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network DIP switch(es) appropriately.**
3. **Connect the power cable.**
4. **Connect a modem to the serial port you are using for this configuration.**

5. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**
6. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed on the console if the console DIP switch is UP.
7. **Type !root at the login: prompt, then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
8. **Press [Return] at the password prompt.**
9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A message is displayed with the new IP address.
10. **Set the netmask and broadcast values if necessary.**
11. **Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

12. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software on the PortMaster

In order to use PMconsole to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

Setting Global Parameters

Set the name of the system to “office” using the System Name parameter. If you are using PMconsole, this parameter is found in the SNMP Window. Refer to your *Administrator’s Guide* for more information.

Set the Default IP Gateway parameter to the address of your ISP’s router.

For this configuration, none of the other global parameters need to be set. However, you may want to define some of these parameters for your installation.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 12-2.

Table 12-2 Ethernet Port Parameter Values

Parameter	**Value**
Protocol	IP
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet port parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Serial Port Parameters for Dial-Out

For continuous dial out on a serial port, configure the port parameters with the values shown in Table 12-3.

Table 12-3 Serial Port Parameter Values for Continuous Dial Out

Parameter	**Value**
Port Type	Network
Network Type	Dial Out

Table 12-3 Serial Port Parameter Values for Continuous Dial Out *(Continued)*

Parameter	**Value**
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise.
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Dial Group	1

All the other parameters should be left with their default values. For more information about the asynchronous ports and configuring modems, refer to Chapter 6, "Configuring an Asynchronous Port."

Setting the Serial Port Parameters for a Hardwired Connection

To establish a hardwired connection on a serial port, configure the port parameters with the values shown in Table 12-4.

Table 12-4 Serial Port Parameter Values for a Hardwired Port

Parameter	**Value**
Port Type	Network
Network Type	Hardwired
Protocol	PPP
MTU	1500
Speed 1	Use 115200 if the attached device supports this speed. Otherwise, use the speed suggested by the device manual.
Modem Control	On (If using a modem or CSU/DSU.) Off (If using a direct physical connection.)
Flow Control	RTS/CTS

Table 12-4 Serial Port Parameter Values for a Hardwired Port *(Continued)*

Parameter	**Value**
IP Destination	192.168.5.6
Netmask	255.255.255.0 for a Class C address
Routing	Typically Off; however, your ISP may request that you set this parameter to Broadcast.
Compression	Enabled

All the other parameters should be left with their default values. For more information about asynchronous ports, refer to Chapter 6, "Configuring an Asynchronous Port."

Defining a Dial-Out Location

If you are using a continuous dial-out link, a location entry on the PortMaster must be created for the location identified as isp. This allows the PortMaster to establish a connection with the Internet Service Provider as soon as it is booted. The new location isp should be configured with the parameter values shown in Table 12-5, or as instructed by your ISP.

Table 12-5 Location Table Parameter Values for Location isp

Parameter	**Value**
Location Name	isp
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified, change the Type to Continuous.)
Protocol	PPP
IP Destination	Specified 192.168.5.6
Netmask	255.255.255.0
Routing	Typically Off; however, your ISP may request that you set this parameter to Broadcast.
MTU	1500
Compression	On (If you are not using multi-line load-balancing.)

Table 12-5 Location Table Parameter Values for Location isp *(Continued)*

Parameter	**Value**
Input Filter	internet.in
Output Filter	internet.out (if needed)
Idle Timeout	0
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	1
Send and Expect Pairs	Send: ATDT5551212\r Expect: CONNECT Send: \r Expect: ogin: Send: office\r Expect: ssword: Send: passwd\r Expect: PPP

Note – The strings you send following the login: and password: prompts must be provided to you by your ISP. Your chat script may differ from this example depending on your ISP.

You can also authenticate using CHAP if it is supported by the ISP. To use CHAP authentication, use only the first Send and Expect string in the chat script shown above. You must also create a user called "isp" with the password "passwd." For more information about configuring users, refer to Chapter 8, "Configuring Dial-In Users." For more information about configuring Location Table parameters, refer to Chapter 9, "Configuring Dial-Out Locations."

After the configuration is entered and saved, the port should be reset to make the new settings active.

Testing the Continuous Dial-Out Setup

The configuration should be tested before the location isp is set for continuous dialing. To test the configuration, follow these steps:

1. **Use the Dialer to connect to the ISP.**

   Select Dialer from the PMconsole View menu. Set the Watch Dialer parameter to Yes. If you are using the command line interface, type: `dial isp -x`

2. **Monitor the dial and connect sequence between the two locations.**

3. **If everything connects as expected, reset the port and change the Location Type parameter to Continuous.**

4. **If there is a problem, reset the port and change the dial script or other parameters. Dial the ISP again. Repeat this procedure until the connection is made correctly.**

   Contact your ISP if you are unable to connect as expected. They may be able to provide additional information.

Note – You may need to get specific dial script examples from the ISP before configuring the location.

Testing the Network Hardwired Setup

To test the configuration, follow these steps:

1. **Reset the newly configured serial port.**

   The network hardwired connection should be established within a few seconds.

2. **Verify that the connection becomes ESTABLISHED.**

   Use the `show s1` command (if you are using port s1).

3. **If there is a problem, check your configuration.**

   Contact your ISP if you are unable to connect as expected.

Setting Network Filtering

Your connection to the Internet can be vulnerable to attack from other Internet users. Therefore, it is recommended that you add an input filter to the location isp for the continuous dial-out connection. For a hardwired connection, the input filter can be attached to the hardwired port.

Note – This section describes an example filter that may not protect your network from all forms of attack. For more information about filters, refer to “References” and Chapter 10, “Configuring Filters.”

The filter named internet.in is written as follows:

```
deny 192.168.200.0/24 0.0.0.0/0 log
permit tcp estab
permit 0.0.0.0/0 mail.edu.com/32 tcp dst eq smtp
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq ftp
permit 0.0.0.0/0 www.edu.com/32 tcp dst eq www-http
permit tcp src eq ftp-data dst gt 1023
permit udp dst eq domain
permit tcp dst eq domain
permit icmp
```

Table 12-6 describes the filter.

Table 12-6 Description of Internet Filter

Rule	Description
1	Deny any incoming packets claiming to be from your own network (192.168.200.0). This blocks IP spoofing attacks and logs the attempt.
2	Permits already established TCP connections.
3	Permits SMTP connections to the mail server mail.edu.com.
4	Permits FTP to the host ftp.edu.com.
5	Permits WWW http connections to the web server www.edu.com.
6	Permits FTP data channel.

Table 12-6 Description of Internet Filter *(Continued)*

Rule	**Description**
7	Permits Domain Name Service.
8	Permits Domain Name Service zone transfers. (You may wish to restrict this rule to allow only connections to your name servers.)
9	Permits ICMP packets.

If your Domain Name Server is outside your local network, refer to "Domain Name Server is Outside Your Local Net" on page 10-16.

Using ISDN for Internet Connections

Using the ISDN BRI port on the PortMaster Office Router-ISDN (OR-U) is very similar to using the PCMCIA port on the OR-M, except you must do the following:

- Configure the ISDN switch type as a global parameter
- Set the SPID on the port
- Do not set the port speed, flow control, or modem control
- Use a V.25bis dialing script in the Location Table setup

For more information about ISDN connections, see Chapter 18, "ISDN Connections" and for information about V.25bis dialing scripts, see Chapter 9, "Configuring Dial-Out Locations."

Configuring User Dial-In Access 13

This chapter describes how to use the PortMaster to allow users access to centralized hosts and networks. This application is used by Internet Service Providers, academic environments, and corporate telecommuters. In this configuration multiple asynchronous ports are configured with modems for answering incoming calls from users who will then access a networked host connected via Ethernet to the PortMaster.

The following topics are described:

- Overview of the login user configuration
- Description of hardware configuration
- Description of an example software configuration on the PortMaster

Overview of Dial-In User Configuration

The PortMaster configuration described in this example allows up to seven 30 port PortMasters to be connected together to provide up to 210 dial-in asynchronous ports. The PortMaster communications server allows dial-in users to access a host for shell accounts and/or PPP, SLIP, or CSLIP connections. Internet Service Providers can use this example to configure their PortMasters to allow host and network access by dial-in users. The number of ports used is a function of the number of expected subscribers; one port per ten subscribers is the typical ratio, but peak usage and average usage per port should be monitored closely to determine the need for additional ports. RADIUS Accounting can help you to evaluate port usage. See the *RADIUS Administrator's Guide* for more information.

The same application can be used by companies to allow remote users access to their own accounts on the corporate network. Once users are authenticated they can access network resources as if they were connected to the corporate network directly.

Although this example uses seven PortMasters, many more can be used. With more than seven PortMasters, the configuration is the same except that the assigned pools would be arranged differently.

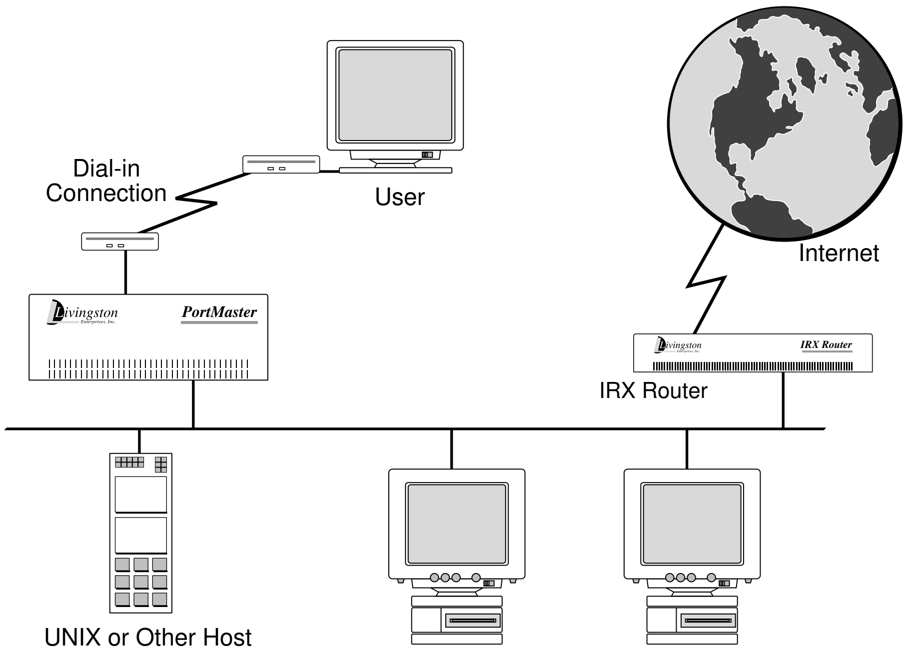

Figure 13-1 Login User Configuration

Description of Sample Configuration

The Internet Service Provider example described in this chapter uses the values shown in Table 13-1. Change variable values to actual values that reflect your network.

Table 13-1 Example Configuration Variables

Variable Description	Value for this Example
Address type	Class C assigned by your provider
Class C IP network	192.168.1.0
IP address and name of router connecting to the Internet	192.168.1.1 (gw.edu.com)
IP address and name of host running RADIUS	192.168.1.2 (rk2.edu.com)

Table 13-1 Example Configuration Variables *(Continued)*

Variable Description	**Value for this Example**
IP address and name of host running DNS	192.168.1.2 (rk2.edu.com)
IP address of RADIUS accounting server	192.168.1.2 (rk2.edu.com)
IP address of RADIUS backup accounting server	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host running backup RADIUS	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host that shell users log into	192.168.1.4 (rk4.edu.com) (Optional)
IP addresses reserved for future hosts	192.168.1.5-15, 23-32
IP address and name of first PortMaster	192.168.1.16 (pm1.edu.com)
IP addresses and names for additional PortMasters	192.168.1.17-22 (pm2.edu.com through pm7.edu.com)
Reserved pool of assigned addresses for PortMaster 1	192.168.1.33-62
Reserved pool of assigned addresses for PortMaster 2	192.168.1.65-94
Reserved pool of assigned addresses for PortMaster 3. Continue until PortMaster 7.	192.168.1.97-126
Reserved pool of assigned addresses for PortMaster 7	192.168.1.225-254

You can set the assigned pools a little closer together as long as they do not overlap, however, having the pools fall within bit boundaries makes packet filters easier to write.

Note – This example assumes you are using a PM-2E-30 PortMaster. If you are using a PM-25, the assigned pools can be moved closer together.

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the "Troubleshooting" chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switches appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.
5. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics as it boots. The self diagnostics are displayed to the console if the console DIP switch is UP. Booting takes less than one minute.
6. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.
7. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
8. **Press [Return] at the password prompt.**
9. **Set the IP address of the new PortMaster by typing:**

```
Command> set address 192.168.1.16
```

   In this example, 192.168.1.16 is the IP address of the first PortMaster (pm1.edu.com). A confirmation message is displayed showing the new IP address.
10. **Set the netmask if it is not 24 bits and set the gateway if you need to assign a default gateway.**

11. Save the address in the nonvolatile memory of the PortMaster by typing:

```
Command> save all
```

12. Exit the command mode by typing:

```
Command> quit
```

13. Connect your modems to the serial ports using straight-through modem cables.

V.34 modems that are capable of 28.8Kbps are best but V.32bis modems that run at 14.4Kbps also work. Modems slower than 14.4Kbps work but are not recommended for network users.

14. Make sure that the modem cables are securely fastened and that there is enough room for the modems to stay cool.

Configuring the Software on the PortMaster

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster address is set.

The UNIX version of PMconsole includes the `pmcommand` utility that allows you to define a command script and upload the script to the PortMaster. This utility is useful when you are performing the same configuration on multiple PortMasters.

Note – This example describes how to configure the first PortMaster pm1.edu.com. Use a similar configuration for the remaining PortMasters.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 13-2.

Table 13-2 Global Parameter Values

Parameter	**Value**
Default Host	192.168.1.4
Alternate Host	any other shell host, if available
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Name Service	DNS
Name Server	192.168.1.2
Domain	edu.com
Sysname	pm1
Loghost	192.168.1.2
Assigned Address	192.168.1.33

For more information about global parameters, refer to Chapter 4, “Configuring a PortMaster.”

Setting the RADIUS Parameters

RADIUS is usually implemented for user authentication when there are multiple PortMasters and more than a few dozen users. Only a few hundred users can be configured in the User Table and stored in the nonvolatile memory of the PortMaster. This example assumes the use of RADIUS.

The RADIUS parameters are given in Table 13-3, however for information about RADIUS and its parameters, refer to the *RADIUS Administrator's Guide* or FTP from `ftp://ftp.livingston.com/pub/livingston/radius/radius.install`.

Table 13-3 RADIUS Parameter Values

Parameter	Value
Secret	anyvalue (Must be the same secret for pm1.edu.com in the `/etc/raddb/clients` file on the RADIUS server.)
Authentication Server	192.168.1.2
Alternate Authentication Server	192.168.1.3 (optional) This server must have an identical RADIUS database.
Accounting Server	192.168.1.2
Alternate Accounting Server	192.168.1.3 (optional) This must be another RADIUS server.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 13-4.

Table 13-4 Ethernet Parameter Values

Parameter	Value
IP Address	192.168.1.16
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Asynchronous Port Parameters

The serial modem ports are designated S0 through S29 on the PortMaster. If you are using PMconsole, you can configure one port and clone the configuration to the other serial ports. If you are using the command line interface, use the `set all` command to set the same values for each of the serial ports. The port parameters shown in Table 13-5 can be set on all asynchronous ports. Use the Modem Table described in Chapter 6, “Configuring an Asynchronous Port” to configure the attached modems or set each port as a host device as described in Chapter 14, “Configuring the PortMaster to Access Shared Devices” and configure each modem individually.

Note – V.34 modems should lock the DTE rate at 115200 bps unless the modem manual instructs otherwise. V.32bis modems should lock the DTE rate at 57600 bps. Use the fastest DTE interface speed supported by your modem.

A list of modems and their initalization strings is found in Table 6-6 on page 6-14. The recommended configuration has the modem do the following:

- Raise carrier when a call comes in
- Reset itself when DTR is dropped
- Lock the DTE rate
- Use hardware flow control (RTS/CTS)

If you have already configured your modems on another machine, you should connect to the modem through the PortMaster and set the modem back to the factory default. Then use the recommended modem string to properly configure each modem.

Table 13-5 Serial Port Parameter Values for All Ports

Parameter	Value
Port Type	Login Network
Network Type	Dial In
Security	On
Modem Type	(set to your modem type)

Table 13-5 Serial Port Parameter Values for All Ports *(Continued)*

Parameter	**Value**
The following five parameters are set by the Modem Table when you reset the port, provided the port has its default setting.	
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS

Once all of the ports are configured as shown above, save and reset all of the ports.

Defining a Dial-In Login User

Note – The instructions in this section are only used if you are not using RADIUS and you are not using pass-through logins.

A user account must be set up on the PortMaster for each authorized user. Each new user user1 should be configured with the parameter values shown in Table 13-6.

Table 13-6 User Table Parameter Values for user1

Parameter	**Value**
User Name	user1
Password	passwd
User Type	Login/Normal
Host	Default
Login Service	PortMaster (if the `in.pmd` daemon is running on the default host, otherwise select “rlogin”)

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-In Network User

Note – The instructions in this section are only used if you are not using RADIUS.

A user account must be set up on the PortMaster for each authorized network user. Each new user user2 should be configured with the parameter values shown in Table 13-6.

Table 13-7 User Table Parameter Values for user2

Parameter	**Value**
User Name	user2
Password	passwd (any)
User Type	Network/Normal
Protocol	PPP/IP
Address Type	Assigned
Compression	On
Routing	Off

You can also use SLIP or CSLIP instead of PPP, refer to Chapter 8, “Configuring Dial-In Users” for more information about this configuration.

Configuring the PortMaster to Access Shared Devices 14

This chapter describes how to use the PortMaster to connect from networked hosts to shared devices connected to the PortMaster. This type of connection is designed to allow access to modems, printers, and other RS-232 devices.

The following topics are described:

- Overview of shared device configurations
- Description of hardware configuration
- Description of general software configuration
- Description of the specific software configurations for each application
- Testing the configuration

Overview of Shared Device Configurations

There are two methods of accessing shared devices on the PortMaster. The first method requires a UNIX host that supports the PortMaster `in.pmd` daemon. With this daemon, you can configure ports as host devices and access them as pseudo-tty from the host using tip, UUCP, and other applications.

Alternatively, you can configure the ports as network devices and access them using telnet, rlogin, or a clear channel TCP connection (netdata).

Host Device Configuration

One of the functions of a communications server is to provide network users access to shared devices such as printers and modems. This can be done if the port connected to the printer or modem is configured as a host device port. This configuration is also useful for tip and UUCP services.

Once a port is defined as a host device, the device service is configured as PortMaster, and a pseudo-tty is chosen for the port. The host device port can now be accessed by establishing a pseudo-tty connection to the port from a UNIX host with the PortMaster daemon software installed. In this case, the port operates as a host-controlled device. Figure 14-1 shows a diagram of the host device configuration using the PortMaster device service and a pseudo-tty connection.

Once the port type is set as host device, the device service must be selected and the host name entered either for the port, or as the global default host. If the device service is set to PortMaster for pseudo-tty operation, a host name and pseudo-tty must be specified. The PortMaster `in.pmd` daemon must be installed on the specified host in order to use the PortMaster device service.

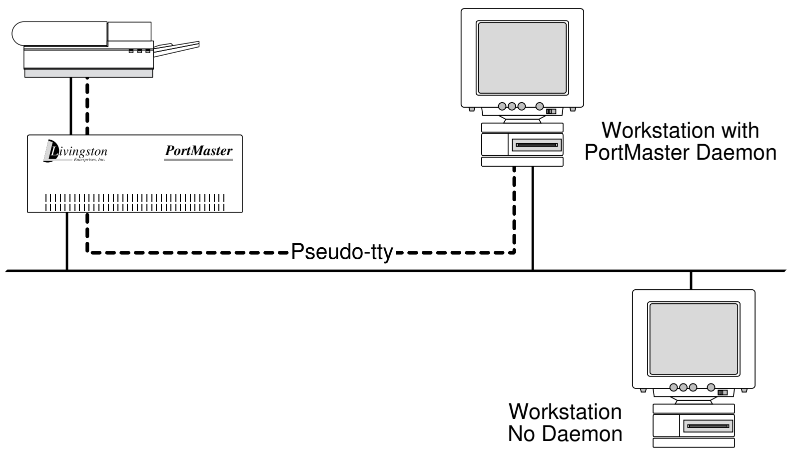

Figure 14-1 Host Device Configuration

In this configuration, a workstation with `in.pmd` installed can access a printer attached to a PortMaster port as though it was attached to the workstation even if the printer is on the other side of the country.

Network Device Configuration

This configuration sets the port for host device access but uses the rlogin, telnet, or netdata device service to access the attached device. In this configuration the host device name is set as `/dev/network`. This configuration is used in cases where users want to telnet or rlogin to the shared device from multiple hosts or from a host that does not support `in.pmd`. Figure 14-2 shows an example of the network device configuration.

The network user configuration is most commonly used to allow a telnet session with the device attached to a specified PortMaster port. The example in this chapter sets ports for network access so the administrator can telnet to each modem connected to a

PortMaster port for configuration purposes. In this application, each port is identified by a unique port number assigned during the configuration process. You can also configure a pool of ports at a single TCP port number.

The netdata (TCP clear) device service is most often used when you want to have a custom application open a TCP connection to an RS-232 device, or to connect two serial devices across a network.

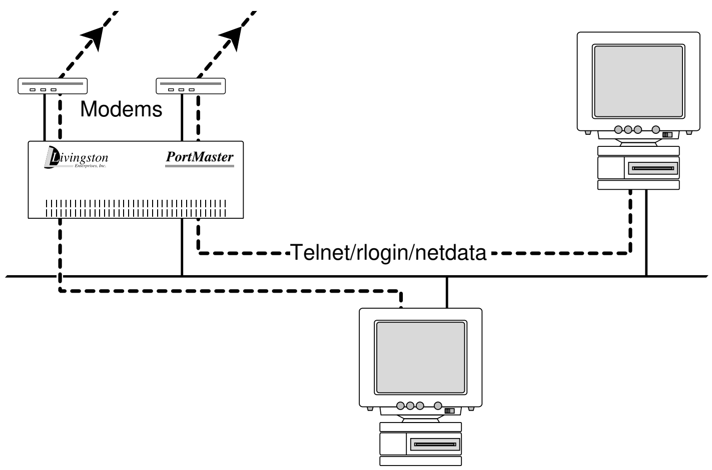

Figure 14-2 Network Device Configuration

Description of Sample Configuration

The example described in this chapter allows a user to dial into port S2 on the PortMaster to login to a workstation, and access a serial printer attached to port S9, as `/dev/ttyre`, using the PortMaster device service. The workstation user would also like to access port S2 as `/dev/ttyrf` when it is not being used for login service.

The modem attached to port S2 is connected with a straight-through cable and uses hardware flow control and carrier detect. The DTE rate between the modem and the PortMaster is locked.

In order to use the PortMaster login or device service, the workstation user must install the PortMaster daemon, `in.pmd` in the `/usr/etc` directory and modify the `/etc/services` and `/etc/inetd.conf` files to tell the workstation where to find `in.pmd`. You must also add `/dev/ttyrf` to the `/etc/remote` file and `/dev/ttyre` to the `/etc/printcap` file.

Change the variable values shown in Table 14-1 to actual values that reflect your network.

Table 14-1 Example Configuration Variables

Variable Description	**Value for this Example**
Name of PortMaster	pm
IP address of PortMaster	192.168.200.1
Default Host	192.168.200.2 (the workstation)
Speed of modem	28800 bps (DTE rate 115200 bps)
Host device on S2 (modem)	/dev/ttyrf
Host device on S9 (printer)	/dev/ttyre
Speed of printer	9600 baud

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch(es) appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.

7. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. **Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

11. **Exit the command mode by typing:**

```
Command> quit
```

12. **Attach the modem to port S2 with a straight-through cable.**

13. **Attach the printer to port S9 with a null modem cable if the printer is a DTE device.**

    Pinouts for both cables are given in the *Hardware Installation Guide*.

Configuring the Software for Shared Device Applications

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible PC. Once the software is installed and started according to the instructions in the appropriate *Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using telnet once the PortMaster address is set.

Setting the Global Parameters

Set the name of the system to pm using the System Name parameter. If you are using PMconsole, the parameter is found in the SNMP window. Refer to your *Administrator's Guide* for more information. Set the Default Host parameter to 192.168.200.2 using the Global Parameter window. You can also set the host for ports S2 and S9 to 192.168.200.2 if you plan to use the other ports for some other host. Set other global parameters that apply to your installation.

Setting the Ethernet Port Parameters

Set the following Ethernet parameters to the values shown in Table 14-2.

Table 14-2 Ethernet Parameter Values

Parameter	Value
Protocol	PPP/IP
IP Address	192.168.200.1
Netmask	255.255.255.0
Broadcast Address	high (192.168.200.255)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, "Configuring the Ethernet Interface."

Setting the TwoWay Serial Port (S2) Parameters

In our example, the workstation user wants to dial in to port S2 sometimes and tip out to the modem connected to port S2 at other times. Configure the S2 port parameters with the values shown in Table 14-3.

Table 14-3 Serial Port Parameter Values (S2)

Parameter	**Value**
Port Type	User Login and Host Device (or twoway for command line)
Host Device	/dev/ttyrf
Speed 1	Use 57600 for V.32bis modems and 115200 for V.34 modems, unless your modem manual instructs otherwise.
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	RTS/CTS
Host	Default (or 192.168.200.2)
Security	Off (if Security is On, you must configure the User Table or RADIUS)
Login Service	PortMaster
Device Service	PortMaster

All the other parameters should be left at their default values. Once all of the ports are configured as shown above, save and reset all of the ports. For more information about asynchronous ports, refer to Chapter 6, “Configuring an Asynchronous Port.”

Setting the Serial Printer Port (S9) Parameters

In our example, a serial printer is connected to port S9. Configure the S9 port parameters with the values shown in Table 14-4. If the printer is a DTE use a null modem cable to connect to the port.

Table 14-4 Serial Port Parameter Values (S9)

Parameter	**Value**
Port Type	Host Device
Host Device	/dev/ttyre
Speed 1	9600
Speed 2	Same as speed 1
Speed 3	Same as speed 1
Modem Control	On
Flow Control	Xon/Xoff
Host	Default (or 192.168.200.2)
Device Service	PortMaster

Once all of the ports are configured as shown above, save and reset all of the ports. The workstation printer subsystem should now be able to send printer jobs to `/dev/ttyre` and reach the printer.

Setting the Parallel Port (P0) Parameters

The parallel port P0 can be used to access a printer. To configure the P0 port for a printer, use the values shown in Table 14-5.

Table 14-5 Parallel Port Parameter Values (P0)

Parameter	**Value**
Port Type	Host Device
Host Device	/dev/ttyre

Table 14-5 Parallel Port Parameter Values (P0) *(Continued)*

Parameter	Value
Host	Default (or 192.168.200.2)
Device Service	PortMaster

Configuring a Network Device for Telnet Access

To access modems or other devices attached to PortMaster ports using telnet, use the general configuration given earlier in this chapter but use the parameters shown in Table 14-6.

Table 14-6 Serial Port Values to Allow a Telnet Connection to Ports S0-S29

Parameter	Value
Port Type	Host Device
Host Device	/dev/network
Modem Control	Off
Device Service	Telnet 6000 through 6029 for ports S0 through S29

To access port S1 using telnet from your host, type:

```
% telnet pm1 6001
```

Where pm1 is the host name of the PortMaster you are accessing and 6001 is the TCP port set for the port you are accessing. You can also set several ports to the same TCP port to create a pool of ports available for telnet access.

Note – If you are using this configuration to configure your modems, see “Configuring Modems and Modem Parameters” on page 6-13 first.

Synchronous Leased Line Connections 15

This chapter describes how to use the PortMaster to connect to a synchronous leased line at speeds up to T1 (1.544 Mbps) or E1 (2.048 Mbps). This chapter also describes how to configure a dial backup connection for your synchronous line.

The following topics are described:

- Overview of the leased line configuration
- Description of hardware configuration
- Description of the software configuration for a leased line
- Testing the configuration

Overview of the Leased Line Configuration

PortMasters support leased line connections using synchronous ports and the PPP protocol. In this configuration one PortMaster is usually connected to another PortMaster or other router over a leased line where each router uses its own Ethernet address for the serial link (known as "IP unnumbered") and the address of the other end is discovered dynamically. In this way a dedicated high-speed connection is established between two routers located in separate sites. The leased line connection requires a CSU/DSU and a carrier that provides external clock. Figure 15-1 shows an example of the leased line connection.

If you are connecting two networks together for the first time you should make sure first that there are no conflicts in the network numbering; that is, make sure that the two networks are not using the same subnet twice in different locations. For more information on network numbers and subnetting see "Network Addressing" on page 2-1.

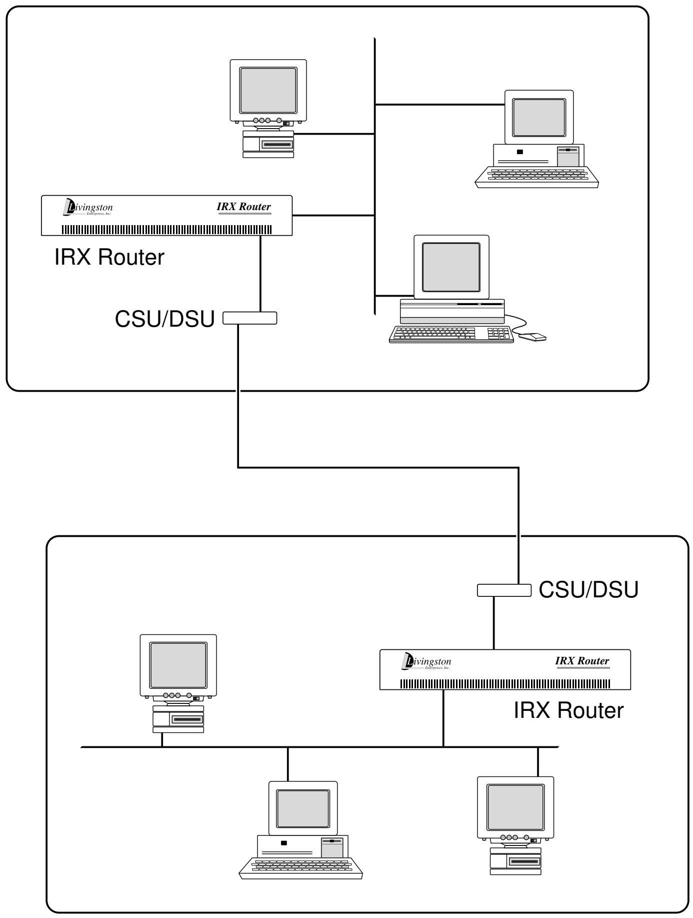

Figure 15-1 Leased Line Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster router located in one office with a PortMaster router located in another office using a dedicated leased line. The variables shown in Table 15-1 are used in this example. Change variable values to reflect the actual values for your network.

Table 15-1 Example Configuration Variables for Leased Line Connections

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the "Troubleshooting" chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**
3. **Connect the power cable.**

4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.

5. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.

6. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.

7. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.

8. **Press [Return] at the password prompt.**

9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

10. **Set the netmask and broadcast values if necessary.**

11. **Save the address in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

12. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software for a Leased Line Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate PMconsole Administrator's Guide, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

In the leased line configuration described in this section, the Ethernet address of the PortMaster is used as the address for the serial link and the CSU/DSU must provide external clock or pass external clock from the carrier. Since the PortMaster always uses external clock, you do not need to set the speed on the synchronous port, the port speed is whatever the carrier sends. If you choose to set a speed it is for documentation purposes only; the speed is ignored by the PortMaster.

Note – The PortMaster also supports numbered IP interfaces on leased lines, but this is not recommended since it wastes IP address space.

Setting the Global Parameters

Set the following global parameters to the values shown in Table 15-2. These values only apply to this example. Use values appropriate for your network.

Table 15-2 Global Parameter Values

Parameter	**Value**
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast and Listen
Name Service (optional)	DNS
Name Server (optional)	192.168.200.2
Sysname	office1

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Interface Parameters

Set the following Ethernet parameters to the values shown in Table 15-3.

Table 15-3 Ethernet Parameter Values

Parameter	**Value**
Protocol	IP/IPX (or IP)
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1 (if you are using IPX)
IPX Frame Type	802.2 (if you are using IPX)
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, "Configuring the Ethernet Interface."

Setting the Synchronous Port Parameters for a Leased Line Connection

Configure the WAN port parameters with the values shown in Table 15-4 for this example only.

Table 15-4 WAN Port Parameter Values

Parameter	**Value**
Port Type	Network
Network Type	Hardwired
Transport Protocol	PPP
Port IP address	Unnumbered (0.0.0.0)
IP Destination	192.168.1.1 (or Negotiated)
Netmask	255.255.255.0

Table 15-4 WAN Port Parameter Values *(Continued)*

Parameter	**Value**
IPX Network	000000F3
Line Speed	Speed is a comment only, the actual speed is set by the external clock
Modem Control	On or Off depending on the CSU/DSU configuration
Routing	On (Broadcast and Listen)
MTU	1500

If you are not sure of the IP address on the other end of the connection, you can set the IP Destination parameter to Negotiated (255.255.255.255).

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, "Configuring a Synchronous WAN Port."

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. However, if you are having problems use the information in this section to debug your configuration.

If you are having trouble with a leased line connection, verify the following:

- Use the following commands to view the PPP negotiation on port S1, if this is the port you are using:

```
Command> set console
Command> set debug 0x51
Command> reset s1
```

  For more information about the interpreting the results of the debug command, refer to "Interpreting LCP and IPCP Debug Output" on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0x0
Command> reset console
```

- The error counters should be 0 except for abort errors. If your counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cable and it is attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch next to the synchronous port is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing clock to the PortMaster. The CSU/DSU can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- If you have a Cisco router on the other end of your connection, it must be running software release 9.14(5) or later and use PPP encapsulation not hdlc.
- If the framing errors are greater than 0, verify that the router on the other end of the connection is running the PPP protocol.
- If you are still having problems, set the following:

```
Command> set debug 0x51
Command> set console
```

Then set the CSU/DSU for local loopback. You should see the following message:

```
LCP_APPARENT_LOOP
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4.

- If the local loopback works, take the CSU/DSU out of loopback and set line loopback on the remote CSU/DSU. You should see the same result. If you do not, the problem is either in the configuration of one of the CSU/DSU’s or in the line itself.
- When you have finished, turn off debugging by typing:

```
Command> set debug 0
Command> reset console
```

- Contact your carrier to review your configuration and the status of their line.

Synchronous Frame Relay Connections 16

This chapter describes how to use the PortMaster to connect to a synchronous line using Frame Relay.

The following topics are described:

- Frame Relay terms
- Overview of the Frame Relay configuration
- Description of hardware configuration
- Description of the software configuration for Frame Relay
- Testing the configuration

Frame Relay Terms

Frame Relay uses several special terms that have created a large amount of confusion because of the differences between Frame Relay and other traditional telecommunications methods. In this section, the technology behind Frame Relay is described briefly, and special terms which are defined in the glossary are highlighted in **bold print**.

Frame Relay is a switched digital service, which supports multiple **virtual circuits** being simultaneously connected to a site by a single **physical circuit**. The principle is that a site connects via a physical circuit to a Frame Relay network or cloud. Each site requires only one physical circuit into the cloud, but can have as many virtual circuits as necessary to reach any other sites attached to the cloud. It is possible for Frame Relay to support Switched Virtual Circuits (**SVC**s) or Permanent Virtual Circuits (**PVC**s) but the PortMaster (and most communications providers) only support PVCs. A PVC is used to connect any point A attached to the network to any other point B attached to the network. Each PVC is given a unique number on each physical circuit in the path from point A to point B. This number is called a **DLCI** (Data Link Channel Identifier). The DLCI is automatically changed as it passes through each switch in the path to the number for the PVC on the next physical circuit in the path. Generally, the only two DLCI numbers the customer ever sees are the ones used on the physical circuits at each end. Other numbers are usually kept internal to the telecommunications provider. A DLCI is different from a network address, in that it identifies a circuit in both directions, not a particular endpoint. That is, a frame contains only one DLCI, not a source and destination.

The physical circuit between point A and the network must be ordered with a certain **line speed**. This is the physical maximum bandwidth for your connection to the Frame Relay network. Expansion beyond this limit is not possible without a hardware change, and a new circuit installation.

The connection into the telecommunications provider's Frame Relay network must be ordered at a particular **port speed**, which is the maximum bandwidth rate that the telecommunications provider accepts from your connection. This number must be less than or equal to the line speed. This speed is the maximum rate at which you can transmit data to any of your PVCs under any circumstances. The port speed differs from line speed only in that it can be upgraded through software without a circuit installation or hardware change.

Each PVC has a property known as Committed Information Rate (**CIR**), which represents the guaranteed minimum bandwidth available to the particular PVC under all conditions. In some implementations, an additional property can be assigned to a PVC, known as "burst speed" or "maximum burst". This speed represents the highest rate at which data is allowed to flow over a given PVC regardless of bandwidth availability.

The PortMaster pushes as much data out of the serial port as it can at port speed for any PVC that has traffic, regardless of CIR. The Frame Relay switch passes as much of the data as possible on to the next link. However, once a particular PVC has transmitted its CIR worth of bits each second, the switch marks any additional frames as "Discard Eligible". If the switch receives more frames than it can pass along, the frames are automatically discarded in the following order:

- Frames that would be marked Discard Eligible even if they are forwarded
- Frames received that were marked as Discard Eligible
- If the switch must discard other frames, the behavior is undefined. In this case, the Frame Relay network is improperly configured because the CIR total exceeds the line speed or port speed.

When ordering Frame Relay service for a private network, it is generally best to order large bandwidth physical circuits (T1), with port speed appropriate to the application, and a CIR that is just barely high enough to provide minimally acceptable performance for your application. Remember, in most cases you usually get close to your port speed. The CIR is a guaranteed minimum throughput, not a maximum limit. Port speed is the maximum limit.

The following Frame Relay terms relate to network management. The Frame Relay specification supports automatic network status updates, which are exchanged between adjacent devices in the Frame Relay network. These status updates are known as Local Management Interface (**LMI**). There are two forms of LMI available in the Portmaster. Cisco/Stratacom LMI, which is commonly referred to as LMI, and ANSI T1.617 Annex D LMI, which is commonly referred to as **Annex-D**. Generally, your telecommunications provider offers three options for LMI on your physical circuit: LMI, Annex-D, or none. LMI is only between your router and the switch to which your physical circuit connects. Therefore, it does not matter what the remote ends of any of your PVCs are using. However, it is important that your circuit LMI matches the configuration on your PortMaster. Generally, Annex-D is recommended, since it is a more feature-rich and robust version of LMI.

Overview of the Frame Relay Configuration

Frame Relay is a method of encapsulating network information that allows for fast delivery and high line utilization. PortMasters support Frame Relay over synchronous ports. The PortMaster IRX supports speeds up to T1/E1 on ports S1 and S3. The IRX also supports speeds up to 64Kbps on ports S2 and S4. The PortMaster PM-2R series supports up to T1/E1 speeds on the W1 port.

Frame Relay is configured by selecting the Frame Relay protocol, setting the IP address of the port, and specifying the Data Link Connection Identifiers (DLCIs) during the synchronous port configuration. The PortMaster can also discover DLCIs dynamically and learn the IP addresses of the other routers through inverse ARP if you use either LMI or Annex-D keepalives and the other routers on your Frame Relay cloud support inverse ARP as specified in RFC 1490. Both LMI and Annex-D keepalives are supported on PortMasters. In this configuration, the PortMaster sends an LMI status request every 10 seconds (default). Every sixth request is a full status request, the others are keepalives. In this configuration the port state is CONNECTING until it receives replies from the switch, then the port state becomes ESTABLISHED. After six unanswered requests, the PortMaster resets the port. Figure 16-1 shows an example of a Frame Relay connection.

Note – All synchronous ports require external clock to regulate the port speed.

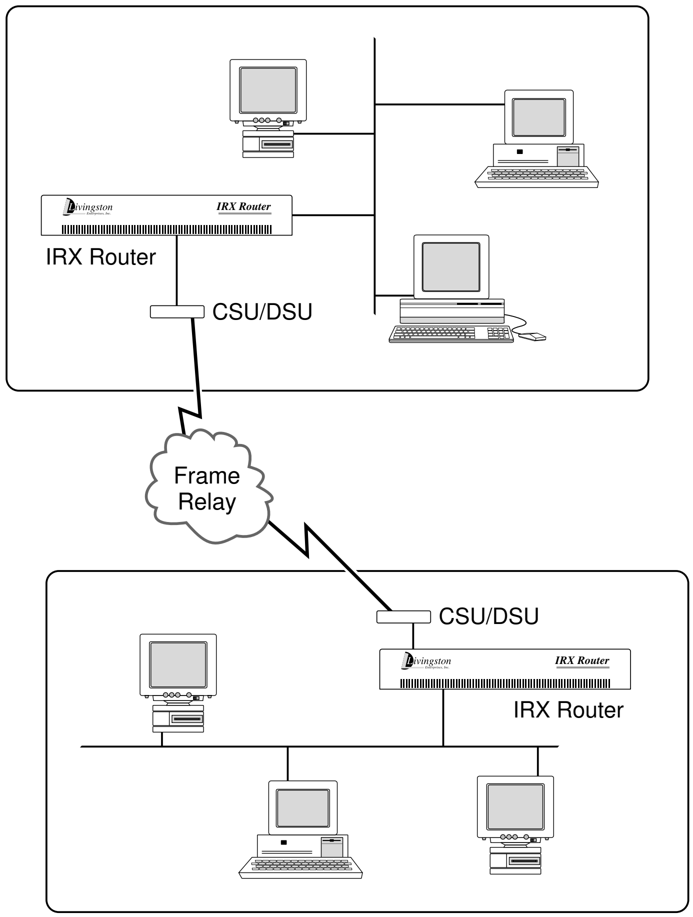

Figure 16-1 Frame Relay Configuration

Description of Sample Configuration

The example described in this chapter connects a PortMaster router located in one office with a PortMaster router located in another office using Frame Relay on a synchronous interface. The values shown in Table 16-1 are used in this example. Change values to reflect the actual values for your network.

Table 16-1 Example Configuration Variables for Frame Relay Connections

Variable Description	**Value for this Example**
Name of router in office1	office1
Ether0 IP address of router in office1	192.168.200.1
Ether0 Netmask	255.255.255.0
Gateway	192.168.20.2
Protocol for port S1 in office1	Frame Relay
IP address for port S1 in office1	192.168.20.1
Netmask for port S1 in office1	255.255.255.0
DLCI list for port S1 in office1[1]	16:192.168.20.2
Annex-D for port S1 in office1	10 seconds (If used, DLCI list is optional); LMI is also available.
Name of router in office2	office2
Ether0 IP address of router in office2	192.168.1.1
Ether0 Netmask	255.255.255.0
Protocol for port S1 in office2	Frame Relay
IP address for port S1 in office2	192.168.20.2
Netmask for port S1 in office2	255.255.255.0
DLCI list for port S1 in office2	16:192.168.20.1
Annex-D for port S1 in office2	10 seconds (If used, DLCI list is optional); LMI is also available.

1. The two ends of a Private Virtual Circuit (PVC) do not have to use the same number for their DLCI's. Use the DLCI's provided by your carrier.

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the "Troubleshooting" chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switches appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.
5. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.
6. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.
7. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
8. **Press [Return] at the password prompt.**
9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.
10. **Set the netmask and broadcast values if necessary.**

11. Save the address in the PortMaster nonvolatile memory by typing:

```
Command> save all
```

12. If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:

```
Command> quit
```

Configuring the Software for a Frame Relay Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible computer. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

Setting Global Parameters

Set the name of the system to office1 using the System Name parameter and the IP Gateway parameter to 192.168.20.2. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

For this example configuration, none of the other global parameters need to be set. However, you may want to define some of these parameters for your installation.

Setting the Ethernet Interface Parameters

Set the following Ethernet parameters on office1 to values appropriate for your network. The values shown in Table 16-2 apply to this example only.

Table 16-2 Ethernet Parameter Values

Parameter	Value
IP Address	192.168.200.1
Netmask	255.255.255.0

Table 16-2 Ethernet Parameter Values *(Continued)*

Parameter	Value
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, "Configuring the Ethernet Interface."

Setting the Synchronous Port Parameters for a Frame Relay Connection

Configure the WAN port parameters with values appropriate for your network. The values shown in Table 16-3 apply to this example only.

Table 16-3 WAN Port Parameter Values

Parameter	Value
Port Type	Network
Network Type	Hardwired
Protocol	Frame Relay
Port IP address	Specified 192.168.20.1
Netmask	255.255.255.0
Speed	(speed is set by external clock)
Modem Control	On or Off depending on the CSU/DSU configuration
Routing	On (Broadcast and Listen)
Compression	Disabled
Annex-D	10 seconds (LMI can be used instead of Annex-D)
DLCI List	16:192.168.20.2 (or empty if remote router supports inverse ARP)

If LMI or Annex-D is set, the PortMaster receives DLCI information in the full status update messages from the Frame Relay switch. The PortMaster then attempts to discover IP addresses of other routers using inverse ARP. You can set DLCI lists statically as well. The `show arp frm1` command lists both the static and dynamic DLCI lists for the S1 port.

If Annex-D is available from your carrier for a new connection, it is preferable to LMI.

To connect to Cisco routers using Frame Relay, the Cisco router must be set to use `encapsulation frame-relay ietf` for the serial interface; otherwise, the frame map for your DLCI must have the `ietf` argument appended.

For more information about synchronous ports, refer to Chapter 7, "Configuring a Synchronous WAN Port."

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you are having problems use the information in this section to debug your configuration.

If you are having trouble with a Frame Relay connection, verify the following:

- The error counters should be 0 except for abort errors. If your counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cables and they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing the clock to the PortMaster. The CSU/DSU can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- Contact your carrier to review your configuration and the status of their line.
- Use the following two commands to view the LMI or Annex-D keepalives:

```
Command> set console
Command> set debug 0x51
```

Once you have verified that the proper keepalives are being received, type:

```
Command> set debug 0
Command> reset console
```

- If you have a Cisco router on the other end of your connection, it must be set for `encapsulation frame-relay ietf` for the serial interface; otherwise, the frame map for your DLCI must have the `ietf` argument appended on the Cisco.

Frame Relay Subinterface

The PortMaster supports a feature called DLCI bundling to allow splitting one synchronous port, with multiple DLCIs, into two Frame Relay subinterfaces. In this configuration the DLCIs are divided between the subinterfaces using the Location Table and the DLCI Table. Only two subinterfaces per port are currently supported, and are referred to as the "primary subinterface" and "secondary subinterface." Each subinterface must have its own subnet or assigned network. Active discovery of DLCIs via LMI or Annex-D only occurs on the primary subinterface. The secondary subinterface can have an unlimited number of DLCIs.

The Frame Relay subinterfaces can only be set using the command line interface. For example, add a location with the protocol type set to frame:

```
Command> set s1 group 1
Command> add location example
Command> set location example protocol frame
Command> set location example group 1
```

The rest of the Location Table entries are set as described in Chapter 9, "Configuring Dial-Out Locations," including IP address for the interface, routing, and filtering.

The next step in configuring the subinterfaces is to create an entry in the DLCI Table. Entries can be followed with an optional IP address or hostname. The keyword "ipdlci" is a synonym for "dlci". The keyword "ipxdlci" is also available for IPX networks. To create a DLCI Table entry, type:

```
Command> add dlci example 16
Command> add dlci example 19 192.168.2.19
Command> add ipdlci example 20 192.168.2.20
Command> add ipxdlci example 21 0e0a001e
```

To remove an entry, use the delete command as follows:

```
Command> delete dlci example
Command> delete ipxdlci example 21
```

There is no `show table dlci` command. Instead, entries which are added or deleted are linked to the Location Table. Therefore, the `show location` *`example`* command displays the DLCI entries.

You can only have one Location Table entry per Frame Relay interface (allowing one secondary subinterface), so you can have some DLCIs as part of one location and other DLCIs as part of the port interface. Multiple secondary subinterfaces are not supported yet.

Troubleshooting Subinterfaces

Packets received on a subinterface can only be identified as belonging to that subinterface if the DLCI is properly entered in the DLCI Table for that location. If you are having problems, verify the following:

- Check the list of DLCIs tied to each location using the `show location` *`Location_Name`* command
- Verify the DLCI list on a location using the `show arp frm`*`XX`* command
- Always reset the port after changing the DLCI list
- Verify that all DLCIs are accounted for by checking the DLCI list for your primary interface. If you enter the wrong DLCI for the subinterface then the real DLCI for the subinterface shows up as belonging to the primary interface, if LMI or Annex-D is in use.

Example of a Frame Relay Subinterface

This example is for an IRX-111 with Frame Relay coming into port S1 with DLCIs 16, 17, and 18. Port S1 has already been configured for Frame Relay, so that portion is not shown here. The following commands split the Frame Relay into a primary subinterface for DLCI 18, and a secondary subinterface for DLCIs 16 and 17.

```
Command> set s1 group 1

Command> add location sub1
Command> set location sub1 protocol frame
Command> set location sub1 group 1
Command> set location sub1 address 192.168.3.1
Command> set location sub1 netmask 255.255.255.0
Command> set location sub1 routing on

Command> add dlci sub1 16
Command> add dlci sub1 17

Command> same all
Command> reset s1
```

You now have the following two subinterfaces:

- DLCI 18 on s1
- DLCI 16 and 17 on s1 (sub1)

Note – You could not define another subinterface on port S1 using other DLCIs, but you could add other DLCIs to either of these two existing subinterfaces. A future release will remove this restriction and allow you to divide each Frame Relay interface into as many virtual subinterfaces as you like.

Synchronous V.25bis Dial-Up Connections 17

This chapter describes how to use the PortMaster to connect two Local Area Networks (LANs) via synchronous V.25bis dialing applications such as, ISDN, terminal adapters, or switched 56K.

The following topics are described:

- Overview of the ISDN and switched 56K configuration
- Description of hardware configuration
- Description of the software configuration for ISDN with a V.25bis terminal adapter or switched 56K
- Testing the configuration

Overview of the ISDN and Switched 56K Configurations

PortMasters support dial on-demand ISDN and switched 56K connections using synchronous ports and the PPP protocol. ISDN speeds of up to 64Kbps are possible with an outside carrier and an external terminal adapter (TA). Speeds of up to 128Kbps are possible if the TA supports B-channel BONDING. Contact your service provider for specific information about the required terminal adapter.

Switched 56K connections require an external CSU/DSU. ISDN and switched 56K connections can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the Location Table for dial-out connections and a dial-in user must be specified in the User Table for dial-in connections.

PAP is available for dial-in authentication, when a router dials into your PortMaster. CHAP is available for dial-in and dial-out authentication.

When connecting an asynchronous ISDN terminal adapter to an asynchronous port using AT commands to dial, configure the PortMaster just as you would for a modem. Refer to Chapter 11, “Connecting a Branch Office to the Main Office” and Chapter 12, “Connecting Your Office to the Internet” for more information. In this configuration, keep in mind that a 115.2Kbps asynchronous DTE rate can only support a single 64Kbps B-channel, because it takes 10 bits to send a byte of asynchronous data (including the start and stop bits). However, it takes only 8 bits to send a byte of synchronous data. Therefore, a 115.2Kbps DTE rate cannot properly support two 64Kbps B-channels because the TA is unable to buffer the excess data when data is coming in from the ISDN line at 16 kilobytes/second and the DTE can only accept 11.5 kilobytes/second.

Figure 17-1 shows an example of an ISDN or switched 56K connection.

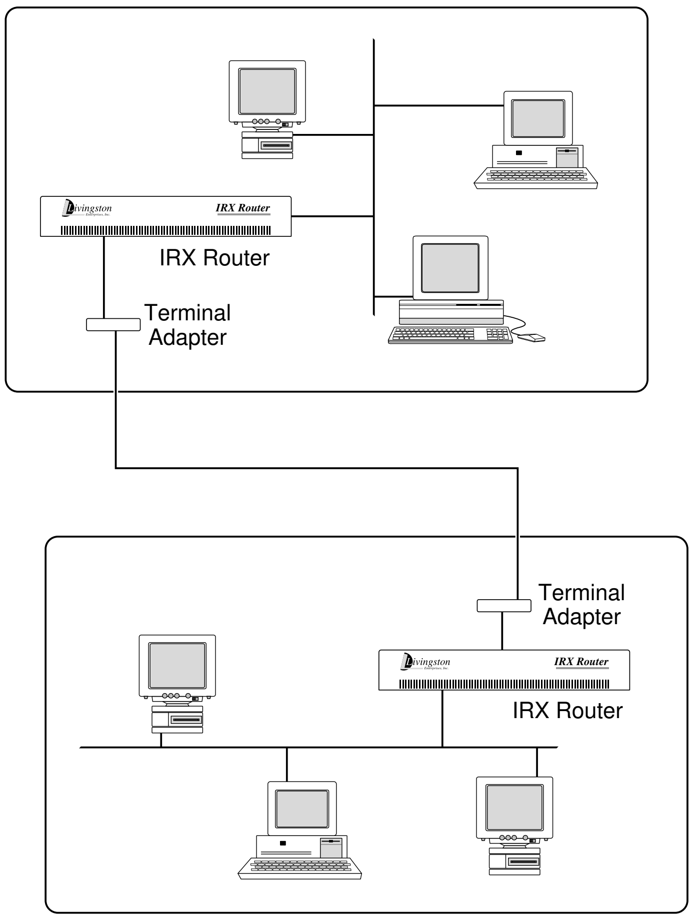

Figure 17-1 Example of an ISDN or Switched 56K Connection

Description of Sample Configuration

This example connects a PortMaster located in one office with a PortMaster located in another office using a synchronous interface that is initiated on-demand using an ISDN or switched 56K connection. The variables shown in Table 17-1 are used in this example. Change variable values to reflect the actual values for your network.

Table 17-1 Example Configuration Variables for V.25bis Connections

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
Phone number of router in office1	17005551111
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of router in office2	000000F2
IPX Frame Type	IEEE 802.2 on Ethernet
Phone number of router in office2	17005552222
IPX network of the serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the “Troubleshooting” chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**

3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.
5. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.
6. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.
7. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
8. **Press [Return] at the password prompt.**
9. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

   In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.
10. **Set the netmask and broadcast values if necessary.**
11. **Save the address in the PortMaster nonvolatile memory by typing:**

```
Command> save all
```

12. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software for an ISDN or Switched 56K Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a PC running Microsoft Windows. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

The configuration using V.25bis dialing for both ends of the connection is given in this section.

Configuring ISDN or Switched 56K on office1

The PortMaster in Office 1 (office1) is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Office 2 (office2).

Setting the Global Parameters on office1

Set the following global parameters to the values shown in Table 17-2. These values only apply to this example. Use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 17-2 Global Parameter Values on office1

Parameter	**Value**
IP Gateway	192.168.1.1
Default Route	Broadcast
Sysname	office1

For more information about global parameters, refer to Chapter 4, “Configuring a PortMaster.”

Setting the Ethernet Interface Parameters on office1

Set the following Ethernet parameters to the values shown in Table 17-3.

Table 17-3 Ethernet Parameter Values on office1

Parameter	**Value**
Protocol	IP/IPX
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, “Configuring the Ethernet Interface.”

Setting the Synchronous Port Parameters on office1

Configure the synchronous WAN port parameters with the values shown in Table 17-4 for the example in this chapter. Your configuration should reflect your network.

Table 17-4 WAN Port Parameter Values on office1

Parameter	**Value**
Port Type	Network
Network Type	Twoway (Dial In&Out)
Line Speed	The speed is a comment only, the actual speed is set by the external clock
Modem Control	On
Dial Group	0 (same as for Location Table entry)

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, "Configuring a Synchronous WAN Port."

Defining the Dial-In User on office1

A user account must be set up on the router office1 so the PortMaster office2 can dial in when traffic is queued. The new user office2 should be configured on office1 with the parameter values shown in Table 17-5.

Table 17-5 User Table Parameter Values for User office2

Parameter	**Value**
User Name	office2 (must be the SNMP system name of the remote PortMaster)
Password	anypasswd (The password must match the password for user office1 on PortMaster office2)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500

No compression is used on synchronous lines. For more information about configuring User Table parameters, refer to Chapter 8, "Configuring Dial-In Users."

Defining a Dial-Out Location on office1

A location entry on the PortMaster office1 must be created for the location identified as office 2. This allows the router office1 to call the PortMaster office2 when network traffic is queued. The new location office2 should be configured on office1 with the parameter values shown in Table 17-6.

Table 17-6 Location Table Parameter Values for Location office2

Parameter	Value
Location Name	office2
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Idle Timeout	5 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0 (same as for WAN port)
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005552222 (V.25bis dialing does not require the carriage return) Expect: =DCD=

For more information about configuring Location Table parameters, refer to Chapter 9, “Configuring Dial-Out Locations.”

After the port, user, and location parameters are entered, the port should be reset to make the new configuration active.

Configuring a V.25bis Dial-Up Connection on office2

The PortMaster in Office 2 (office2) is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Office 1 (office1).

Setting the Global Parameters on office2

Set the following global parameters to the values shown in Table 17-7. These values only apply to this example; use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 17-7 Global Parameter Values on office2

Parameter	**Value**
IP Gateway	Set to the address of the next upstream router
Default Route	Off
Sysname	office2

Setting the Ethernet Interface Parameters on office2

Set the following Ethernet parameters to the values shown in Table 17-8.

Table 17-8 Ethernet Parameter Values on office2

Parameter	**Value**
Protocol	IP/IPX
IP Address	192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

Setting the Synchronous Port Parameters on office2

Configure the synchronous port parameters with the values shown in Table 17-9 for the example in this chapter. Your configuration should reflect your network.

Table 17-9 WAN Port Parameter Values for office2

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Transport Protocol	PPP
Port IP address	Un-numbered
Netmask	255.255.255.0
Line Speed	The speed is a comment only, the actual speed is set by the external clock
Modem Control	On
Group	0

Defining the Dial-In User on office2

A user account must be set up on the router office2 so the PortMaster office1 can dial in when traffic is queued. The new user office1 should be configured on office2 with the parameter values shown in Table 17-10.

Table 17-10 User Table Parameter Values for User office1

Parameter	Value
User Name	office1 (must be the SNMP system name of the remote system)
Password	anypasswd (The password must match the password for user office2 on PortMaster office1)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1

Table 17-10 User Table Parameter Values for User office1 *(Continued)*

Parameter	**Value**
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	Off

No compression is used on synchronous lines. For more information about configuring User Table parameters, refer to Chapter 8, "Configuring Dial-In Users."

Defining a Dial-Out Location on office2

A location entry on the PortMaster, office2, must be created for the location identified as office1. This allows the router, office2, to call the PortMaster, office1, when network traffic is queued. The new location office1 should be configured on office2 with the parameter values shown in Table 17-11.

Table 17-11 Location Table Parameter Values for Location office1

Parameter	**Value**
Location Name	office1
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Idle Timeout	5 minutes

Table 17-11 Location Table Parameter Values for Location office1 *(Continued)*

Parameter	**Value**
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	0
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005551111 Expect: =DCD=

Use the dialer to connect between the two offices. Once everything is working properly, reset the ports and change the Location Type parameter from Manual to On-Demand on both routers.

Troubleshooting the Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you have problems use the information in this section to debug your configuration.

Troubleshooting V.25bis Dial-Up Connections

If you are having trouble with a V.25bis dial-up connection, verify the following:

- The error counters should be 0 except for a small number of abort errors resulting from plugging cables in or out. If your error counters are non-zero, there is a problem external to the PortMaster.
- Verify that you are using the correct cables and they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Livingston cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU or synchronous terminal adapter is providing the clock to the PortMaster. The CSU/DSU or TA can generate the clock or receive it from the carrier, it does not matter to the PortMaster.
- Verify that the CSU/DSU or synchronous terminal adapter is configured properly.
- Contact your carrier to review your configuration and the status of their line.

- Use the following commands to view the PPP negotiation:

```
office1> set console
office1> set debug 0x55
office1> dial office2
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0
Command> reset console
```

ISDN Connections 18

This chapter describes how to use the PortMaster to connect two Local Area Networks (LANs) via ISDN using V.25bis dialing on a BRI interface with integrated NT1.

The following topics are described:

- Overview of the ISDN configuration
- ISDN BRI configuration commands
- Description of hardware configuration
- Description of the software configuration for ISDN with integrated NT1
- Testing the configuration

Overview of the ISDN Configuration

PortMasters support dial on-demand ISDN connections using BRI ports and the PPP protocol. Each BRI supports two 64 Kbps B channels for data and one 16 Kbps D channel for signalling. Multiple lines can be used to increase bandwidth, either using multi-link PPP as defined in RFC 1717 or using Livingston's multi-line load balancing. ISDN BRI ports are easier to configure than asynchronous or synchronous ports because the NT1 is integrated in the port, so no modem, CSU/DSU, or external terminal adapter is required.

ISDN ports can also be used to do anything that an asynchronous port can be used for except network hardwired. Async or sync usage is autodetected. 56K or 64K speed is also autodetected.

ISDN connections can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the Location Table for dial-out connections and a dial-in user must be specified in the User Table or RADIUS for dial-in connections. Figure 18-1 shows an example of an ISDN connection.

CHAP is available for dial-in or dial-out authentication. PAP is available for dial-in authentication, and is available for dial-out authentication if the =PAP= Send string is used in the V.25bis dialing script.

Contact your service provider for specific information about your ISDN switch type and Service Profile Identifier (SPID).

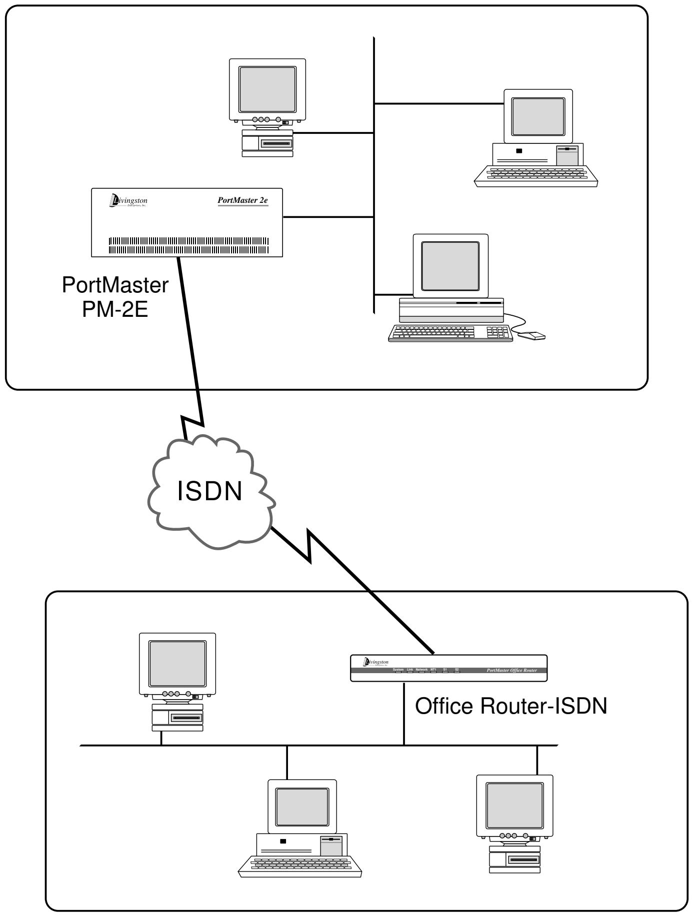

Figure 18-1 Example of an ISDN Connection

ISDN BRI Port Configuration Commands

Two special parameters need to be configured on the PortMaster to permit ISDN service: the ISDN Switch type and a Service Profile Identifier (SPID) for each port. Optionally a directory number for each port can be specified.

To display ISDN debug information on the console, use the following commands:

```
Command> set console
Command> set debug isdn on
```

To turn off debugging, use the following commands:

```
Command> set debug isdn off
Command> reset console
```

ISDN Switch Type

The ISDN Switch Type is a global configuration parameter that can be set to one of three values: DMS-100, NI-1 (National ISDN-1), or 5ESS, also known as ATT-5ESS. Obtain the switch type from your telephone company. Use one of the following commands to set the switch type. The default is NI-1.

```
Command> set isdn-switch ni-1
Command> set isdn-switch dms-100
Command> set isdn-switch 5ess
```

SPID

The Service Profile Identifier (SPID) is a number up to 20 digits long set for each port, which identifies the port to the telephone company. The telephone company provides you with the SPIDs for each line. To set the SPID, use the following command:

```
Command> set s10 spid 1510555121200
```

The `set debug isdn on` command shows any invalid SPIDs.

Terminal Identifier (TID)

The Terminal Identifier (TID) is a numeric value used by some telephone companies for additional identification. Some telephone companies require the SPID, while others require a TID as well. When configuring the PortMaster, append the TID to the SPID if required by your carrier.

Directory Number

The optional Directory Number is a 10-digit phone number provided by the telephone company. If it is set, an incoming call must match this number to determine which port the call should be taken on. The Directory Number must be set in order to allow V.120 multilink calls from the PowerLink128 ISDN Card.

Use either of the following commands to set the Directory Number.

```
Command> set s10 dn 510555111
Command> set s10 directory 510555111
```

ISDN Port Configuration Tips

ISDN ports are simpler to configure than asynchronous ports. Note the following:

- Modem control (carrier detect), flow control, and speed are not set on an ISDN port. The PortMaster senses the speed and sets the port to 64000 bps or 56000 bps accordingly. Flow control is not set on a synchronous line since clock is provided by the telephone company and carrier detect is always used.

  Refer to your *Hardware Installation Guide* for information on ISDN LED activity.
- The ISDN ports support synchronous PPP and asynchronous V.120 PPP or SLIP. The `show` *`port`* command displays 64000/async if the port is in use for an asynchronous V.120 connection.
- ISDN ports can be configured for all of the same functions as an asynchronous port, except that network hardwired is not supported.
- When using the ISDN port for network dial-out, the dial-out location should use a V.25bis script and authenticate using CHAP, or using PAP with the =PAP= V.25bis Send string.

Description of Sample Configuration

This example connects a PortMaster located in one office with a PortMaster located in another office using an on-demand ISDN connection. The variables shown in Table 18-1 are used in this example. Change variable values to actual values that reflect your network.

Table 18-1 Example Configuration Variables for an ISDN Connection

Variable Description	Value for this Example
Name of router in office1	office1
IP address of router in office1	192.168.200.1
Netmask	255.255.255.0
Gateway	192.168.1.1
IPX network of router in office1	000000F1
IPX Frame Type	IEEE 802.2 on Ethernet
ISDN Switch Type for office1	NI-1
ISDN Phone numbers of 2 B channels in office1	17005551111, 17005551112
SPID for 2 B channels in office1	700555111100, 700555111201
Name of router in office2	office2
IP address of router in office2	192.168.1.1
Netmask	255.255.255.0
IPX network of router in office2	000000F2
IPX Frame Type	IEEE 802.2 on Ethernet
ISDN Switch Type for office2	NI-1
ISDN Phone numbers of 2 B channels in office2	17005552222, 17005552223
SPID for 2 B channels in office2	700555222200, 700555222301
IPX network of the serial link	000000F3

Configuring the Hardware

To install the hardware for this configuration, follow these steps and the instructions in the *Hardware Installation Guide* for your PortMaster. If you need additional help, refer to the "Troubleshooting" chapter of your *Hardware Installation Guide*.

1. **Unpack the PortMaster router.**
2. **Connect your local Ethernet network to the Ethernet port and set the network selection DIP switch appropriately.**
3. **Connect the power cable.**
4. **Connect a terminal or PC (9600, 8, N, 1) to the console port marked S0 with a null modem cable.**

   Refer to the *Hardware Installation Guide* for your PortMaster for more information about connecting and configuring a terminal.
5. **Connect the BRI port to the ISDN telephone line.**

Caution – Do not plug an analog telephone line into the PortMaster BRI RJ-45 connector. The analog line does not work and the PortMaster could be damaged.

6. **Turn on the power switch.**

   The PortMaster performs power on self diagnostics. The self diagnostics are displayed to the console if the console DIP switch is UP.
7. **Press [Return] on the console.**

   The PortMaster login prompt is displayed.
8. **Type !root then press [Return].**

   You are prompted for the administrative password. The PortMaster is shipped from the factory without a password.
9. **Press [Return] at the password prompt.**
10. **Set the IP address of the new PortMaster by typing:**

```
Command> set ether0 address 192.168.200.1
```

In this example, 192.168.200.1 is the IP address of the PortMaster. A confirmation message is displayed showing the new IP address.

11. **Set the netmask and broadcast values if necessary.**
12. **If your version of PMconsole does not support setting the ISDN switch type, SPID, and directory number, then set these parameters from the command line as follows:**

```
Command> set isdn-switch ni-1
Command> set s1 spid 700555111100
Command> set s2 spid 700555111201
Command> set s1 dn 7005551111
Command> set s2 dn 7005551112
```

13. **Save the configuration in the nonvolatile memory of the PortMaster by typing:**

```
Command> save all
```

14. **If you are using PMconsole to configure your PortMaster, instead of the command line interface, exit the command line interface by typing:**

```
Command> quit
```

Configuring the Software for an ISDN Connection

In order to use the PMconsole graphical user interface to configure the PortMaster, you must install the software on a UNIX workstation or a Microsoft Windows-compatible PC. Once the software is installed and started according to the instructions in the appropriate *PMconsole Administrator's Guide*, proceed with the configuration. You can also configure the PortMaster from the console using the command line interface, or using administrative telnet once the PortMaster IP address is set.

Configuring ISDN on office1

The PortMaster in office1 is being configured for an ISDN dial-up connection to the PortMaster in office2.

Setting the Global Parameters on office1

Set the following global parameters to the values shown in Table 18-2. These values only apply to this example. Use values appropriate for your network.

Table 18-2 Global Parameter Values on office1

Parameter	**Value**
IP Address	192.168.200.1
IP Gateway	192.168.1.1
Default Route	Broadcast
Sysname	office1
ISDN Switch	NI-1 (or as identified by the carrier)

For more information about global parameters, refer to Chapter 4, "Configuring a PortMaster."

Setting the Ethernet Port Parameters on office1

Set the following Ethernet parameters to the values shown in Table 18-3.

Table 18-3 Ethernet Parameter Values on office1

Parameter	**Value**
Protocol	IP/IPX
IP Address	192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F1
IPX Frame Type	802.2
Broadcast Address	high (192.168.200.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

For more information on Ethernet parameters, refer to Chapter 5, "Configuring the Ethernet Interface."

Setting the ISDN Port Parameters on office1

Configure the ISDN port parameters with the values shown in Table 18-4 for the example in this chapter. Your configuration should reflect your network. This example assumes the BRI used is port S1-S2 on a PortMaster Office Router-ISDN (OR-U). If your application uses ports S10 through S29 on a PM-2E, adjust these values accordingly.

Table 18-4 ISDN Port Parameter Values on office1

Parameter	**Value**
Port Type	Network
Network Type	Twoway (Dial In&Out)
Dial Group	2
SPID	S1:700555111100 S2:700555111201

All the other parameters should be left at their default values. For more information about synchronous ports, refer to Chapter 7, "Configuring a Synchronous WAN Port."

Defining the Dial-In User on office1

A user account must be set up on the router office1 so that PortMaster office2 can dial in when traffic is queued. The new user office2 should be configured with the parameter values shown in Table 18-5.

Table 18-5 User Table Parameter Values for User office2

Parameter	**Value**
User Name	office2 (must be the system name of the remote system)
Password	anypasswd (The password must match the password for user office1 set on the remote PortMaster.)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.1.1
Netmask	255.255.255.0

Table 18-5 User Table Parameter Values for User office2 *(Continued)*

Parameter	Value
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On

For more information about configuring User Table parameters, refer to Chapter 8, "Configuring Dial-In Users."

Defining a Dial-Out Location on office1

A location entry on the PortMaster office1 must be created for the location identified as office2. This allows the router office1 to call the PortMaster office2 when network traffic is queued. The new location office2 should be configured with the parameter values shown in Table 18-6.

Table 18-6 Location Table Parameter Values for Location office2

Parameter	Value
Location Name	office2
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On
Idle Timeout	2 minutes

Table 18-6 Location Table Parameter Values for Location office2 *(Continued)*

Parameter	Value
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	2
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005552222[1] Expect: =DCD=

1. V.25bis dialing does not require a carriage return at the end of the string.

For more information about configuring Location Table parameters, refer to Chapter 9, "Configuring Dial-Out Locations." After the port, user, and location parameters are entered and saved, the port should be reset to make the new configuration active.

Configuring an ISDN Dial-Up Connection on office2

The PortMaster office2 is being configured for an ISDN dial-up connection to the PortMaster office1.

Setting the Global Parameters on office2

Set the following global parameters to the values shown in Table 18-7. These values only apply to this example, use values appropriate for your network. If you are using PMconsole, the System Name parameter is found in the SNMP Window. Refer to the *PMconsole Administrator's Guide* for more information.

Table 18-7 Global Parameter Values on office2

Parameter	Value
IP Gateway	Set to the address of the next upstream router
Default Route	Off
Sysname	office2
ISDN Switch Type	NI-1

Setting the Ethernet Port Parameters on office2

Set the following Ethernet parameters to the values shown in Table 18-8.

Table 18-8 Ethernet Parameter Values on office2

Parameter	Value
Protocol	IP/IPX
IP Address	192.168.1.1
Netmask	255.255.255.0
IPX Network	000000F2
IPX Frame Type	802.2
Broadcast Address	high (192.168.1.255)
Routing	On (Broadcast and Listen)
Ethernet	Enabled

Setting the ISDN Port Parameters on office2

Configure the ISDN port parameters with the values shown in Table 18-9 for the example in this chapter. Your configuration should reflect your network.

Table 18-9 WAN Port Parameter Values on office2

Parameter	Value
Port Type	Network
Network Type	Twoway (Dial In&Out)
Dial Group	2
SPID	S1:700555222200 S2:700555222301

Defining the Dial-In User on office2

A user account must be set up on the router office2 so the PortMaster office 1 can dial in when traffic is queued. The new user office1 should be configured with the parameter values shown in Table 18-10.

Table 18-10 User Table Parameter Values for User office1

Parameter	**Value**
User Name	office1 (must be the system name of the remote system)
Password	anypasswd (The password must match the password used for user office2 set on the PortMaster office1.)
Type	Network User/Normal
Protocol	PPP
User IP Address	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On

For more information about configuring User Table parameters, refer to Chapter 8, “Configuring Dial-In Users.”

Defining a Dial-Out Location on office2

A location entry on the PortMaster office2 must be created for the location identified as office1. This allows the router office2 to call the PortMaster office1 when network traffic is queued. The new location office1 should be configured with the parameter values shown in Table 18-11.

Table 18-11 Location Table Parameter Values for Location office1

Parameter	Value
Location Name	office1
Type	Manual (The location is set for manual dialing until after the configuration has been tested. Once the configuration is verified the Type is changed to On-Demand.)
Protocol	PPP
IP Destination	Specified 192.168.200.1
Netmask	255.255.255.0
IPX Network	000000F3
Routing	On (Broadcast and Listen)
MTU	1500
Compression	On
Idle Timeout	2 minutes
Maximum Ports	1 (If you are not using multi-line load-balancing.)
High Water Mark	0 (If you are not using multi-line load-balancing.)
Dial Group	2
Dial Script	V25bis
Send and Expect Pairs	Send: CRN17005551111[1] Expect: =DCD=

1. V.25bis dialing does not require a carriage return at the end of the string.

Use the dialer to connect between the two offices. Once everything is working properly, change the Location Type parameter from Manual to On-Demand on both routers and reset the ports.

Troubleshooting the Configuration

Most ISDN configurations come up with little trouble if you have configured the PortMaster using information from your carrier. However, if you are having problems use the information in this section to try to debug your configuration.

If you are having trouble with an ISDN connection, verify the following:

- The error counters should be 0 except for a few abort errors. If your counters are non-zero, there is a problem external to the PortMaster or the values received from your carrier may be incorrect.
- Verify that you are using the correct cables and they are attached securely to the correct port.
- Verify that the ISDN status light is on solid; otherwise, refer to the *Hardware Configuration Guide* for more information. This indicates connectivity to the ISDN switch.
- Verify your configuration as described in this chapter.
- Contact your carrier to review the ISDN switch type, SPIDs, and the status of their line.
- Use the following commands to view the PPP negotiation:

```
Command> set console
Command> set debug 0x51
```

For more information about the interpreting the results of the debug command, refer to “Interpreting LCP and IPCP Debug Output” on page 19-4. Once you have verified that the PPP negotiation is correct, type:

```
Command> set debug 0
Command> reset console
```

ISDN Port Status

Table 18-12 describes how to interpret the output of the ISDN BRI ports.

Table 18-12 ISDN BRI Port Status

Port Status	Modem Status	Description
`NO-SERVICE`	`DCD- CTS- TELCO- NT1-`	No SPID set
`NO-SERVICE`	`DCD- CTS- TELCO- NT1+`	No cable or no circuit to TelCo
`NO-SERVICE`	`DCD- CTS+ TELCO+ NT1+`	Cable and ISDN circuit OK but SPID not registered
`IDLE`	`DCD- CTS+ TELCO+ NT1+`	SPID registered and ready to use
`ESTABLISHED`	`DCD- CTS+ TELCO+ NT1+`	Connecting or providing device service but no carrier sensed
`ESTABLISHED`	`DCD+ CTS+ TELCO+ NT1+`	Connected
`ESTABLISHED`	`DCD+ CTS- TELCO+ NT1+`	Connected with V.120 async but flow controlled by other end

ISDN Status LEDs

On each ISDN board there is a green LED next to each of the five RJ-45 connectors. When you first turn power on, each LED blinks 8 times per second for about one second while performing an internal self-test of the NT1. If the self-test does not occur, contact Livingston Technical Support.

The LED goes off if no SPID is set on the port and there is no circuit to the telephone company. If no SPID is set on the port but there is a circuit to the telephone company, the LED blinks once per second. If there is a valid SPID and a circuit, the LED blinks once per second while synchronizing with the telephone company, then becomes solid.

Note – On the PortMaster Office Router ISDN (OR-U) this LED is on the front panel, labeled NT1.

Troubleshooting the PortMaster Configuration 19

This chapter describes how to analyze and evaluate issues with your PortMaster configuration. The following topics are discussed:

- How to recognize a network problem
- How to debug a network problem
- PPP negotiation quick reference information
- Booting from the network

Recognizing Network Problems

If you suspect you have a network problem there are several things you can do to try to determine the exact cause of the problem. A problem may be indicated if packets are not sent and received by the PortMaster the way you intended. Use the information in this section to troubleshoot your network.

Most of the commands described in this section can only be accessed using the command line interface, which is useful for debugging for the following reasons:

- The command line can be accessed from a console terminal regardless of network condition.
- The command line provides the most detailed feedback about events in the system and on the network.

Verifying Your Network Connections

You can use the Ping command to verify connectivity between your PortMaster and devices on your network. The Ping command sends an ICMP echo request to the host specified and listens for the corresponding echo reply from the specified host. If a reply is received, there is connectivity. If no reply is received there is a lack of connectivity somewhere on your network between the machine issuing the Ping request and the specified device.

If you do not receive a Ping response, check the following:

- Verify that the host you pinged is running and connected to the Ethernet.
- Verify that all of the cables are connected to the PortMaster properly.

- If the machine you pinged is on another subnet, verify that you are using the correct netmask.

Verifying Your Configuration

If you have verified that everything is connected properly, you should check the configuration of your PortMaster interfaces using the `ifconfig` command. The `ifconfig` command allows you to view the active configuration of each network interface by showing the name of the interface, various flags, and other configuration information. The `ifconfig` flags are described in Table 19-1.

Table 19-1 `ifconfig` Flags

Flag	Description
IP_UP	Indicates that the interface is up and running the IP protocol.
IP_DOWN	Indicates that the IP protocol is not in use.
IPX_UP	Indicates that the interface is up and running the IPX protocol.
IPX_DOWN	Indicates that the IPX protocol is not in use.
BROADCAST	Indicates that this is an Ethernet interface.
POINT_TO_POINT	Indicates that the network connection on this interface is a point-to-point connection.
LISTEN	Indicates that the interface is set to listen for RIP packets but not broadcast them.
RIPSEND	Indicates that RIP packets are being sent out from the interface but are not listened for.
PRIVATE	Indicates that no routing information is being sent or listened to on this interface.
SUSPENDED	Indicates that this interface is set for on-demand dial-out operation and is available, but does not have an active telephone connection to the remote site.
COMPRESS	Van Jacobsen TCP/IP header compression is being done on this interface.

The second and third lines of the `ifconfig` response contain the information described in Table 19-2.

Table 19-2 Additional `ifconfig` Information

Information	Description
inet	Indicates the IP address of the interface.
dest	Indicates the destination IP address of a point-to-point connection.
netmask	Indicates the netmask for the IP address shown in inet or dest.
broadcast	Indicates the broadcast address of the interface (only on Ethernet interfaces.)
mtu	Indicates the maximum transmission unit for the interface.
ipxnet	Indicates the IPX network number of the interface.
ipxframe	Indicates the IPX frame type for the interface (only on Ethernet interfaces.)

Debugging Network Problems

The following subsections describe some of the things that you can do to correct network problems related to your PortMaster once they are discovered. Most of the commands described in this section can only be accessed using the command line interface.

Determining the Software Version

When PMconsole is started the software version is displayed. To determine the version of the ComOS, either look at the bottom of the PMconsole screen after you have logged into a PortMaster or telnet to the PortMaster, login as `!root` and type `version`.

Note – Always include the version number of your ComOS when reporting problems to Livingston Technical Support.

Resetting Ports

PortMaster ports should be reset after any change to their configuration to make the new settings active. Resetting a port causes DTR to be held low for 500 milliseconds. Ports are reset when a connection drops. You can reset the whole system or specific ports using the `reset` command or by clicking the Reset button in PMconsole.

Disabling a Synchronous Port

A synchronous network hardwired port can be disabled by setting its IP address to 0.0.0.0 and the destination IP address to 0.0.0.0.

Tracing Routes with IP

You can use the `traceroute` command to identify the routers used to reach a remote host. The `traceroute` command sends UDP packets to the specified host and listens for ICMP messages returning. A host name or IP address of the destination host is entered with the `traceroute` command, and a list of router addresses in the order seen is printed.

To stop the `traceroute` command, enter the `traceroute` command with no address.

Interpreting LCP and IPCP Debug Output

The PPP negotiation process can be debugged and interpreted using the commands and information given in this section.

To debug PPP negotiations, type the following commands:

```
Command> set console
Command> set debug 0x51
```

To stop the debug output, type the following:

```
Command> set debug 0
Command> reset console
```

PPP Quick Reference

The information that follows describes the PPP protocol.

Frame format

Flag	Addr	Ctrl	Protocol	Data	FCS	Flag
7E	FF	03				7E

All the values shown are in hexadecimal. Adjacent frames may be separated by a single flag. Address and control bytes are omitted in nonLCP frames if Address-and-Control-Field-Compression is negotiated. If the first byte of the Protocol field is zero, it is omitted in nonLCP frames if Protocol-Field-Compression is negotiated. On asynchronous links, special characters (flags, escapes, and control characters selected in the negotiated remote Async-Control-Character-Map) between the flags are replaced by an escape (7D) and the original byte with bit 6 inverted (XOR'ed with 0x20).

Table 19-3 shows protocol values. The Network Protocol (NCP) is used to establish a connection for the associated data transfer protocol.

Table 19-3 Protocol Values

Protocol	Value	NCP Value
Internet Protocol (IP)	0021	8021
OSI Network Layer	0023	8023
DECnet Phase IV	0027	8027
Appletalk	0029	8029
Novell IPX	002B	802B
VJ Compressed TCP/IP	002D	
VJ Uncompressed TCP/IP	002F	
Banyan Vines	0035	8035
Link Control Protocol (LCP)		C021
Password Authentication Protocol (PAP)		C023
Link Quality Report (LQM)		C025
Challenge Handshake Authentication Protocol (CHAP)		C223

LCP Packet Formats

Configure-Request

01	ID	Length	Configuration Options

Configure-Nak

03	ID	Length	Configuration Options

Terminate-Request

05	ID	Length	Data

Code-Reject

07	ID	Length	Rejected-Packet

Echo-Request

09	ID	Length	Magic-Number	Data

Discard-Request

0B	ID	Length	Magic-Number	Data

Configure-Ack

02	ID	Length	Configuration Options

Configure-Reject

04	ID	Length	Configuration Options

Terminate-Ack

06	ID	Length	Data

Protocol-Reject

08	ID	Length	Rej'd-Protocol	Rej'd-Info

Echo-Reply

0A	ID	Length	Magic-Number	Data

LCP Configuration Options

Maximum-Receive-Unit

01	04	MRU

Default 1500 decimal

Authentication-Protocol

03	Length	Auth-Prot	Data

Default is no authentication

	04	C0	23		(PAP)
	05	C2	23	05	(CHAP using MD5)

Magic-Number

05	06	Magic-Number

Default is no magic number

Address-and-Control-Field-Compression

08	02

Default is no compression

Async-Control-Character-Map

02	06	Async-Map

Default is FFFFFFFF

Quality-Protocol

04	Length	Qual-Prot	Data

Default is no LQM

	08	C0 25	Reporting-Period

Protocol-Field-Compression

07	02

Default is no compression

IPCP Configuration Options

The IP Control Protocol is similar to LCP, except only codes 1 through 7 are used.

IP-Addresses

01	0A	Source-IP-Address	Deprecated
Destination-IP-Address			

IP-Address

03	06	IP-Address	No Default

IP-Compression-Protocol

02	Length	Compress-Prot	Data	Default is no compression
	06	00 2D	Max-Slot-ID Comp-Slot-ID	

(Van Jacobson Compressed TCP/IP)

PAP Packet Formats

Authenticate-Request

01	ID	Length	IDLen	Peer-ID
PwLen	Password			

Authenticate-Nak

03	ID	Length	MsgLen	Message

Authenticate-Ack

02	ID	Length	MsgLen	Message

CHAP Packet Formats

Challenge

01	ID	Length	ValSize	Value
Name				

Success

03	ID	Length	Message

Response

02	ID	Length	ValSize	Value
Name				

Failure

04	ID	Length	Message

Tracing Packets

The `ptrace` command allows you to see packet information as it passes through the PortMaster. Filters are used to define which packets you want to view. The `ptrace` command uses the name of a filter as its argument. All packets passing through the PortMaster are evaluated against the selected filter, except UDP and ICMP packets generated by the PortMaster itself. Packets that are permitted by the filter are displayed on the console with the following packet information:

- Source address of the packet
- Destination address of the packet
- Protocol
- Other protocol specific information, including source and destination port

Filters are used to narrow the `ptrace` output to only those packets of interest.

If no filter is specified with the `ptrace` command, packet tracing is disabled.

Note – If you are using `ptrace` through an administrative telnet session, your filter should deny your telnet packets. Otherwise, the `ptrace` command displays information for all of your own packets, creating an infinite loop of packets to tell you about the packets being generated.

The following example uses a filter that denies all telnet packets while allowing all other IP traffic for evaluation

```
Command> add filter all
Command> set filter all 1 deny tcp src eq 23
Command> set filter all 2 deny tcp dst eq 23
Command> set filter all 3 permit
Command> ptrace all
```

To stop viewing packet trace information, type:

```
Command> ptrace
```

Backing Up the PortMaster Configuration

The PortMaster configuration can and should be backed up. The backup file is not in human-readable form but can be reloaded using the `pminstall` program or the install function of PMconsole, which calls `pminstall`. The program used to backup the PortMaster configuration is `/usr/portmaster/pmreadconf`, use the syntax that follows.

Once the output file is created, change its permissions to 600 and move the file to the `/usr/portmaster/pm_data` directory, where it can be read by `pminstall`.

```
# /usr/portmaster/pmreadconf pm_name pm_passwd output_file
# chmod 600 output_file
# mv output_file /usr/portmaster/data
```

If you are using PMconsole for Windows, backing up the PortMaster is even simpler; just click the Backup Configuration button. See the *PMconsole for Windows Administrator's Guide* for more information.

Port State Verification

When PortMaster asynchronous ports are configured before cables and modems are attached, you may see two different port states when the `show port` command is invoked. Ports on the main system board may show IDLE, while ports on older expansion boards may show USERNAME. This is normal behavior because the value of carrier detect (CD) floats high on older expansion boards but not on the main system board.On more recent expansion boards, carrier is pulled low the same way it is on the main system board. On both old and new boards, as soon as modems are attached with &C1 set and modem control turned on for the port, the ports should show a state of IDLE. For more information about port states, refer to Table 3-2 on page 3-6.

Administrative Telnet Sessions

The PortMaster supports up to four administrative telnet connections at a given time. To establish an administrative telnet session, telnet to your PortMaster and login as `!root` with your administrative password. If you are having trouble establishing an administrative telnet session, verify the TCP port for telnet access by typing "`show global`". Check for stale telnet sessions by typing `show netcon` and looking for administrative connections to that port. Reset any connections that are stale by typing "`reset n#`" where # is the handle from the first column of the "`show netcon`" output.

You can make an administrative telnet session the console with the "`set console`" command. To release the console, use the "`reset console`" command.

In addition to four telnet sessions, you can have only one `pmcommand` or `pmconsole` or `pminstall` or `pmreadconf` program running at one time with a given PortMaster.

Diagnostic Mode

To force the PortMaster S0 port into diagnostic mode, follow these steps:

1. **Attach a terminal to the console port S0 using a null modem cable.**

   Configure the terminal for 9600 8N1. For more information, refer to the *Hardware Installation Guide* that came with your PortMaster.

2. **Raise the Console DIP switch #1 left-most, on the back of the PortMaster to put the console into Diagnostic Mode.**

   Refer to your *Hardware Installation Guide* for detailed information about the PortMaster DIP switches.

3. **Turn the power on and observe the diagnostic output.**

   If the PortMaster completes its diagnostics and produces a login: prompt, then the PortMaster booted correctly. If not, network booting may be required. Refer to the "Troubleshooting" chapter of your *Hardware Installation Guide* for more information on diagnostic boot messages.

Forgotten Passwords

This section describes what to do if you have forgotten the administrative password. If you are running a ComOS version prior to 2.4, IRX ComOS prior to 1.8R, or your ROM revision is F or earlier, follow the instructions in “Booting from the Network” instead.

If you are running ComOS version 2.4 or later or IRX ComOS version 1.8R or later, follow these steps if you have forgotten your password.

1. **Place the PortMaster in diagnostic mode as described in “Diagnostic Mode” on page 19-10.**
2. **Login to the PortMaster at the PortMaster Console login: prompt using** `!root` **and a password of** `override`**.**

   A 16-character encrypted challenge is displayed.
3. **Contact Livingston Technical Support for the appropriate 16-character one-time encrypted response.**

   For information about contacting Technical Support, see page xxxii in the Preface of this guide.
4. **Login to the PortMaster as** `!root` **and enter the 16-character encrypted response given by technical support as the password.**
5. **Change the administrative password using the** `set password` **command.**
6. **Type the** `save all` **command to save the new password to nonvolatile memory.**

Booting from the Network

Network booting is necessary if the FLASH RAM on your PortMaster becomes corrupted. You can determine that the FLASH is corrupt if any of the following occur:

- Your PortMaster never reaches the login: prompt during self diagnostics—when DIP switch #1 is UP.
- A checksum error on the ComOS is reported during the diagnostic boot process.
- Three unsuccessful upgrade attempts on PortMasters with a ComOS of version 3.0.4 or prior or IRX ComOS version 3.0.1R or prior. In this case the ComOS has run out of file descriptors.
- Netbooting is also required if you have forgotten the administrative password on a PortMaster with a ComOS prior to 2.4 or IRX ComOS versions prior to 1.8R.

Note – Network booting only works if you have a host on the Ethernet that supports TFTP. Otherwise, you must boot from the PROM monitor using the `download` command.

Network Booting

If you have determined that it is necessary to boot your PortMaster from the network, follow these steps:

1. **FTP the appropriate net-bootable ComOS, by typing:**

```
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd pub/livingston
ftp> get README.NETBOOT
ftp> quit
```

2. **Read the README.NETBOOT file to determine which net-bootable ComOS to download using FTP.**

   The ComOS is referred to as GENERIC.OS in the rest of this example.

3. **Repeat step 1 to download the appropriate *GENERIC.OS*.**

4. **If your boot host supports RARP and is on the same Ethernet segment as the PortMaster, add the Ethernet address of the PortMaster to your** `/etc/ethers` **file or your NIS map.**

5. **Start the** `rarpd` **service, if it is not already running, by typing:**

```
% rarpd -a
```

Note – The exact command may vary depending on your operating system; refer to your system manual for more information about running `rarpd`.

If your boot host does not have RARP, use the procedures in "PROM Booting" on page 19-16.

6. **Set up TFTP on your boot host by typing:**

```
% umask 22
% mkdir /tftpboot
% mv GENERIC.OS /tftpboot/GENERIC.OS
% cd /tftpboot
% ln -s . tftpboot
```

This procedure should be done even if your host does not support RARP.

If you are booting a PM-2, PM-2E, PM-2R, or PM-2ER from the network, the file *GENERIC.OS* should be moved to `/tftpboot/GENERIC.PM2`. If you are booting an IRX from the network, the *GENERIC.OS* file should be moved to `/tftpboot/GENERIC.IRX`.

7. **Using a text editor, uncomment the** `tftp` **entry in the** `/etc/inetd.conf` **file. To have the** `inetd` **daemon reread the** `/etc/inetd.conf` **file, send a SIGHUP signal to the** `inetd` **process.**

This procedure applies to most UNIX systems. However, the procedure for enabling TFTP on your system may vary. Consult your system documentation.

8. **Set the network boot (#2) DIP switch on the PortMaster to UP and turn the power switch ON.**

9. **Boot the PortMaster and login as** `!root` **with no password.**

10. If you want to save your PortMaster configuration before reformatting the FLASH RAM and your host is supported, type the following on your UNIX host:

```
% /usr/portmaster/pmreadconf pm_name pm_password output_file
```

There have been occasions when something in the configuration corrupted the FLASH RAM. If this is the case, reconfigure your PortMaster completely after you have installed the new ComOS in FLASH RAM.

11. To erase the configuration information stored in FLASH RAM, do one of the following on the PortMaster console:

– If you are running ComOS 3.0, 3.0R, or later, type:

```
Command> set register 0xffff 0x0102
```

After about thirty seconds, the following message is displayed:

```
Successfully formatted FLASH 2
```

– If you are running ComOS 2.4 or older, type:

```
Command> set register 0xffff 0x0f02
```

After a few moments, the following message is displayed:

```
Successfully formatted FLASH 2
```

Then type:

```
Command> set register 0xffff 0x0f03
```

After a few moments, the following message is displayed:

```
Successfully formatted FLASH 3
```

– If you are performing this procedure because the ComOS in the FLASH RAM is corrupted, type:

```
Command> set register 0xffff 0x0f63
```

After about 30 seconds, the following message is displayed:

```
Successfully formatted FLASH 99
```

Caution – This command formats all four FLASH chips, thereby removing the entire ComOS. Do not reboot the PortMaster until you reinstall the ComOS.

These procedures have reformatted the FLASH RAM on the PortMaster.

12. **If you have chosen one of the noconfig files, you need to set the IP address so that you can connect to the PortMaster using the PMconsole program installed on one of your workstations, by typing:**

```
Command> ifconfig ether0 address 192.168.200.1
```

In this case, 192.168.200.1 is the IP address of the PortMaster. If you are using a netmask other than 255.255.255.0 on your network, you must enter the netmask now by typing (for example):

```
Command> ifconfig ether0 netmask 255.255.255.192
```

13. **To install the new ComOS into the FLASH RAM, run PMconsole on your workstation and select the Upgrade option from the Install menu.**

14. **Turn off the power on the PortMaster. Remove the terminal from the console port and return the DIP switches to their normal operating positions. Turn on the PortMaster power to reboot the PortMaster.**

Everything should be working at this point. You must now reenter your configuration parameters.

PROM Booting

Beginning with PROM level F, a feature has been added that allows you to boot using the PROM instead of RARP. You can either boot from the `tftpd` daemon, or you can send a ComOS from your workstation to the console port on the PortMaster over a serial cable and boot from that.

If you have determined from the previous section that it is necessary to boot your PortMaster from PROM, follow these steps:

Note – This procedure only works with PROMs of level F or higher. The PROM version is displayed at boot time if the console port is in diagnostic mode.

1. **Place the PortMaster in diagnostic mode as described in "Diagnostic Mode" on page 19-10.**
2. **Attach a terminal to the console port of the PortMaster.**
3. **Turn the power switch to ON.**
4. **As the PortMaster starts to boot, press [ESC] or type ^[to display a > prompt.**

   The commands shown in Table 19-4 are now available.

Table 19-4 PROM Commands

Command	Description
address	Allows you to set the address of the Ethernet interface.
netmask	Allows you to set the netmask of the Ethernet interface. Default is 255.255.255.0.
gateway	Allows you to set the default gateway in order to boot from a server on another network.
tftp	Causes the PortMaster to issue the TFTP request to the boot server.
download	Allows you to download the ComOS using the serial port.
continue	Causes the PortMaster to continue attempting to boot using RARP.

5. Enter the address of the PortMaster Ethernet port by typing:

```
> address 192.168.200.1
```

6. Set the gateway and netmask, if needed.

7. FTP the appropriate net-bootable ComOS to the workstation you want to use as the boot server, by typing:

```
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd pub/livingston
ftp> get README.NETBOOT
ftp> quit
```

8. Read the README.NETBOOT file to determine which net-bootable ComOS to download using FTP.

9. Repeat step 7 to download the appropriate *GENERIC.OS*.

If you are booting a PM-2, PM-2E, PM-2R, or PM-2ER from the network, the *GENERIC.OS* file should be moved to /tftpboot/GENERIC.PM2. If you are booting an IRX from the network, the *GENERIC.OS* file should be moved to /tftpboot/GENERIC.IRX.

10. Set up TFTP on your boot host by typing:

```
% umask 22
% mkdir /tftpboot
% mv GENERIC.OS /tftpboot/GENERIC.OS
% cd /tftpboot
% ln -s . tftpboot
```

This procedure should be done even if your host does not support RARP.

11. Using a text editor, uncomment the `tftp` entry in the `/etc/inetd.conf` file. To have the `inetd` daemon reread the `/etc/inetd.conf` file, send a SIGHUP signal to the `inetd` process.

This procedure applies to most UNIX systems. However, the procedure for enabling TFTP on your system may vary. Consult your system documentation.

12. Use one of the following to boot the PortMaster.

– To boot the ComOS from the boot server using TFTP, on the console type:

```
> tftp 192.168.200.2
```

Where *192.168.200.2* is the IP address of the TFTP host that has the *GENERIC.OS* software. The PortMaster then boots using the ComOS from the boot server. The new ComOS has not yet been loaded into the FLASH RAM of your PortMaster.

– To download the ComOS directly through the serial line, type:

```
> download size
```

Where *size* is the number of bytes of ComOS that follows. The PortMaster then boots using the ComOS downloaded from the serial connection. The new ComOS has not yet been loaded into the FLASH RAM of your PortMaster.

13. To install the new ComOS into the FLASH RAM, run PMconsole on your workstation and select the Upgrade option from the Install menu or run `pminstall`**.**

14. After the upgrade has completed, turn off the power on the PortMaster. Remove the terminal from the console port and return the DIP switches to their normal operating positions. Turn on the PortMaster power.

This reboots the PortMaster. Everything should be working at this point.

Command Line Summary 20

This chapter provides a summary of the syntax for all of the commands available from the command line interface for ComOS 3.1.4, 3.2.1R, and 3.2L, except for obsolete or experimental commands. The ISDN-related commands are available in ComOS 3.3 and ComOS 3.3L.

The Values table in the next section describes the different kinds of values that are used with the various commands. These values are shown in uppercase italics (like this: *`Device`*) to distinguish them from the actual keywords of the commands, which are in a lowercase plain font (like this: `version`).

The rest of the tables in this chapter describe the syntax for commands related to various functions. The choices are seperated by vertical bars, like this: `on|off`, where one keyword from the list should be used. Optional portions of a command are surrounded by square brackets, like this: `[optional]`. Default values are underlined like this: on|<u>off.</u>

Values

Table 20-1 does not contain commands, it describes the different kinds of values that are used in commands.

Table 20-1 Values

Variable	Usage
Device	`/dev/network` or a pseudo-tty on a UNIX host
Ether0	`ether0` or `ether1` (on IRX-211), defaults to `ether0` if omitted
Filtername	string up to 12 characters long naming a filter
Group	an integer from 0 to 99, 0 is default
Handle	n followed by a number, with no space between them
Hex	hexadecimal number with leading 0x
Interface	interface specification, e.g. ether0, frm1, ptp1, frmW1, ptpW1

Table 20-1 Values *(Continued)*

Variable	Usage
Ipaddress	IP dotted quad or hostname
Ipmask	dotted quad with 1's in high order bits, 0's in low order bits
Ipxaddress	IPX address in hex format Ipxnetwork:node
Ipxnetwork	32-bit hexadecimal number
Isock	IPX socket
Itype	ICMP packet type, 0 or higher
Locname	string up to 12 characters long naming a location
MTU	integer from 100 to 1500
Metric	integer from 1 to 15, defaults to 1
Minutes	integer from 0 to 240; note that 1 has special meaning
ModemName	Modem table entry
NM	integer 0 to 32, expressing the number of high-order bits set to 1 in a netmask
Number	number 0 or higher
Password	string up to 16 characters long
Rule Number	integer 1 or higher
S0	any async port s0-s29, or all
S1	any async or sync port s0-s29, w1, or all
S10	ISDN port s1-s2 or s10-s29, depending on model
Seconds	number 0 or higher
String	string of ASCII characters
Tport	TCP/IP port, integer from 0 to 65535
Uport	UDP/IP port, integer from 0 to 65535
Username	string up to 8 characters long naming a user
W1	any sync port s1-s4, w1, or all

General Commands

Table 20-2 lists commands for troubleshooting, general administration, and displaying the configuration of the PortMaster.

Table 20-2 General Commands

<table>
<tr><th>Command Syntax</th></tr>
<tr><td>version</td></tr>
<tr><td>reboot</td></tr>
<tr><td>quit</td></tr>
<tr><td>done</td></tr>
<tr><td>exit</td></tr>
<tr><td>help</td></tr>
<tr><td>ifconfig interface [address Ipaddress] [netmask Ipmask]
[destination Ipaddress] [ipxnet Ipxnetwork]
[ipxframe ethernet_802.2|ethernet_802_ii|ethernet_802.3|
ethernet_ii] [up] [down] [private] [-private]</td></tr>
<tr><td>dial Locname [-x]</td></tr>
<tr><td>ping [Ipaddress]</td></tr>
<tr><td>traceroute [Ipaddress]</td></tr>
<tr><td>ptrace [Filtername]</td></tr>
<tr><td>pmlogin Ipaddress</td></tr>
<tr><td>rlogin Ipaddress</td></tr>
<tr><td>telnet Ipaddress</td></tr>
<tr><td>set debug Hex</td></tr>
<tr><td>set debug isdn [on|off]</td></tr>
<tr><td>set register Hex Hex</td></tr>
<tr><td>set console [S0|p0]</td></tr>
<tr><td>save Ether0|S0|W1|all|console|filter|host|location|netmask|p0|
routes|snmp|user</td></tr>
</table>

Table 20-2 General Commands *(Continued)*

Command Syntax
`reset` *Handle*|*S0*|*W1*|`all`|`console`|`dialer`|`nic`|`p0`
`show all`
`show arp` *Interface*
`show global`
`show ipxroutes`
`show memory`
`show netconns`
`show netstat`
`show routes`
`show sap`
`show sessions`
`show table filter`|`host`|`location`|`netmask`|`snmp`|`user`

Global Configuration

Table 20-3 contains all the global configuration commands that affect the entire PortMaster. For more information about global commands, refer to Chapter 4, "Configuring a PortMaster."

Table 20-3 Global Configuration Commands

Command Syntax
`show global`
`set password` *Password*
`set telnet` *Tport*
`set host [ 1`|`2`|`3`|`4 ]` *Ipaddress*
`set loghost` *Ipaddress*
`set namesvc domain`|`nis`
`set nameserver` *Ipaddress*

Table 20-3 Global Configuration Commands *(Continued)*

Command Syntax
`set domain` *String*
`set gateway` *Ipaddress Metric*
`set default on|off|broadcast|listen`
`set assigned_address` *Ipaddress*
`set reported_ip` *Ipaddress*
`set netbios on|off`
`set pap on|off`
`set maximum pmconsole` *Number*
`set isdn-switch att-5ess|5ess|dms-100|ni-1`

RADIUS Client Configuration

The commands shown in Table 20-4 allow you to configure the PortMaster to use a RADIUS server. RADIUS is consulted if a port is set for `security on` and a user is not found in the PortMaster User Table. For more information about RADIUS commands, refer to the *RADIUS Administrators Guide*.

Table 20-4 RADIUS Client Commands

Command Syntax
`set authentication_server` *Ipaddress*
`set alternate_auth_server` *Ipaddress*
`set accounting [ 2 ]` *Ipaddress*
`set secret` *Password*

Ethernet Configuration

The commands shown in Table 20-5 allow you to configure the Ethernet interface(s) `ether0` and (on the IRX-211) `ether1`. For more information about Ethernet interface commands, refer to Chapter 5, "Configuring the Ethernet Interface."

Table 20-5 Ethernet Interface Commands

Command Syntax
`set` *`Ether0`* `address` *`Ipaddress`*
`set` *`Ether0`* `netmask` *`Ipmask`*
`set` *`Ether0`* `broadcast high|`<u>`low`</u>
`set` *`Ether0`* `routing` <u>`on`</u>`|broadcast|listen|off`
`set` *`Ether0`* `ipxnet` *`Ipxnetwork`*
`set` *`Ether0`* `ipxframe ethernet_802.2|ethernet_802.3|ethernet_ii`
`set ether0 ip up|down|enabled|disabled` [1]
`set ether0 ipx up|down|enabled|disabled` [1]

1. This command is nly available on ether0 port, even on the IRX-211

Asynchronous Port Configuration

The commands shown in Table 20-6 allow you to configure asynchronous serial ports. Commands marked with a leading bullet (•) can only be used if the port is configured for network hardwired operation. For more information about asynchronous port commands, refer to Chapter 6, "Configuring an Asynchronous Port."

Table 20-6 Asynchronous Port Commands

Command Syntax
`show all`
`show S0`
`save S0`
`set S0 extended on|`<u>`off`</u>

Table 20-6 Asynchronous Port Commands *(Continued)*

<table>
<tr><th></th><th>Command Syntax</th></tr>
<tr><td></td><td>set S0 login [device Device]
[network dialin|dialout|twoway]</td></tr>
<tr><td></td><td>set S0 device Device [network dialin|dialout|twoway]</td></tr>
<tr><td></td><td>set S0 twoway Device [network dialin|dialout|twoway]</td></tr>
<tr><td></td><td>set S0 network dialin|dialout|twoway</td></tr>
<tr><td>•</td><td>set S0 network hardwired</td></tr>
<tr><td></td><td>set S0 speed [1|2|3] 300|600|1200|2400|4800|9600|19200|
38400|57600|76800|115200</td></tr>
<tr><td></td><td>set S0 parity even|none|odd|strip</td></tr>
<tr><td></td><td>set S0 databits 5|6|7|8</td></tr>
<tr><td></td><td>set S0 stopbits 1|2</td></tr>
<tr><td></td><td>set S0 xon/xoff on|off</td></tr>
<tr><td></td><td>set S0 rts/cts on|off</td></tr>
<tr><td></td><td>set S0 override xon|rts|speed|parity|databits on|off</td></tr>
<tr><td></td><td>set S0 modem|cd on|off</td></tr>
<tr><td></td><td>set S0 modem ModemName</td></tr>
<tr><td></td><td>set S0 group Group</td></tr>
<tr><td></td><td>set S0 idletime Minutes</td></tr>
<tr><td></td><td>set S0 security on|off</td></tr>
<tr><td></td><td>set S0 message String</td></tr>
<tr><td></td><td>set S0 prompt String</td></tr>
<tr><td></td><td>set S0 username|autolog String</td></tr>
<tr><td></td><td>set S0 hangup on|off</td></tr>
<tr><td></td><td>set S0 dialback_delay Seconds</td></tr>
<tr><td></td><td>set S0 dtr_idle on|off</td></tr>
</table>

Table 20-6 Asynchronous Port Commands *(Continued)*

	Command Syntax
	`set S0 service_login netdata|portmaster|rlogin|telnet [ Tport ]`
	`set S0 service_device netdata|portmaster|rlogin|telnet [ Tport ]`
	`set S0 host default|prompt|Ipaddress`
	`set S0 access on|off`
	`set S0 termtype String`
	`set S0 ifilter Filtername`
•	`set S0 ofilter Filtername`
•	`set S0 protocol slip|ppp`
•	`set S0 address Ipaddress`
•	`set S0 netmask Ipmask`
•	`set S0 destination Ipaddress [ Ipmask ]`
•	`set S0 mtu MTU`
•	`set S0 routing on|off|broadcast|listen`
•	`set S0 ipxnet Ipxnetwork`
•	`set S0 compression on|off`

Synchronous Port Configuration

The commands shown in Table 20-7 are used to configure synchronous serial ports. Commands marked with a leading bullet (•) can only be used if the port is configured for network hardwired operation. For more information about synchronous port commands, refer to Chapter 7, "Configuring a Synchronous WAN Port."

Table 20-7 Synchronous Port Commands

Command Syntax
`show all`
`show W1`

Table 20-7 Synchronous Port Commands *(Continued)*

<table>
<tr><th></th><th>Command Syntax</th></tr>
<tr><td></td><td><code>save W1</code></td></tr>
<tr><td></td><td><code>set W1 extended on|<u>off</u></code></td></tr>
<tr><td></td><td><code>set W1 network dialin|dialout|twoway|hardwired</code></td></tr>
<tr><td></td><td><code>set W1 protocol ppp</code></td></tr>
<tr><td>•</td><td><code>set W1 protocol frame</code></td></tr>
<tr><td>•</td><td><code>set W1 address Ipaddress</code></td></tr>
<tr><td>•</td><td><code>set W1 netmask Ipmask</code></td></tr>
<tr><td>•</td><td><code>set W1 destination Ipaddress [Ipmask]</code></td></tr>
<tr><td>•</td><td><code>set W1 ipxnet Ipxnetwork</code></td></tr>
<tr><td>•</td><td><code>set W1 routing on|off|broadcast|listen</code></td></tr>
<tr><td>•</td><td><code>set W1 ifilter Filtername</code></td></tr>
<tr><td>•</td><td><code>set W1 ofilter Filtername</code></td></tr>
<tr><td>•</td><td><code>set W1 mtu MTU</code></td></tr>
<tr><td>•</td><td><code>set W1 lmi|annex-d Seconds</code></td></tr>
<tr><td>•</td><td><code>set W1 dlci Dlci_list</code></td></tr>
<tr><td></td><td><code>set W1 group Group</code></td></tr>
<tr><td></td><td><code>set W1 hangup on|off</code></td></tr>
<tr><td></td><td><code>set W1 idletime Minutes</code></td></tr>
<tr><td></td><td><code>set W1 modem|cd on|<u>off</u></code></td></tr>
<tr><td></td><td><code>set W1 speed 9600|14400|19200|38400|57600|76800|115200|
56000|64000|1344k|1536k|2048k|t1|t1e|e1</code></td></tr>
<tr><td></td><td><code>set W1 encode nrz|nrzi</code></td></tr>
</table>

ISDN Port Configuration

ISDN BRI ports can be configured similarly to synchronous and asynchronous (V.120) ports. In addition, there are commands that allow you to configure the SPID and (optionally) the directory number (DN). The ISDN port configuration commands are shown in Table 20-8. For more information about ISDN port commands, refer to Chapter 18, "ISDN Connections."

Table 20-8 ISDN Port Commands

Command Syntax
`show all`
`show S10`
`save S10`
`set S10 extended on|off` (default: off)
`set S10 login [ device` *Device* `] [ network dialin|dialout|twoway ]`
`set S10 device` *Device* `[ network dialin|dialout|twoway ]`
`set S10 twoway` *Device* `[ network dialin|dialout|twoway ]`
`set S10 network dialin|dialout|twoway`
`set S10 spid` *String*
`set S10 directory|dn` *String*
`set S10 group` *Group*
`set S10 idletime` *Minutes*
`set S10 security on|off` (default: off)
`set S10 message` *String*
`set S10 prompt` *String*
`set S10 username|autolog` *String*
`set S10 hangup on|off` (default: off)
`set S10 dialback_delay` *Seconds*
`set S10 service_login netdata|portmaster|rlogin|telnet [` *Tport* `]` (default: portmaster)

Table 20-8 ISDN Port Commands

Command Syntax
set S10 service_device netdata|<u>portmaster</u>|rlogin|telnet [*Tport*]
set S10 host <u>default</u>|prompt|*Ipaddress*
set S10 termtype *String*
set S10 ifilter *Filtername*

Parallel Port Configuration

The commands shown in Table 20-9 allow you to configure the parallel port P0.

Table 20-9 Parallel Port Commands

Command Syntax
show p0
save p0
set p0 extended on|off
set p0 device *Device*
set p0 disabled
set p0 service_device netdata|portmaster|rlogin|telnet [*Tport*]
set p0 host default|*Ipaddress*
set p0 disconnect *Seconds*|infinity

DLCI Table Configuration

The commands shown in Table 20-10 allow you to configure the DLCI table, which is used to split a Frame Relay interface into two subinterfaces. For more information about Frame Relay commands, refer to Chapter 16, "Synchronous Frame Relay Connections."

Table 20-10 DLCI Table Commands

Command Syntax
`show location` *Locname*
`add dlci` *Locname Dlci* [*Ipaddress*]
`add ipdlci` *Locname Dlci* [*Ipaddress*]
`add ipxdlci` *Locname Dlci* [*Ipxnetwork*]
`delete dlci` *Locname Dlci*
`delete ipdlci` *Locname Dlci*

Host Table Configuration

The commands shown in Table 20-11 allow you to configure the host table inside the PortMaster in cases where DNS or NIS is not available.

Table 20-11 Host Table Commands

Command Syntax
`show table host`
`save host`
`add host` *Ipaddress String*
`delete host` *Ipaddress|String*

Filter Table Configuration

The commands shown in Table 20-12 allow you to configure the filter table. Filters can be applied to users, locations, or network hardwired ports, and can be used for debugging with the `ptrace` command. For more information on setting filters, refer to Chapter 10, "Configuring Filters."

Table 20-12 Filter Table Commands

<table>
<tr><th>Command Syntax</th></tr>
<tr><td>show table filter</td></tr>
<tr><td>show filter Filtername</td></tr>
<tr><td>save filter</td></tr>
<tr><td>add filter Filtername</td></tr>
<tr><td>delete filter Filtername</td></tr>
<tr><td>set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress/NM] [log]</td></tr>
<tr><td>set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress/NM] tcp [src eq|lt|gt Tport]
[dst eq|lt|gt Tport] [established] [log]</td></tr>
<tr><td>set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress/NM] udp [src eq|lt|gt Tport]
[dst eq|lt|gt Tport] [log]</td></tr>
<tr><td>set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress/NM] icmp [type Itype] [log]</td></tr>
<tr><td>set ipxfilter Filtername RuleNumber permit|deny
[srcnet Ipxnetwork] [srchost Ipxaddress]
[srcsocket eq|gt|lt Isock] [dstnet Ipxnetwork]
[dsthost Ipxaddress] [dstsocket eq|gt|lt Isock]</td></tr>
<tr><td>set sapfilter Filtername RuleNumber permit|deny
[server String] [network Ipxnetwork]
[host Ipxaddress] [socket eg|gt|lt Isock]</td></tr>
</table>

Location Table Configuration

The commands shown in Table 20-13 are used to configure the Location Table, used to specify network dial-out locations. For more information about Location Table commands, refer to Chapter 9, "Configuring Dial-Out Locations."

Table 20-13 Location Table Commands

Command Syntax
`show table location`
`show location` *`Locname`*
`save location`
`add location` *`Locname`*
`delete location` *`Locname`*
`set location` *`Locname`* `continuous`|`manual`|`on_demand`
`set location` *`Locname`* `protocol slip`|`ppp`|`frame`
`set location` *`Locname`* `destination` *`Ipaddress`*
`set location` *`Locname`* `netmask` *`Ipmask`*
`set location` *`Locname`* `ipxnet` *`Ipxnetwork`*
`set location` *`Locname`* `routing on`|`off`|`broadcast`|`listen`
`set location` *`Locname`* `group` *`Group`*
`set location` *`Locname`* `map` *`Hex`*
`set location` *`Locname`* `compression on`|`off`
`set location` *`Locname`* `mtu` *`MTU`*
`set location` *`Locname`* `script`|`v25bis` *`RuleNumber String String`*
`set location` *`Locname`* `maxports` *`Number`*
`set location` *`Locname`* `high_water` *`Number`*
`set location` *`Locname`* `idletime` *`Minutes`*
`set location` *`Locname`* `ifilter` *`Filtername`*
`set location` *`Locname`* `ofilter` *`Filtername`*

Table 20-13 Location Table Commands *(Continued)*

Command Syntax
`set location` *`Locname`* `multilink on|off`

Modem Table Configuration

The commands shown in Table 20-14 allow you to configure the modem table, which describes how to initialize a modem attached to an asynchronous port. See the `set modem` command in Table 20-6 on page 20-6 for additional information. For more information about configuring modems, refer to Chapter 6, "Configuring an Asynchronous Port."

Table 20-14 Modem Table Commands

Command Syntax
`show table modem`
`show modem` *`ModemName`*
`add modem` *`ModemName String Speed String`*
`delete modem` *`ModemName`*

Netmask Table Configuration

The commands shown in Table 20-15 allow you to configure the netmask table used for routing noncontiguous subnets. Use caution if configuring static netmasks.

Table 20-15 Netmask Table Commands

Command Syntax
`show table netmask`
`save netmask`
`add netmask` *`Ipaddress Ipmask`*
`delete netmask` *`Ipaddress`*

Route Table Configuration

The commands shown in Table 20-16 allow you to add and remove static routes to the routing table. The `show route` command marks static routes with the `HS` (for host) and `NS` (for network) flags.

Table 20-16 Route Table Commands

Command Syntax
`show route`
`save route`
`add route` *`Ipaddress Ipaddress Metric`*
`delete route` *`Ipaddress`*
`add ipxroutes` *`Ipxnet Ipxaddress Metric Ticks`*

SNMP Configuration

The commands shown in Table 20-17 allow you to configure the PortMaster as an SNMP agent. Use caution if you are allowing SNMP writes.

Table 20-17 SNMP Commands

Command Syntax
`show table snmp`
`save snmp`
`set sysname` *`String`*
`set snmp on|off`
`set snmp readcommunity|writecommunity` *`String`*
`add snmphost reader|writer any|none|`*`Ipaddress`*

User Table Configuration

The commands shown in Table 20-18 allow you to configure the User Table that is used to authenticate dial-in users. RADIUS can also be used to authenticate dial-in users; however, the User Table is consulted first. For more information about User Table commands, refer to Chapter 8, "Configuring Dial-In Users."

Table 20-18 User Table Commands

Command Syntax
`show table user`
`show user` *`Username`*
`save user`
`add netuser` *`Username`* `[ password` *`Password`* `]`
`add user` *`Username`* `[ password` *`Password`* `]`
`delete user` *`Username`*
`set user` *`Username`* `password` *`Password`*
`set user` *`Username`* `dialback` *`Locname`*|*`String`*
`set user` *`Username`* `host default`|`prompt`|*`Ipaddress`*
`set user` *`Username`* `service netdata`|`portmaster`|`rlogin`|`telnet [` *`Tport`* `]`
`set user` *`Username`* `protocol slip`|`ppp`
`set user` *`Username`* `destination Assigned`|`Negotiated`|*`Ipaddress`*
`set user` *`Username`* `netmask` *`Ipmask`*
`set user` *`Username`* `ipxnet` *`Ipxnetwork`*
`set user` *`Username`* `routing on`|`off`|`broadcast`|`listen`
`set user` *`Username`* `compression on`|`off`
`set user` *`Username`* `ifilter` *`Filtername`*
`set user` *`Username`* `ofilter` *`Filtername`*
`set user` *`Username`* `mtu` *`MTU`*
`set user` *`Username`* `map` *`Hex`*

Glossary

A

agent A software program installed in a managed network device. An agent stores management information and responds to the manager's request for this information.

alias A name assigned by the user to a hub or node.

Annex-D Refers to the ANSI T1.617 Frame Relay Annex D version of the LMI (Local Management Interface) protocol. The Annex-D protocol has a more robust feature set than the proprietary Cisco/Stratacom LMI, but was developed later.
Recent versions of the PortMaster software support either type of LMI. Earlier versions supported only the Cisco/Stratacom version. See also LMI.

ARP Address Resolution Protocol. This protocol discovers physical hardware network addresses that correspond to the high-level IP address for a given node.

ASCII American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.

AUTOEXEC.BAT A file that is automatically read and executed by DOS during the startup process.

B

baud The number of discrete signal events per second occurring on a communications channel. Although not technically accurate, baud is commonly used to mean bit rate.

B-channel A 64Kbps synchronous channel that is part of an ISDN BRI.

BONDING Bandwidth ON Demand INteroperability Group. A method for combining two B-channels into a single 128Kbps channel.

booting	The process in which a device obtains information and begins to process it to attain a state of normal operation.
bps or b/s	Bits per second, a unit for measuring the data rate.
BRI	Basic Rate Interface. ISDN interface that consists of two 64Kbps B-channels for voice or data and one 16Kbps D-channel for signalling.
broadcast packets	Packets that are sent to all network nodes.

C

click	To position the mouse pointer on an object, then press and release the left mouse button.
client-server environment	An environment where a computer system or process requests a service from another computer system. For example, a workstation may request services from a file server across a network.
committed information rate	The minimum bandwidth guaranteed to be available if required on a Virtual Circuit. (Guaranteed Bandwidth) often called CIR.
community strings	Community strings can be assigned to SNMP agents and are used to restrict access to those devices. SNMP community strings include read community and write community.
console port	A serial port on a PortMaster, used to set its IP address using a terminal and for configuration.
CRC errors	Cyclic Redundancy Check errors. These errors can indicate problems with source station hardware, receivers, retiming modules/repeaters, bridges, cabling, or transceivers.
CSU	Channel Service Unit. An ancillary device needed to adapt the V.35 interface to a port on a telephone carrier switch. The CSU is placed between the DTE and the switch.

D

DCE	Data Communications Equipment, such as a modem.
DDE	Dynamic Data Exchange. A form of interprocess communication that uses shared memory to exchange data between applications. Applications can use a one-time data transfer or ongoing exchanges.

DLCI Data Link Connection Identifier. A unique number that represents a particular PVC on a particular physical segment of the Frame Relay network. As the frame is passed through each switch, the DLCI is remapped as necessary, automatically by the switch. A DLCI identifies a circuit in both directions, not a destination or source.

DLL Dynamic Link Library. Windows automatically loads the applications into memory when required and unloads them when space is needed for other applications.

DMA Direct Memory Access. Direct access to computer memory not mediated by a microprocessor.

DOS The primary Disk Operating System used by IBM and compatible personal computers.

DRAM Dynamic Random Access Memory. A type of memory computer integrated circuit.

DSU Digital Service Unit. An ancillary device needed to adapt the V.35 interface on a port to a leased line or Frame Relay switch.

driver A software module that controls an input/output port or external device such as a keyboard or a monitor. TCP/IP uses a driver to control the network interface cards.

DTE Data Terminal Equipment, such as a terminal. PortMaster serial ports are DTE.

E

echo test A diagnostic test used to check network reachability in which an ICMP or SNMP test packet is sent to elicit a standard response.

Ethernet A network communications system developed and standardized by Digital Equipment Corporation, Intel, and Xerox using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration of Ethernet into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber optic cable, broadband, and unshielded twisted pair.

F

FRAD Frame Relay Asynchronous Device. A special kind of CSU/DSU that takes an asynchronous SLIP (sometimes PPP) connection and turns it into a single PVC for Frame Relay.

frame A packaging structure for network data and control information. A frame consists of the destination address, source address, length field, data, pad, and frame check sequence. The 802.3 standard for Ethernet specifies that the minimum size data frame is 64 bytes and the maximum size data frame is 1518 bytes.

FTP File Transfer Protocol. FTP is a TCP/IP protocol used to log onto a network host, list directories, and transfer files.

G

graphical user interface *See* GUI.

GUI Graphical User Interface. A software interface that is based on a graphical representation of various elements. PMconsole has several different GUIs.

H

hop A router-to-router transmission required when a data packet must be routed to a remote network.

I

icon A graphic symbol on a user interface display.

ICMP Internet Control Message Protocol. This part of the Internet Protocol (IP) allows for generation of error messages, test packets, and informational messages related to IP. This protocol is used by the ping function to send an ICMP Echo Request to a network host, which replies with an ICMP Echo Reply.

in-band signaling Signaling over a network.

interface Connection and interaction between hardware, software, and the user. An interface is activated by programming language commands and hardware signals. The interface between components in a network is called a protocol.

internet A network of networks.

Internet THE network of networks, stretching worldwide to millions of computers and users.

IP The Internet Protocol defined in RFC 791.

IPCP IP Control Protocol. A protocol used by PPP for establishing and configuring an IP link over PPP.

IPX The Internet Packet Exchange protocol defined by Novell, Inc.

IPXWAN IPX Wide Area Network protocol, used to establish and configure an IPX link over PPP, as described in RFC 1634.

ISDN Integrated Services Digital Network. A digital communications standard designed to allow the transmission of voice, data, images, and video over existing copper phone lines.

ISO International Organization for Standards. The international organization that sets standards for network communication protocols.

K

KB Kilobyte(s). 1024 bytes.

Kb Kilobits, 1024 bits.

Kbps Kilobits per second.

L

LAN Local Area Network. A local collection, usually within a single building or several buildings, of personal computers and other devices connected by cabling to a common transmission medium, allowing users to share resources and exchange files.

LCP Link Control Protocol. Used by PPP for establishing, configuring, and testing the data-link connection.

LED Light Emitting Diode.

line speed The speed of the physical wire attached to the interface or interface hardware. The line speed is 10Mbps for Ethernet and 1.544Mbps for T1. Fractional T1 is often implemented with a wire speed of T1 (1.544Mbps) and a lower port speed. See also port speed. Upgrading line speed is generally a hardware change.

LMI Local Management Interface. A protocol used to communicate link status and PVC status in Frame Relay. There are two types of LMI available on Frame Relay; the original proprietary Cisco/Stratacom LMI, and the ANSI T1.617 Annex-D LMI. In the PortMaster, LMI refers to the Cisco/Stratacom implementation. See also Annex-D.

local area network *See* LAN.

M

MAC address Media Access Control address. A unique 48-bit binary number (usually represented as a 12-digit hexadecimal number) encoded in the circuitry of a device to identify it on a local area network.

management information base *See* MIB.

management station A workstation or PC capable of retrieving and analyzing statistical information from networked SNMP agents.

MB Megabyte(s). 1,048,576 bytes.

Mb/s Megabits per second, a unit for measuring data rates.

menu bar An area at the top of a Microsoft Windows display, below the title bar, that displays the names of pull-down menus the user can select with the mouse.

MIB Management Information Base. A set of parameters that an SNMP-based management station can query from the SNMP agent of a network device.

Microsoft Windows The graphical user interface for the IBM and compatible personal computers.

modem A modulator-demodulator; a device that converts between the digital signals used by computers and analog signals that can be transmitted over telephone lines.

mouse	A pointing device, usually containing more than one functional button.
MS-DOS	Microsoft Disk Operating System. A version of DOS used by IBM-compatible personal computers.

N

network	A collection of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances.
network management	In the OSI model, the five functional application areas of accounting management, configuration management, fault management, performance management, and security management.
NIC	Network Information Center. An organization that provides information and services related to networking technologies. NIC also is an acronym for network interface card.
NOC	Network Operations Center.
node	A device, such as a personal computer, server, switching point, bridge, or gateway, connected to a network at a single location; also called station. *See* station.
NT1	An ISDN term that identifies the customer-end termination of the local phone company wires (local loop).

O

ODI	Open Datalink Interface. Novell's extension to its Open Datalink Interface specification. ODI isolates the protocol stack from the network adapter drivers allowing hardware independence for network connectivity.
out-of-band	A remote connection, or a connection outside of the connected networks, established over a modem. This connection is useful when network communications are not available.

P

packet A unit of data sent across a network.

partition Electronic isolation of an Ethernet device from network communications.

physical circuit A physical connection between two devices.

ping Packet INternet Groper. A program that is useful for testing and debugging networks. Ping sends an ICMP echo packet to the specified host and waits for a reply. Ping reports success or failure and statistics about its operation.

port The physical channel or connection through which data flows.

port speed The rate at which data is accepted by the port at the end of the wire. Specifically, in Frame Relay, or other fractional T1 applications, it is common to have a T1 line between the site and the telecommunications provider, but the telecommunications provider only accepts the number of bits per second ordered by the customer into the port on its equipment. Upgrading port speed is generally a software change.

program manager The main display in Microsoft Windows, from which the user selects functions and manages applications.

PVC Permanent Virtual Circuit. A circuit that defines a permanent connection in a switched digital service, such as Frame Relay. Frame Relay is the only switched digital service that uses PVCs supported by PortMasters.

R

RARP Reverse Address Resolution Protocol. A protocol used in network routers.

RFC Request For Comments. A document that describes Internet standards such as the Internet Protocol (IP).

router A device that connects two or more networks and can direct traffic based on network resource availability.

RS-232 interface A standard for data communication using serial data and control signals.

runt packet A packet with a frame size between 8 and 63 bytes with FCS or alignment errors. The runt packet is presumed to be a fragment resulting from a collision.

S

serial port — A bidirectional channel through which data flows one bit as a time. Asynchronous serial ports most often use 10 bits for a character of data including 1 start bit, 8 data bits, and 1 stop bit.

server — A computer or a specialized device that provides and manages access to shared network resources, such as hard disks and printers.

SNMP — Simple Network Management Protocol. This protocol is defined in RFC 1157. This protocol relates to management of devices on IP networks.

SPID — Service Profile Identifier.

station — A device, such as a personal computer, server, switching point, bridge, or gateway, connected to a network at a single location; also called a node. *See* node.

subnet mask — A subnet mask identifies the subnet field of a network address. The subnet mask is a 32-bit Internet address written in dotted-decimal notation with ones in the network and subnet portions of the address.

SVC — Switched Virtual Circuit. A connection established between two physical circuits, such as an ordinary telephone call. The call creates a virtual circuit between the originator and the party called.

T

Telnet — Internet standard protocol for remote terminal connection service. Telnet is described in RFC 854.

terminal — A device with a keyboard, an RS-232 serial interface, and a display for communicating with a computer.

terminal adapter (TA) — A device that provides ISDN compatibility to non-ISDN devices. An asynchronous TA turns an asynchronous bit stream into ISDN and looks like a modem to the PortMaster. A synchronous TA takes a synchronous bit stream and turns it into ISDN, typically supports V.25bis dialing and connects to a PortMaster synchronous port. Some TAs can be configured for synchronous or asynchronous operation.

terminal emulator — A program that makes a PC screen and keyboard act like a video display terminal of another computer.

TFTP Trivial File Transfer Protocol. A simplified version of FTP that transfers files but does not provide password protection or user directory capability. TFTP can be used by diskless devices that keep software in ROM and use it to boot themselves. The PortMaster can be booted using RARP and/or TFTP.

thick Ethernet An Ethernet connection using a 15-pin D-shell connector and an AUI cable connected to a transceiver. Also known as 10Base5.

thin Ethernet An Ethernet connection where the transceivers are built into the device and a BNC connector with cable are used to complete the connection; generally using an RG-58 coaxial cable. Also known as 10Base2.

twisted pair Abbreviated UTP (unshielded twisted pair), a pair of thin-diameter insulated wires commonly used in telephone wiring. The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Used for 10BaseT Ethernet with RJ-45 connectors.

U

U interface The ISDN interface defined as the connection between the NT1 and the telephone company local loop. The U interface standard is set by each country. The U interface described in Livingston documentation refers to the U.S. definition.

UDP User Datagram Protocol. This protocol is defined in RFC 768. This is a connectionless protocol that adds multiplexing to IP.

UNIX A multiuser, multitasking operating system originally developed by AT&T that runs on a wide variety of computer systems.

V

V.120 A CCITT standard for performing asynchronous rate adaptation into ISDN.

V.25bis A CCITT standard defining how to dial on synchronous devices such as ISDN or switched 56K.

V.32bis
An ITU-T standard that extends the V.32 connection range from 4800 bps to 14.4K bps. V.32 bis modems fall back to the next lower speed when line quality is impaired, and fall back further as necessary. They fall forward to the next higher speed when line quality improves.

V.34
An ITU-T standard that allows data rates as high as 28.8K bps.

virtual circuit
A logical connection between two endpoints on a switched digital network. Virtual circuits can be switched or permanent. A switched virtual circuit (SVC) is used when you make an ordinary telephone call, an ISDN connection, or a V.25 switched 56K connection. A permanent virtual circuit (PVC) is used in Frame Relay. See also PVC and SVC.

W

Windows
Graphics-based operating environment from Microsoft that integrates with DOS to provide a desktop environment similar to the Macintosh.

References

CCITT

V.25bis

V.120

Requests For Comments (RFC)

These documents can be found online using any World Wide Web browser.

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specification*

RFC 950, *Internet Standard Subnetting Procedure*

RFC 988, *Host Extensions for IP Multicasting*

RFC 1058, *Routing Information Protocol*

RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1166, *Internet Numbers*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1331, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1334, *PPP Authentication Protocols*

RFC 1362, *Novell IPX Over Various WAN Media (IPXWAN)*

RFC 1490, *Multiprotocol Interconnect Over Frame Relay*

RFC 1597, *Address Allocation for Private Internets*

RFC 1627, *Network 10 Considered Harmful (Some Practices Shouldn't be Codified)*

RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*

RFC 1700, *Assigned Numbers*

RFC 1717, *The PPP Multilink Protocol (MP)*

RFC 1814, *Unique Addresses are Good*

Books

Albitz, Paul and Cricket Liu. *DNS and BIND in a Nutshell*. O'Reilly & Associates, Inc. (ISBN 1-56592-010-4)

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc. 1995. (ISBN 1-56592-124-0)

Cheswick, William R. and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison-Wesley 1994. (ISBN 0-201-63357-4)
Japanese translation (ISBN 4-89052-672-2)
Errata are available from:
ftp://ftp.research.att.com/dist/internet_security/firewall.book

Comer, Douglas. *Internetworking with TCP/IP*. Prentice-Hall. (ISBN 0-13-468505-9)

Hunt, Craig. *TCP/IP Network Administration*. O'Reilly & Associates, Inc. (ISBN 0-937175-82-X)

The Basics Book of ISDN. Addison-Wesley Publishing Company, 1994. (ISBN 0-201-56368-1)

Index

Symbols

A

R

S

T

V

W

X