IRX
User's Manual

PortMaster

Internetwork Router

Part No. 950-1203A Printed in U.S.A. 6/93

REVISION HISTORY

First Edition.....Release 1.1.....9/91

Second Edition.....Release 1.7.....6/93

NOTICE

The information contained in this document is subject to change without notice.

Livingston Enterprises, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Livingston Enterprises, Inc. shall not be liable for errors contained herin or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Livingston Enterprises, Inc.

Copyright © 1993 by Livingston Enterprises, Inc.

FCC WARNING

This equipment has been tested and has been found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the operator, at his own expense, to take whatever steps are necessary to correct the interference.

TRADEMARKS

PortMaster is a trademark of Livingston Enterprises, Inc.

OpenWindows is a trademark of Sun Microsystems, Inc.

Open Look is a trademark of AT&T.

Table of Contents

Introduction 1-1

Operating Modes 1-4
Smart Features 1-5
About This Manual 1-5
Requesting Assistance 1-6

Installation 2-1

Hardware Installation 2-1
Rear Panel Layout 2-1
Configuration Switch Settings 2-2
Ethernet Configuration 2-3
Self-Test and Diagnostic Messages 2-3
Network Booting 2-3
Power Selection and Connection 2-3
WAN Ports 2-4
Ethernet Connection 2-4
Connecting Devices to the Diagnostic/Async Port 2-5
Connecting Serial Communications Devices 2-5
Connecting the Ethernet 2-7
Thin Ethernet 2-7
Thick Ethernet 2-8
Twisted Pair Ethernet 2-8
Workstation Software Installation 2-9
Loading from Tape or Floppy Diskette 2-9
Running PMinstall 2-10
IRX Internet Address Setup 2-11
Host Software Installation 2-12

Administration 3-1

PortMaster Console 3-1
Running pmconsole 3-1
pmconsole with X Windows 3-2
PortMaster Login 3-3
Global Configuration 3-4
Installation from PortMaster Console 3-8
Asynchronous Serial Port Configuration 3-10
Asynchronous Serial Port Configuration 3-10
Serial Port Parameters 3-12
Standard Mode Parameters 3-13
Extended Mode Parameters 3-15
Enabling Serial Port Parameters 3-20
Synchronous WAN Port Configuration 3-20
Synchronous WAN Port Parameters 3-22
Monitoring the PortMaster 3-24
Managing the Hosts Table 3-27
Managing the Locations Table 3-29
Managing the Passwords Table 3-29
Password Parameters 3-31
Managing the Routes Table 3-32
Packet Filters 3-34
Filter Organization 3-36
Managing the Filter Table 3-36
Configuring SNMP 3-42

RADIUS 3-46
pmconsole with an ASCII Terminal 3-47
PortMaster Login 3-48
Global Configuration 3-50
Installation from PortMaster Console 3-54
Asynchronous Port Configuration 3-56
Serial Port Parameters 3-57
Standard Mode Parameters 3-57
Extended Mode Parameters 3-60
Synchronous Port Configuration 3-64
Synchronous WAN Port Parameters 3-66
Monitoring the PortMaster 3-68
Managing the Hosts Table 3-70
Managing the Passwords Table 3-71
Password Parameters 3-73
Managing the Routes Table 3-75
Packet Filters 3-76
Filter Organization 3-77
Managing the Filter Table 3-78
Configuring SNMP 3-82
SNMP Parameters 3-83
RADIUS 3-84

Command Prompt Interface 3-86

The User Commands 3-86
Using the Commands 3-87
SET Command 3-88
Setting Global Parameters 3-88
Setting the Asynchronous Port Type 3-91
Setting Port Parameters 3-92
SHOW Command 3-100
IFCONFIG Command 3-101
PING Command 3-102
PMLOGIN Command 3-102
PTRACE Command 3-102
REBOOT Command 3-103
RESET Command 3-103
RLOGIN Command 3-103
TELNET Command 3-103
TRACEROUTE Command 3-104
QUIT, DONE, EXIT Command 3-104
SAVE Command 3-104
HELP Command 3-105
Managing the Hosts Table 3-105
ADD Command 3-106
DELETE Command 3-106
SHOW Command 3-107
Managing the Passwords Table 3-107
ADD Command 3-108
DELETE Command 3-108
SHOW Command 3-108
SET Command 3-108
SAVE Command 3-110
Managing the Routes Table 3-110
ADD Command 3-111
DELETE Command 3-111

SAVE Command 3-111
Packet Filters 3-111
Filter Organization 3-113
Filter Creation 3-113
Setting Filter Rules 3-114
Deleting Filters 3-115
Viewing Filters 3-115
Saving Filters 3-116
Saving Filters 3-116
Packet Processing 3-116
Ethernet Interface Filters 3-116
Hardwired Serial Interface Filters 3-117
Dial-In User Filters 3-117
Dial-Out Location Filters 3-118
Examples 3-118
Configuring SNMP 3-120
Enabling SNMP 3-121
Setting Community Names 3-121
Setting Read Hosts 3-121
Setting Write 3-122
Saving SNMP Configurations 3-122
Viewing SNMP Configurations 3-122

Appendix

Using Default /dev Entries A-1
Modifying your UNIX kernel A-2
Using MAKEDEV A-2

Utilities

PMcommand A-4
PMdial A-4
PMreset A-5

Specifications

Network Interface A-6
Power Requirements A-7
Environmental Operating Range A-7
Glossary A-8

Command Reference

Command List A-11
Command Options A-11

Index

Introduction _____CHAPTER 1

The PortMaster Internetwork Router IRX is an advanced datacommunications product used to extend networks over long distances using such links as DDS, T1, E1, or leased lines using modems.

The IRX provides the full functionality of an Internet Protocol (IP) Router. It attaches to a local Ethernet network and provides up to 4 high speed connections to remote sites. It utilizies industry standard protocols to provide dynamic or static routing, multilink load balancing, advanced network administration, and interoperability with other vendors products.

The IRX provides the following features and capabilities:

Hardware

- One High Speed HDLC Synchronous Port with speeds to 2.048Mbps (T1/E1)
- One 10Mbps Thick, Thin, Twisted Pair Ethernet Port
- One Async Serial Port for dialup networking or diagnostic access
- One Expansion Slot with the following options:
  - A second synchronous Port with speeds to 64Kbps
  - Three additional synchronous ports - One with speeds to 2.048Mbps & two with speeds to 64Kbps
- RS-232, RS-423, and V.35 Interfaces
- Selectable Data Rates up to 115.2Kbps on asynchronous port
- Full Modem Support and Hardware or Software Flow Control
- Hardwired Support for dedicated leased lines
- Flash Memories for easy upgrades

Administration

- Graphical Administration Software utilizing the X window system on many UNIX workstations
- All communications parameters configurable on-line

- SNMP MIB-2 Support for network administration
- Full Command Line Administration Interface
- Telnet Login Support for command line administration
- Configuration using standard ASCII terminal through diagnostic port
- Full network and communication port monitoring
- Network Downloadable Software Upgrades
- Built-in Ping Utility
- Built-in Traceroute Utility
- Outbound Telnet
- Selective Packet Tracing

General

- Network Independent Booting from local storage
- Multi-line Load Balancing for increased throughput over several lines
- Proxy ARP
- Packet Prioritization
- Alterate tftp Boot via network
- Domain Name Service (DNS) or Network Information Service (NIS)
- Adjustable Maximum Transmission Unit (MTU) on WAN ports
- One IP Address for entire router or IP Address per port
- On-demand Dialup SLIP & PPP Support
- Dial-in SLIP & PPP Support

Security

- Packet Filtering
  - Inbound and Outbound Packet Filters
  - Filter on:
    Source and Destination Addresses
    Protocol

    Source and Destination Ports
    Established Status of connection
- PPP Authentication Protocols (PAP & CHAP)
- Password Security for administrative access
- Host Security for SNMP access
- RADIUS Support (Remote Authentication Server)

Routing

- Dynamic Routing using Routing Information Protocol (RIP)
- Static Routing applied when the interface goes up or down
- Trusted Router RIP Filtering on a per interface basis
- Support for Host Routes, Subnet Routes, and Network Routes
- Selective Default Route Propagation

WAN Protocols

- Point to Point Protocol (PPP) with:
  - PPP Address/Control Field Compression
  - PPP Protocol Field Compression
  - PPP Authentication Protocols (PAP & CHAP)
  - Magic Number for loopback detection
  - Maximum Receive Unit negotiation
  - Async Control Character Map negotiation
  - IP Address Negotiation and Assignment
    Negotiated, Assigned or Specified Address
  - Van Jacobson Compressed TCP/IP
- Frame Relay
- Serial Line IP (SLIP) on async port
- Compressed Serial Line IP (CSLIP) on async port

Industry Standards

- TCP (Transmission Control Protocol)
- IP (Internet Protocol)
- RIP (Routing Information Protocol)
- SLIP & CSLIP (Serial Line Internet Protocol)
- ICMP (Internet Control Message Protocol)
- UDP (User Datagram Protocol)
- ARP (Address Resolution Protocol)
- TELNET (Telnet Protocol)
- Frame Relay (Fully compliant with RFC 1294)
- PPP (Point to Point Protocol)
  - Fully Compliant With:
    RFC 1331
    RFC 1332
    RFC 1334
  - Backward Compatible With:
    RFC 1171
    RFC 1172

Operating Modes

High Speed Synchronous serial ports - S1 and optionally S2, S3, and S4 can be configured to operate using one of the following industry standard interfaces:

CCITT V.35 - This is the industry standard for high speed serial data-communications (ie 56Kb - 2.048Mb). (Note: this mode requires a V.35 adapter cable, model DC-6).

RS-232 - This is the industry standard for serial data communications at speeds below 56Kb.

Asynchronous serial port - (S0) is preconfigured to use RS-232 or RS-423 data communications.

Ethernet port - This industry standard 10-Mbps IEEE 802.3 interface is switch selectable to utilizie one of the three available ethernet ports. These include Thinnet, 15 AUI Connector, or Twisted pair ethernet.

Smart Features

The intelligence of the IRX allow it to be configured and monitored from a remote workstation. By utilizing the X windows graphical user interface all functions of PortMaster can be accessed with the click of a mouse. This includes installation, network setup, port configurations, and I/O monitoring. If a graphical display device is not available all configuration parameters may also be set using a character mode terminal interface.

About This Manual

This manual is intended for use by those who are familiar with Workstations, Ethernet, TCP/IP and networking. Where needed, refer to your computer system documentation for complete information on that product. The manual is organized into three chapters:

Chapter 1: *Introduction* - describes the PortMaster IRX hardware and software.

Chapter 2: *Installation* - describes the steps to follow to complete the installation of the PortMaster hardware and software.

Chapter 3: *Administration* - describes the process used for configuring the serial WAN and ports and the monitoring of IRX operations. This includes:

- The X windows based PortMaster Console program.
- The ASCII Terminal based PortMaster Console program.
- The ASCII Terminal based command interface.

Appendix:

Utilities - Usage for UNIX utilities provided with distribution.
Specifications - lists the PortMaster IRX specifications.
Glossary - Definitions of terms used in the manual.
Command Reference - List of commands for the user prompt interface.
Index - Alphabetical reference for the entire manual

Requesting Assistance

If you have any questions about PortMaster, please use the following, toll-free number:

1-800-458-9966

Outside of the United States call:

510-426-0770

Installation _____CHAPTER 2

This chapter describes installing the PortMaster IRX hardware, the Workstation software, and initializing the PortMaster. The following chapter describes how to use and administer the PortMaster.

Hardware Installation

The IRX can be situated sitting either right-side up or on either side. An optional rack-mount kit is available for easy installation into a rack unit. There are no internal adjustments or modifications for the user. You should locate the unit in a clean, cool environment, such as the normal office environment.

Rear Panel Layout

Figure 2-1 shows the locations of the major features of the IRX rear panel:

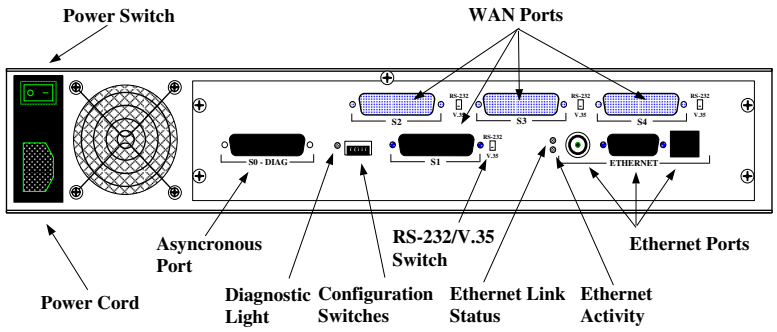

Figure 2-1. Rear Panel Layout

Power - Power switch and power cord connector.

Serial Ports - One RS-423 (RS-232 compatible) port (S0). From one to four synchronous serial ports (S1-S4). Port S1 and S3 support data rates up to 2.048 Mbps . Ports S2 and S4 support data rates up to 64Kbps.

Ethernet - Three connectors, one is a BNC (round barrel) connector for use with Thin Net. The second connector is a 15 pin AUI connector for Thick Ethernet or a compatible transceiver. The third connector is for twisted pair Ethernet (10BaseT). The active Ethernet interface is selected with the configuration switches on the rear of the IRX These configuration settings are described in the next section "Configuration Switch Settings".

Diagnostic Light - This light provides diagnostic information about the status of the IRX. When power is first applied, the system performs a hardware self test. During this time, the diagnostic light will blink several times rapidly. After successfully completing the power on self test, the light will blink on and off once each second while loading the operating system. When the system is fully operational the diagnostic light will remain on, and will blink off once every five seconds.

Ethernet Activity Light - This light blinks red whenever network traffic is detected.

Ethernet Link Status - When using Twisted Pair Ethernet (10BaseT) this light indicates the status of the link to the main hub.

Configuration Switches - These switches are used for Ethernet selection and diagnostic modes for the IRX. The following section describes the possible settings.

Configuration Switch Settings

Located on the rear panel of the unit, next to the diagnostic light, are five switches. The switches are labeled with the numbers 1 through 5 (switch 1 is closest to the diagnostic light). All switches are set at the factory to the down position. These switches are used to set the ethernet configuration, examine self-test and diagnostic messages, and use network booting when necessary.

Ethernet Configuration - The ethernet configuration is performed with switches 4 and 5 according to the following table:

Switch Setting	**4**	**5**
Thin Net	Down	Down
Thick Net (AUI)	Down	Up
Twisted Pair (10BaseT)	Up	Up

Self-Test and Diagnostic Messages - Setting switch 1 to the up position configures port S0 as the diagnostic console. During self-test and loading of the operating system, proper system operating can be verified by attaching a serial device (terminal or modem) to the S0 port at 9600 baud, 8 databits, 1 stopbit and no parity. Return switch 1 to the down position for normal operation.

Network Booting - Booting is normally performed from the FLASH Ram built into the PortMaster. Setting switch 2 to the up position allows Network Booting of the PortMaster.

Switch 3 is for future use. It should be left in the down position.

Power Selection and Connection

AC power to the IRX is connected using a standard power cable. The system uses an auto-ranging power supply which allows it to automatically adjust to match the input voltage without setting a switch. The IRX will operate correctly at any AC voltages from 100V to 260V and frequencies from 50Hz to 60Hz.

To connect power, connect the 3-conductor female plug to the rear panel of the IRX. Connect the 3-pin male plug to the appropriate source of AC power.

WAN Ports

There are up to 5 serial ports, S0 - S4. Each port utilizes a 25-pin D-type female connector. All standard RS-232 signals are available and uses the enhanced RS-423 standard. This allows for complete compatibility with

RS-232 devices as well as RS-423 devices at higher data rates and over longer distances The connection is configured as Data Terminal Equipment (DTE). In addition, the synchronous WAN ports S1-S4 can be configured to operate using a V.35 interface. A switch located to each connector selects RS-232 or V.35. When in V.35 mode, the appropriate adapter cable must be attached to create the correct interface connector.

Ethernet Connection

There are three types of Ethernet connection for the IRX

Thin Ethernet - a BNC connector for direct connection to the Workstation Thin Ethernet connector.

Thick Ethernet - the standard Ethernet D-type connector for connection to a transceiver on the Ethernet.

Twisted Pair Ethernet - a standard modular connector for direct connect to twisted pair hubs.

Which of the these is in effect for your IRX is indicated by the switch settings on the rear of the unit. Consult the section on configuring the switches for more information.

Connecting Devices to the Diagnostic/Async Port

To connect serial devices to the IRX port S0, simply connect a male RS-232 connector to the rear panel connector. This serial port is wired as Data Terminal Equipment (DTE). When connecting serial cables to this port, secure the connectors together using either a screwdriver or the finger-screws mounted to the cable connector. Pin 1 is located in the upper-right corner of each connector (the row with the most pins). The following table lists the diagnostic/asynchronous serial port connections. The directions, input/output, are with respect to the IRX. All pins not listed have no connection. In general, when connecting a modem to the port use a straight through modem cable. When connecting a terminal to the port use a null modem (pins 2 and 3 crossed) cable.

Connections for Diagnostic/Asyncronous Port

Pin	Name	Description	
2	TXD	Transmit Data	(output)
3	RXD	Receive Data	(input)
4	RTS	Request To Send	(output)
5	CTS	Clear To Send	(input)
6	DSR	Data Set Ready	(input)
7	SGND	Signal Ground	
8	DCD	Data Carrier Detect	(input)
20	DTR	Data Terminal Ready	(output)

Connecting Serial Communications Devices

The data communications ports (S1 - S4) can be configured to operate as V.35 or RS-232 compatible ports. This is done by setting the DIP switches on the rear of the unit and attaching the correct cable. The DIP switches are located to the right of each DB-25 port as shown on page 2-6.

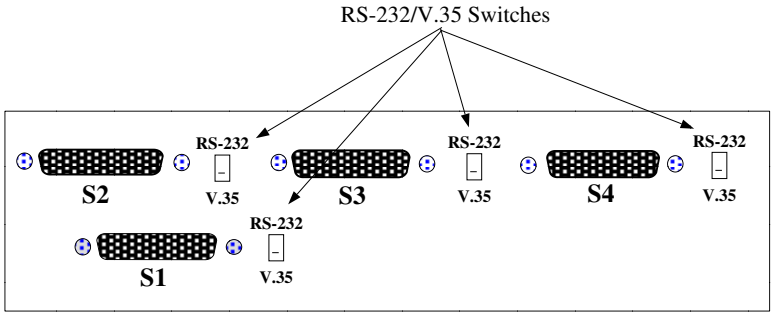

Figure 2-2. RS-232/V.35 Switch Locations

The following table lists the DTE serial port connections. The directions, input/output, are with respect to the IRX. All pins which are not listed have no connection.

Connections for Serial Ports S1 - S4 with V.35

Pin	Name	Description	
2	TXD	Transmit Data	(output)
3	RXD	Receive Data	(input)
4	RTS	Request To Send	(output)
5	CTS	Clear To Send	(input)
6	DSR	Data Set Ready	(input)
7	SGND	Signal Ground	
8	DCD	Data Carrier Detect	(input)
15	ST	Send Timing	(input)
17	RT	Receive Timing	(input)
20	DTR	Data Terminal ready	(output)
24	TT	Terminal Timing	(output)

Connections for Serial Ports 1-4 with V.35

Pin	V.35 Pin	Name	Description	
2	P	TXD	Transmit Data	(output)
14	S	TXD-		
3	R	RXD	Receive Data	(input)
16	T	RXD-		
4	C	RTS	Request To Send	(output)
5	D	CTS	Clear To Send	(input)
6	E	DSR	Data Set Ready	(input)
7	B	SGND	Signal Ground	
8	F	DCD	Data Carrier Detect	(input)
15	Y	ST	Send Timing	(input)
13	AA	ST-		
17	V	RT	Receive Timing	(input)
19	X	RT-		
20	H	DTR	Data Terminal ready	(output)
24	U	TT	Terminal Timing	(output)
12	W	TT-		

Connecting the Ethernet

To connect the Ethernet, either Thin, Twisted Pair, or Thick Ethernet, use the appropriate PortMaster rear panel connector.

Thin Ethernet

The Thin Ethernet BNC connector is the round connector on the left of the 15-pin AUI connector. Connect a coaxial cable between the IRX Thin Ethernet connector and the network. Termination is required at each end of the Thin Ethernet coaxial cable. Use the BNC T-adapter included with the IRX. Figure 2-2 illustrates a Thin Ethernet connection between the IRX and other hosts on the network.

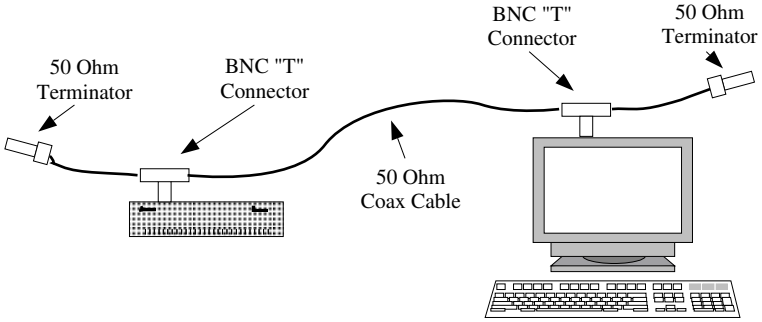

Figure 2-2. Thin Ethernet Connection

Thick Ethernet

A 15 Pin D-type connector is located on the rear panel of the IRX next to the Thin Ethernet BNC connector. Connect the Ethernet transceiver cable to the PortMaster rear panel connector. Slide the locking ring until the connection is secure.

Twisted Pair Ethernet

A modular connector for use with twisted pair Ethernet is located to the right of the 15-pin AUI connector. This connector should be attached via standard twisted pair wiring to a hub unit which supports the 10BaseT standard.

Workstation Software Installation

Included with your IRX is software on one of various forms of media. This software is available for a variety of computer platforms. Consult the Livingston availability list for the correct software for your computer system.

This software is not required when using the IRX. However, it does provide a valuable set of administration software for configuring and monitoring your IRX.

To install the software you will need to have a minimum of 3 MB of disk space.

Loading from Tape or Floppy Diskette

This procedure describes the installation of the PortMaster software on UNIX computer systems. Use the following procedure to load the Port-Master software onto your computer:

1. Log on as root.

2. Using mkdir, create a directory called /usr/portmaster. This is the recommended directory location and name. If you wish to use a different name directory, substitute that name in the following command:

mkdir /usr/portmaster

3. Change your working directory to /usr/portmaster.

cd /usr/portmaster

Note: *It is a good idea to place the portmaster directory in your path command, this will allow you to run the various executables without specifying the full path.*

4. Load the diskette or tape into the appropriate drive.

5. Type the command:

tar xvf /dev/<device>

where <device> is the raw device of your tape or diskette drive. Consult your computer system documentation for the correct device name.

For example, to load the information from a Sun Microsystems Workstation SCSI tape drive, you would type the command:

tar xvf /dev/rst0

While the software is being extracted from the tape or diskette, the list of files being extracted will be displayed. After the software has been fully extracted, go on to "Running PMinstall".

Running pminstall

At this point in the installation procedure you should be logged on as root and have the /usr/portmaster directory as your current working directory. Simply enter the command:

pminstall

After decompressing the PortMaster distribution files, your display should show the following menu:

```
1 Portmaster Internet Address Setup
2 Host Installation
3 Portmaster Upgrade
4 Host Upgrade
5 Exit

Please select an option from above:
```

Use this menu to select the appropriate option. The following paragraphs describe the functions of the first two menu selections.

IRX Internet Address Setup

On some systems, pminstall can be used to automatically notify the IRX of its Internet Address. This is done using the Reverse ARP protocol. If your system does not support this feature, you will be notified when you attempt to run this function. If this is not supported, your IRX IP address should be assigned using a terminal atttached to serial port S0 (default configuration 9600 baud, 8 databits, 1 stop bit). Consult chapter 3 on the use of the command line interface for instructions on setting the IP address.

Please verify that the new IRX has been physically connected to the network and has been powered on before starting this section. If the PortMaster is being installed onto a network which uses DNS or NIS for host information, a valid name and internet address must be assigned by the network administrator prior to running **pminstall**.

From the **pminstal** menu, select item 1, follow by RETURN. The following dialog will be displayed:

```
Please enter the PortMaster name:<portmaster_name>
```

Where <*portmaster_name*> is the "network" name you want to assign to the new PortMaster (ie. portmaster1, portmaster2, etc...). If the PortMaster and UNIX Workstation are being installed on a stand-alone network then any name may be used. If this name has not already been established as a valid network host name, you will receive the following prompt:

```
Cannot find host entry for <portmaster_name>

Would you like to add a new one? (y/n) y
Use system assigned internet address? (y/n) y
Confirm add: Host: <portmaster_name> Address:
192.9.200.2 ? (y/n) y
```

Once the PortMaster name and internet address have been verified, the following messages will appear (this may take between 5 and 20 seconds):

```
Listening on network for heartbeat of new
PortMaster ...

Found heartbeat
PortMaster internet notification complete.
```

Note: *If an error message is displayed during this step which indicates a failure to open any network devices, verify that all networking resources are installed in your UNIX kernel. On Sun Workstations, the pseudo devices: snit, pf, nbuf, and clone must be installed. Refer to the Sun installation documentation for more complete descriptions.*

When the Portmaster Internet Address Setup has completed, the main installation menu will be displayed.

```
1 Portmaster Internet Address Setup

2 Host Installation
3 Portmaster Upgrade
4 Host Upgrade
5 Exit

Please select an option from above: 5
```

At this point, the new IRX is initialized and known to the network. The next chapter, Administration, describes the administration of the IRX, port configurations and so forth. Read the section on starting and logging into the IRX and then complete the steps described in setting the Global Configuration.

Host Software Installation

This function is not used for the PortMaster IRX (it is available for Livingston Enterprises line of Communications Servers - PortMaster PM2 series).

Administration _____CHAPTER 3

PortMaster Console

PortMaster Console (**pmconsole**) is the PortMaster administration program. **pmconsole** is used to administer the Livingston Enterprises line of communications expanders and Internetwork Routers. The program uses one of two user interfaces; X Windows, or a full screen ASCII terminal. The graphical interface provides several windows through which you can configure the PortMaster ports, monitor the performance, and install other PortMasters on your network. The terminal interface provides multiple screens for performing the same functions.

Running pmconsole

To run the **pmconsole** program, enter the following command:

pmconsole *[-o] [-t] [-n]*

If no options are specified, **pmconsole** will automatically use the interface which best matches your current environment (For example if you are running X windows it will use the graphical interface). If you wish to specify a particular user interface, the optional arguments have the following uses:

-o - Use the X windows based User Interface.
-t - Use the ASCII Terminal User Interface.

In normal operation, **pmconsole** will automatically translate all IP addresses into hostnames as defined in your systems hosts database. The **-n** option causes the display of only numeric IP addresses.

The next three sections detail the use of both of the user interfaces. Please move ahead to the section which matches your operating environment.

pmconsole with X Windows

The X Windows graphical interface provides several windows through which you can configure the PortMaster ports, monitor the performance, and install other PortMasters on your network. This can be run from any X-windows compatible device.

Each window in the PortMaster Console has a set of buttons. To select a button, position the mouse cursor inside the button you wish to select and press the left mouse button. **pmconsole** uses the OpenWindows user interface. Windows can be re-positioned as with other OpenWindows applications.

When **pmconsole** is started, the window in Figure 3-1 will be displayed.

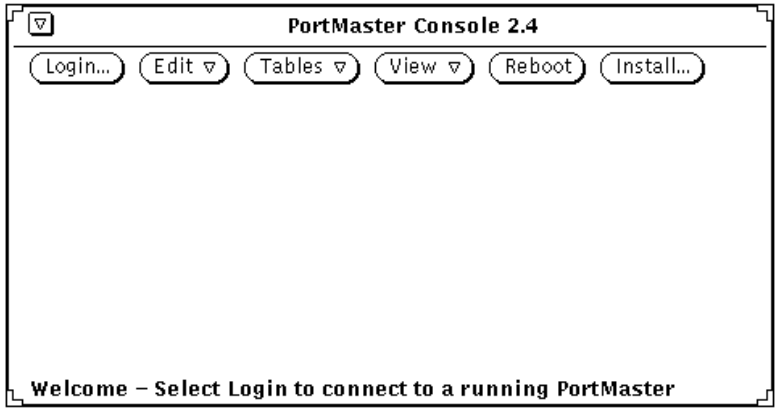

Figure 3-1. PortMaster Console login display

This is the primary window in the PortMaster Console program. From this window all other windows and functions of the software are accessible. The mouse buttons across the top of the window are used to access the various functions. PortMaster Console window has the following buttons:

- **Login** - to access any PortMaster
- **Edit** - to set the port configurations, network configurations, administration password, SNMP and RADIUS.
- **Tables** - to view and edit Dial-out Locations, User Passwords, the Hosts Table, the Static Routing Table or the Packet Filters Table.
- **View** - to view all port configurations and data traffic
- **Reboot** - to remotely reboot the PortMaster
- **Install** - to install a PortMaster onto the network or to install new software releases

A description of each of these button functions is described below.

PortMaster Login

To communicate with any PortMaster which has already been installed onto the network you must use the Login function. This function establishes a link with the PortMaster and allows you to utilize all other functions. To Login, use the following steps:

1. Place your mouse on the LOGIN button and click the left mouse button.

2. The Password Window will be displayed. Enter the PortMaster name assigned during the installation procedure. Then press <RETURN>:

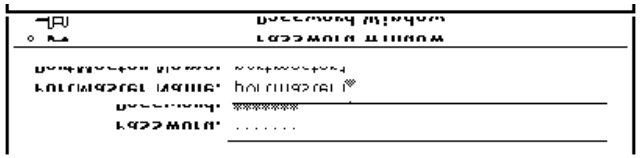

Figure 3-2. PortMaster Password Window

3. Enter the password, if any, and press <RETURN>. When the PortMaster is initially installed there is no password. There will be a message stating that the connection is being attempted. With a successful connection, the main PortMaster window (Figure 3-3) will be displayed.

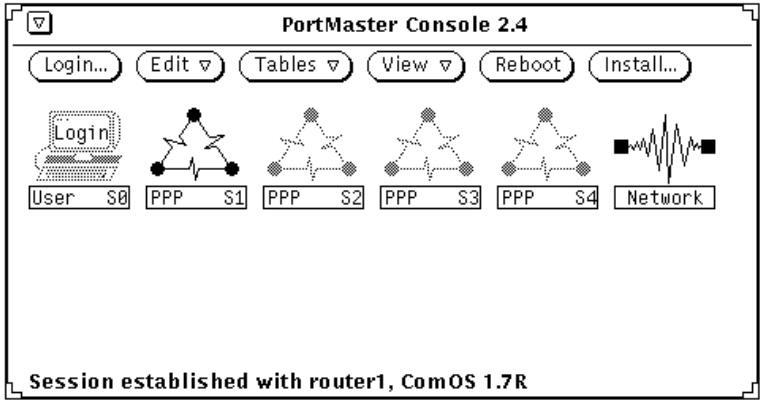

Figure 3-3. PortMaster Console icon window

The PortMaster Console window displays the port icons for the asynchronous and synchronous ports, and for the network (Ethernet and Global Configuration).

Global Configuration

After the **pminstall** program has been run, or if the PortMaster is moved to a new network, you may need to change the global configuration. The global configuration window is also used to change the PortMaster Administration password. From the PortMaster Console, do the following:

1. Position the cursor on the **Network** icon (upper right corner, and click the left mouse button. The **Network** icon will change to reverse video.

2. Select the **EDIT** button. The window in Figure 3-4 will be displayed.

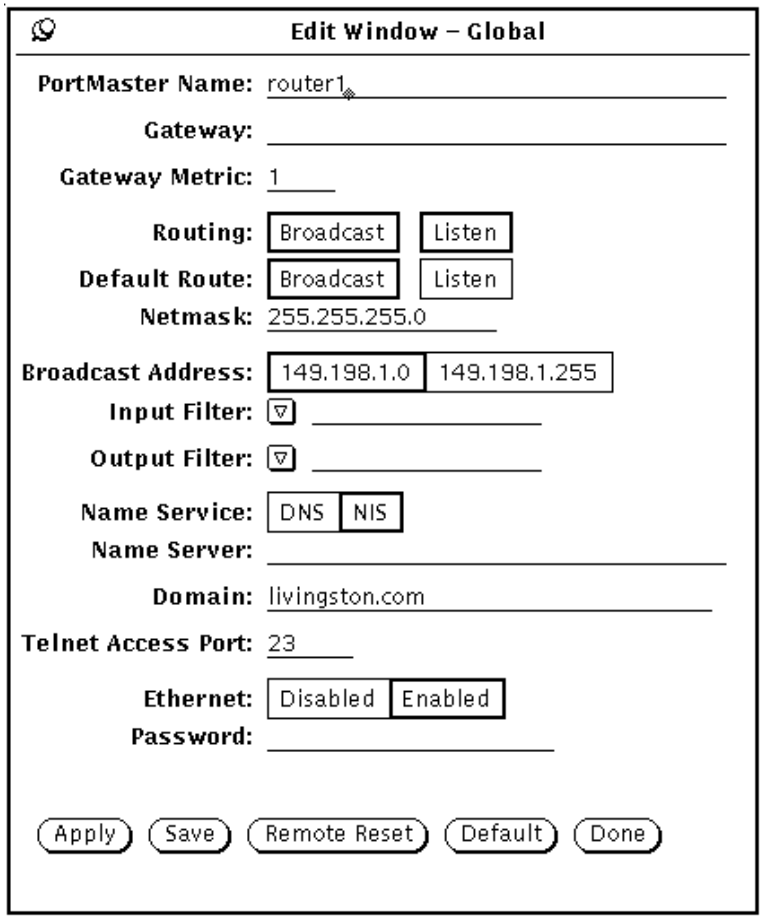

Figure 3-4. Edit Window - Global

3. Enter the following information, terminated by pressing RETURN:

- **PortMaster Name** - name or IP Address of PortMaster as entered at installation.
- **Gateway Name** - If the PortMaster is being connected to a network with gateway systems then the name of the default gateway on the same network should be entered. The PortMaster automatically routes network packets through gateways running the Routing Information Protocol (RIP), but will use the default gateway if no RIP gateways are found.
- **Gateway Metric -** If the Gateway field above is being used this value (from 1-15) is the cost associated with using the default gateway route. This is useful if the PortMaster is configured to listen for default routes coming from other routers. Otherwise this field can be left blank.
- **Routing** - This indicates whether the PortMaster should use the RIP protocol through the Ethernet Interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected the PortMaster will send RIP information to other computers attached to the local Ethernet. If "Listen" is selected, the PortMaster will accept RIP information from other routers on the local Ethernet. The default is to both Broadcast and Listen.
- **Default Route** - This option works in conjunction with the "Routing" field above. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected, the PortMaster will send default route information as part of its normal RIP messages. If "Listen" is selected, the PortMaster will accept default route information coming from other routers on the local Ethernet. The default is to not Broadcast or Listen .
- **Netmask** - defaults to 255.255.255.0. This should only be modified if your site uses sub-netting or Class A or B IP addresses. Consult you network administrator for this information.
- **Broadcast Address** - This is the IP address which the PortMaster will interpret and use as the local broadcast address. This is used by the

RIP protocol and some diagnostic protocols. This value *must* match other computers on the same local Ethernet.

- **Input Filter** - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.
- **Output Filter** - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" toward the end of this chapter
- **Name Service** - For networks which use the Network Information Service (NIS), also known as YP, the PortMaster can be configured to use this service for host name matching. Select DNS if your network is configured for Domain Name Service.
- **Name Server** - Enter the name of the server providing the name service selected above.
- **Domain** - if DNS or NIS is used the domain name must be entered.
- **Telnet Access Port** - The PortMaster allows the system administrator to access all of the PortMaster administration functions through a command line interface. These functions can be reached by logging onto the PortMaster with a telnet session. This field identifies the specific TCP port number for the PortMaster to listen on for incoming telnet administration sessions. The default value is "23". Any number from 0 to 65536 may be used. If 0 is selected, the PortMaster will disable the telnet administration function.
- **Ethernet** - This field enables the Ethernet interface of the PortMaster. It should only be disabled when the PortMaster is not being attached directly to the local Ethernet.
- **Password** - PortMaster administration password.

As each of the first three items is entered, it will be validated against your systems global host table (/etc/hosts, DNS or NIS). These were established by **pminstall** if this is a stand-alone installation, or by your network administrator. The netmask should not be changed unless you are using sub-nets and understand their operation. Refer to your UNIX system documentation for more information on sub-nets. The password entry must be entered twice, to ensure that the password was entered correctly. The password can be changed at any time by following the procedures in this section.

4. Select the **SAVE** button to store the data in the PortMaster. At the bottom of the window will be a message:

Configuration successfully saved.

5. Select the **DONE** button. At this point, the PortMaster has all the information necessary to begin normal communications with the network.

Installation from PortMaster Console

To install a PortMaster from the PortMaster Console, instead of using the program **pminstall** as described in Chapter 2, select the **INSTALL** button. The window in Figure 3-5 will appear. The option buttons in this window are the same options available with pminstall (See Chapter 2, Running **pminstall**:

- New PortMaster
- New Host
- Upgrade PortMaster
- Upgrade Host

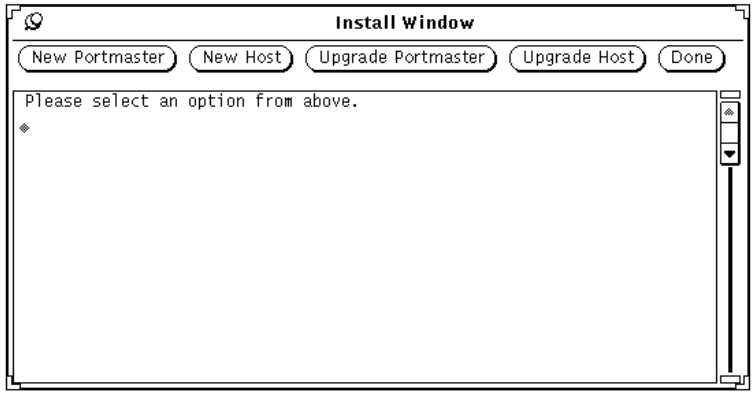

Figure 3-5. PortMaster Install window

One reason for using this method instead of running pminstall from the UNIX command line is that the workstation window can be scrolled. In this way you can view the entire setup process by using the scroll bars. The Upgrade PortMaster is used for the installation of new software releases. The Host Installation and Host Upgrade functions are not used by the PortMaster IRX products and are provided for use with the PortMaster Communications Servers.

Asynchronous Serial Port Configuration

To set the configuration of the asynchronous serial port, use the following general procedure:

1. From the PortMaster Console window, select the serial port icon by placing the mouse cursor on the icon of port S0 and clicking the left button.

2. Select the **EDIT** button. The **Edit Window** for the serial port (Figure 3-6) will appear. From this window you can modify the port configuration parameters.

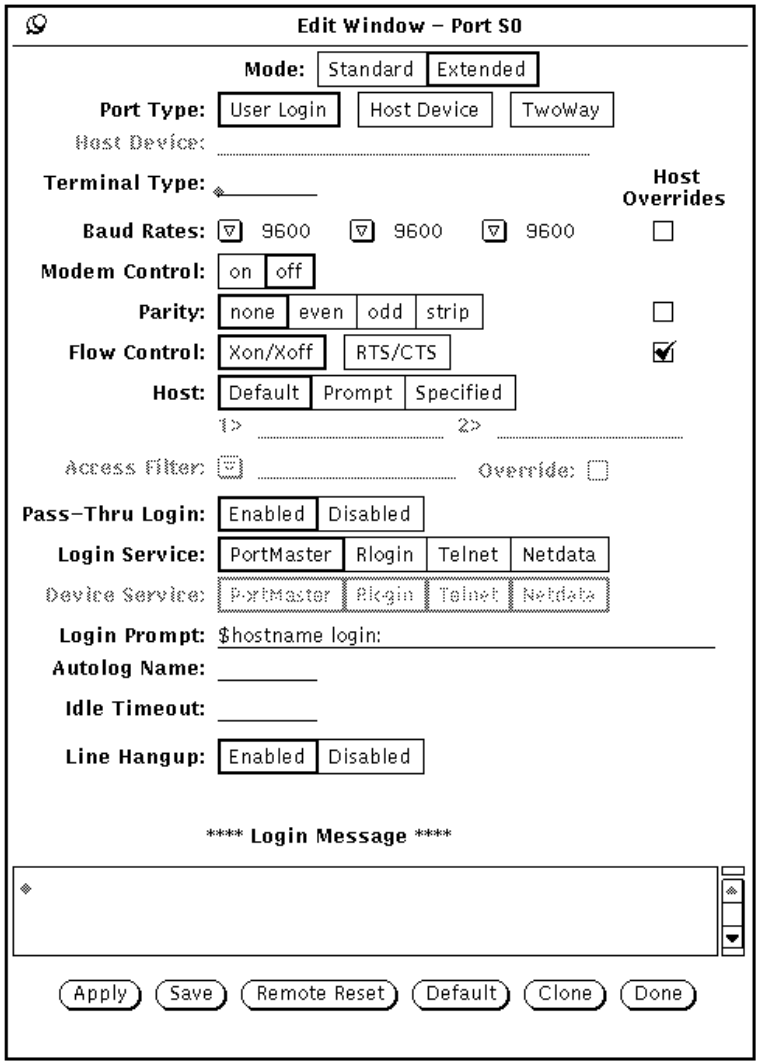

Figure 3-6. Edit Window - Serial Port

This window has the following buttons:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **REMOTE RESET**. These values are temporary until you select **SAVE**. If power is removed from the PortMaster, the new parameter values will no longer be stored in the PortMaster.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster non-volatile storage.
- **REMOTE RESET** - reset the serial port using the values stored by the **APPLY** or **SAVE** selection.
- **DEFAULT** - set the on-screen values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **DONE** - return to the PortMaster Console window.

Serial Port Parameters

This window shows the serial port parameters and the current values. Some selections have a small box with a triangle. Point to the box, click and hold the right mouse button. A menu of choices will be displayed, with a check mark next to the current value. As you move the cursor through the menu, each item, in turn, will become reverse video. When you are positioned at the value you wish to select, release the mouse button.

Some selections show all options in a horizontal line. The option which is selected has a bold box surrounding it. To select an alternate option, simply click your left mouse button on the desired option.

The serial port edit window supports two modes of operation; "Standard" and "Extended". Many users will find that the "Standard" mode will meet all of their needs. "Extended" mode is for users who wish to customize the operation of the serial port more extensively. The desired mode can be selected by selecting a **Mode** option at the top of the edit window.

Standard Mode Parameters

These are the parameters that can be selected from this window:

Port Type

User Login - the specified port will display a login prompt to the user. After successful baud rate matching and receiving a login name, the user will either be authenticated from the PortMaster passwords table or will be transferred directly to a login session on the host computer.

Host Device - the port operates as a host controlled device on the host workstation. The Host Device field described below must be entered.

Two-Way - the port will operate in User Login mode if carrier is detected on pin 8 of the RS-232 connector. Otherwise it can be accessed as a host controlled device on the host workstation. The Host Device field described below must be entered.

Dialnet (default) - This option can be selected in combination with the other Port Types if the "Dialnet Type" field is set to a value other than "Hardwired". Consult the Dialnet User's Manual for more information on this field and the "Dialnet Type" field.

Dialnet Type

This field sets the type of network access (SLIP or PPP) services supported by this port. In the hardwired mode, a direct SLIP or PPP asynchronous router connection may be established. The Dial type selections are described in the Dialnet User's Manual.

Host Device

This is field will be displayed (and is required) in either the Host Device or Two-Way modes when using the PortMaster device service. The Host Device name is the name of a pseudo tty device in the workstation directory /dev. Standard device entries are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

There is a utility included with the PortMaster software called **lstty**. This program lists only the pseudo-tty devices that are in /dev, sorted in numerical order. It is a quick way to check on what pseudo-tty devices you have in your /dev directory. This program resides in the /usr/portmaster directory. Simply use the command:

lstty

Since other programs on the host computer use these same pseudo tty devices, care should be taken in selecting the devices for the PortMaster. Each PortMaster port which binds to a specific device should be allocated a unique device name. In addition, since most dynamically allocated devices are taken from the beginning of the above list, it is recommended that devices at the end of the list be used for the PortMaster.

See Appendix A for discussion of device drivers.

Terminal Type

This optional field will be displayed in either the User Login or Two-Way modes. When a new session is established on the host workstation, this terminal type will automatically be set in the user's environment. A valid entry from the host's termcap or terminfo database should be entered. If this field is left blank, the host workstation will assume a "dumb" terminal.

Baud Rates

Three different baud rates may be specified. These baud rates are used for speed matching with the device being attached to the PortMaster. Speeds are sequentially matched from the first baud rate (left side) through the third baud rate (right side). In Host Device mode, only the first baud rate is used. With newer modems and terminals the baud rate should be set to always run at a fixed data rate. This is done by setting all three baud rates to the same value.

- First baud - the first baud rate that PortMaster uses to synchronize with the attached device. (default = 9600 baud)

- Second baud - the second baud rate that PortMaster uses to synchronize with the attached device. (default = 2400 baud)
- Third baud - the third baud rate that PortMaster uses to synchronize with the attached device. (default = 1200 baud)

Modem Control

On or off may be selected. The default is "off". If "on" is selected, the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted.

Parity

Even, odd, none, or strip may be selected. The default is "none". This value should be set to match the device being attached to the PortMaster. When even or odd is selected, 7 databits and 1 stopbit are assumed. When none or strip is selected, 8 databits and 1 stopbit are assumed. When strip is selected, the parity bit will be removed from the data as it is received by the PortMaster. See the "Command Line Interface" section if another combination is required.

Login Message

The message to be displayed to the user prior to the login prompt. Up to 240 characters can be in the message.

Extended Mode Parameters

In addition the the parameters described above in "Standard Mode Parameters", the following parameters may be set when Extended Mode is selected.

Flow Control

PortMaster supports two types of flow control:

Xon/Xoff - This is a software flow control supported by most devices. By using ASCII control characters DC1 and DC3 the PortMaster communicates with the attached device to start and stop the flow of data.

RTS/CTS - This is for devices where hardware flow control is required.

When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.

Host

The port can be configured to support three different ways of determining the Host to establish a session on:

Default - In this mode, no host will be used for the port.

Prompt - In this mode, the user is given a host prompt (before the standard login prompt). The user then is required to enter a valid host name or internet address for a host on the network.

Specified - In this mode a primary and alternate host may be entered for this specific port. When this option is selected, the additional fields will appear on the display for the entry of the host names.

Access Filter

If the PortMaster is set to prompt the user for a host on this port, an optional access control filter can be specified. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the users connection will be allowed. If not, access will be denied. In addition, if the Access Override field is checked, and access has been denied, the user will be prompted for a username and password. The user's access filter from the Password Table will then be used to determine if the users private access filter provides sufficient additional capability to allow access to the designated host.

Pass-Thru Login

If this field is enabled, user's whose names do not match the local PortMaster passwords file will automatically be forwarded to the Host specified in the "Host" field above. If this field is disabled, only users who are in the local password file will be able to logon.

Login Service

The port can be configured to use one of four different network services for establishing login sessions.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. In addition, it is the most efficient and highest performance service available.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, where it is impractical to utilize the PortMaster service, Rlogin should be selected.

Telnet - This service is generally supported by most TCP/IP computers. Therefore, in a network where mixed hardware and operating systems will be used by this port, Telnet should be selected. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used to create a virtual connection between this port and another serial port on a different PortMaster or for allowing clear channel TCP network connections from other hosts on the network. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. If using the virtual connection service, the serial port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

Device Service

The port can be configured to use one of four different network device services.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically

installed in the workstation. When selected, the port is accessed through a /dev/tty device on the host workstation.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, this service can be utilized to allow UNIX based workstations on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. When the serial port is in use, new users will be given a "Connection Refused" indication.

Telnet - This service is supported by most TCP/IP computers. Therefore, this service can be utilized to allow many different types of computers on the network to initiate a telnet session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. When the serial port is in use, new users will be given a "Connection Refused" indication. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or a similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port operating parameters are set with **pmconsole**. The application can then open the socket connection and immediately begin reading and writing data to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required.

Login Prompt

This field allows the administrator to customize the login prompt the user will see. Any valid ASCII characters may be entered. The default is to display the Host Name followed be the word "login:". If the string "$hostname" is included in the login prompt, the active hostname is substituted for the string.

Autolog Name

If this field is filled in, the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the host system as if the user had typed the **Autolog Name** in response to the login prompt.

Idle Timeout

The idle timeout specifies how long the PortMaster should wait after the activity on the port stops before disconnecting the session. The idle timeout is specified in minutes and can be any value from 0 to 240. If set to 0, no timeout will be used.

Line Hangup

If this field is enabled, the DTR signal on the RS-232 connector will be momentarily dropped to cause a hangup after the termination of a user session. If disabled, DTR will not drop after the session terminates.

Dial Group

This field is used by Dialnet for creating dial-out pools when establishing remote network connections. Consult the Dialnet User's Manual for complete information.

Host Overrides

The PortMaster allows host overrides to be selected for Baud Rate, Parity, Databits, and Flow Control. This feature allows the host to alter the active parameters via software control (i.e. system ioctl calls). Parameters which have a check mark in the box opposite them can be overridden. The default is that the Host can only turn Xon/Xoff flow control on and off. This is useful for many UNIX utilities like uucp and tip. If the parameter is not checked it cannot be overridden. In this case system requests to change these parameters will be ignored.

Enabling Serial Port Parameters

If you would like to try a new port configuration, without saving to the PortMaster permanent configuration:

1. Select **APPLY**

2. Select **REMOTE RESET**

The new port configuration will now be in effect, until power is removed from the PortMaster or changed again.

If you want to save the new configuration in the permanent PortMaster configuration, select **SAVE**.

Synchronous WAN Port Configuration

To set the configuration of the sync ports, use the following general procedure:

1. From the PortMaster Console window, select the synchronous port icon by placing the mouse cursor on one of the synchronous port icons and clicking the left button.

2. Select the **EDIT** button. The Edit Window for the synchronous port (Figure 3-7) will appear. From this window you can modify the port configuration parameters.

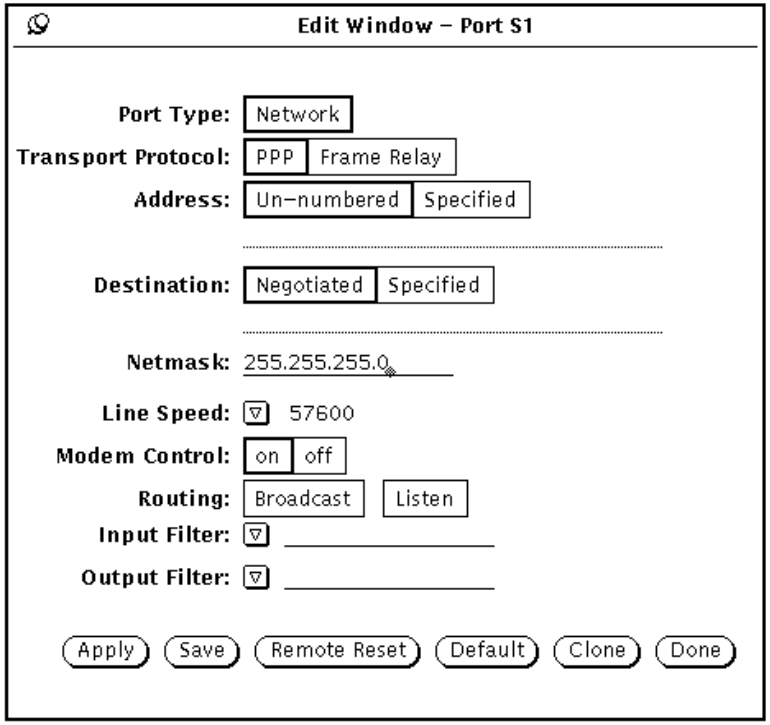

Figure 3-7. Synchronous Port Window

This window has the following buttons:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **REMOTE RESET**. These values are temporary until you select **SAVE**. If power is removed from the PortMaster, the new parameter values will no longer be stored in the PortMaster.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster non-volatile storage.
- **REMOTE RESET** - reset the port using the values stored by the **APPLY** or **SAVE** selection.

- **DEFAULT** - set the on-screen values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **DONE** - return to the PortMaster Console window.

Synchronous WAN Port Parameters

This window shows the synchronous port parameters and the current values. Some selections have a small box with a triangle. Point to the box, click and hold the right mouse button. A menu of choices will be displayed, with the current value highlighted. As you move the cursor through the menu, each item, in turn, will become reverse video. When you are positioned at the value you wish to select, release the mouse button.

Some selections show all options in a horizontal line. The option which is selected has a bold box surrounding it. To select an alternate option, simply click your left mouse button on the desired option.

Port Type

This value is always wet to Network for synchronous ports and is not configurable.

Transport Protocol

PPP - Point to Point Protocol. This protocol should be used for direct leased line connections between routers.

Frame Relay - Frame Relay should be selected when attaching the router to a Frame Relay network via a Frame Relay Switch.

Address

Un-numbered - This option may be selected for use with the PPP protocol. When selected an IP Address is not assigned directly to the port. Instead, the router's Ethernet IP Address is used to identify the router. This option eliminates the need to use extra network or subnet numbers for the Point-to-Point link.

Specified - This option must be selected for Frame Relay connections and is optional for PPP connections. When selected, an IP Address

should be entered in the line below. This IP Address is used as the address of the port on the router.

Destination - This option is only used for PPP connections. It allows you to specify the IP Address of the remote router when Specified is selected, or to Negotiate (or learn) the address of the remote router automatically via the PPP protocol option negotiation.

Netmask - This is the netmask to be used for the IP network of this port.

Line Speed - Speeds from 9600 bps up 2048K (E1 for Europe) can be selected. Actual line speed is set by the external clock from the device to which the router is attached (i.e. DSU/CSU). This setting is used for administrative reference only.

Modem Control - On or off may be selected. The default is "off". If "on" is selected, the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted.

Routing - This indicates whether the PortMaster should use the RIP protocol through the WAN Interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected the PortMaster will send RIP information to other computers attached to the WAN Interface. If "Listen" is selected, the PortMaster will accept RIP information from other routers on the WAN Interface. The default is to both Broadcast and Listen.

Input Filter - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received by this interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Output Filter - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to this interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" toward the end of this chapter.

DLCI List - When using Frame Relay, a scrolling window is provided for entering the list of DLCI's which are accessible through the Frame Relay network by this port. The PortMaster IRX will automatically use ARP and Inverse ARP requests to learn the IP Addresses of routers attached to the permanent virtual circuits represented by these DLCI's. Alternately the IP Addresses can be specified directly opposite their corresponding DLCIs. If an address is specified, the router will statically configure these entries into its ARP table.

Monitoring the PortMaster

pmconsole allows the monitoring of traffic and errors through the serial ports, as well as monitoring statistics for each of its network interfaces. The View button on the main console window allows selection of either "Ports" or "Netstats".

Port View Window

From the PortMaster Console window, select **VIEW** with your right mouse button. Then select "**Ports**" from the pull-down menu. A window similar to Figure 3-8 will be displayed.

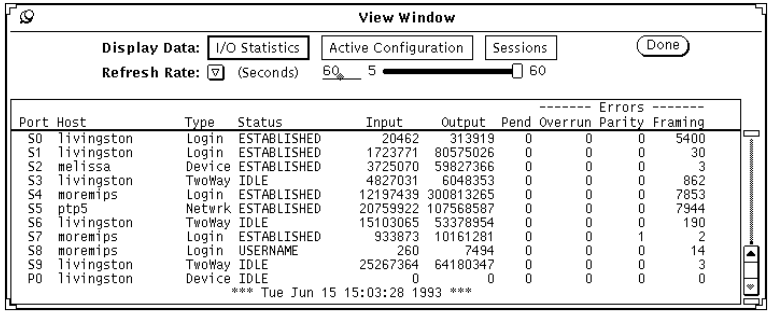

Figure 3-8. View Window

This window allows you to view the configuration and Status of each port. These values are refreshed at a specific rate as defined by the "**Refresh Rate**" values. Use the slide bar to set the **Refresh Rate**. The

Refresh Rate slide bar can be set to correspond to either seconds, minutes or hours by choosing an option from the **Refresh Rate** menu.

Three sets of data can be displayed in the view window. These are the "**I/O Statistics**", "**Active Configuration**" and the "**Sessions**". All modes display the port, its active host, the port type, and the current status of the port.

When "**Active Configuration**" is selected, the window displays data communications parameters such as baud rate, databits and parity.

When "**I/O Statistics**" is selected the window displays input and output information. There are three columns labeled: Input, Output, and Pending. These relate to the number of bytes transferred in our out the port and the number of bytes in the PortMaster output buffer which are pending to be output. There are also three error counts displayed: Overrun, Parity and Framing errors.

When "**Sessions**" is selected the window displays active user (if the session was started by a dial-up process) the direction in which the connection was started, the time since the active session was started, how long the port has been idle, and the idle timeout if one has been set.

Network Statistics

After selecting "**Netstats**" from the pop-up menu, the window in figure 3-9 will be displayed.

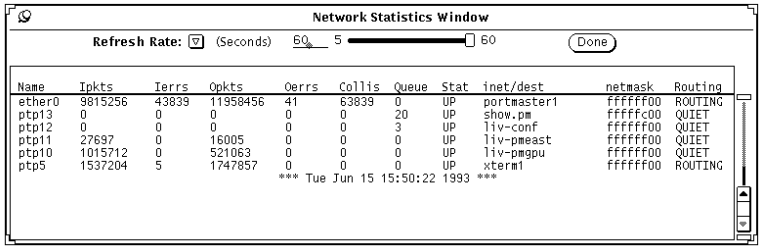

Figure 3-9. Netstats Window

This window allows you to view the Status of each network interface in the PortMaster. These values are refreshed at a specific rate as defined by the "**Refresh Rate**" values. Use the cycling-arrow icon or the slide bar to set the **Refresh Rate**. The **Refresh Rate** slide bar can be set to correspond to either seconds, minutes or hours by selection with the mouse.

The values which are displayed are:

- **Name** - The name of the network interface. The Ethernet interface is named "ether0" and each interface through the serial ports are named "ptp" or "frm", followed by a uniquely assigned number. "ptp" interfaces are using the PPP or SLIP protocol. "frm" interfaces are using Frame Relay.
- **Ipkts** - The number of input packets received by the interface.
- **Ierrs** - The number of input packets received by the interface which were dropped due to errors.
- **Opkts** - The number of output packets sent by the interface.
- **Oerrs** - The number of output packets which were not sent by the interface due to errors.
- **Collis** - The number of collisions experienced while trying to send packets out the interface.
- **Queue** - The number of packets currently queued for transmission on the interface.
- **Stat** - Either "UP" or "DOWN" indicating whether the interface is active.
- **inet/dest** - For the Ethernet interface, the internet address of the PortMaster. For the ptp interfaces, the internet address of the remote system. For frm interfaces, the internet address of the port.
- **netmask** - The netmask of the inet/dest field.
- **Routing** - "Routing", "Sending", "Listen", or "Quiet" indicating whether RIP protocol packets are being transmitted or received by the interface.

Dialer Window

The Dialer Window is used to initiate Dial-Out network connections to sites defined in the Locations Table. The Dialnet User's manual describes the use of this window.

Managing the Hosts Table

Each device attached to the network (with uses TCP/IP) is assigned a unique internet address. Internet addresses are four byte numerical values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique and easy to remember name. This is done on UNIX systems in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

If the hostname specified by the user is not found in the hosts table, then the PortMaster will attempt to match the hostname using either the Network Information Service (NIS), also known as "NIS", or DNS, the Domain Name Service See the section "Global Configuration" for more information on setting the NIS or DNS server and domain.

To view or edit the PortMaster hosts table, log in to the PortMaster and select the "**Hosts**" button from the main console.

The following window will be displayed:

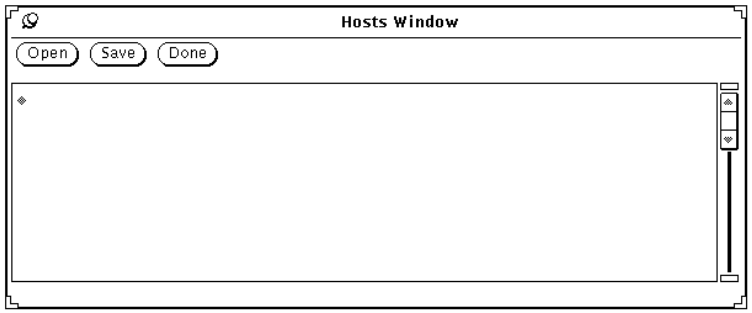

Figure 3-10. Hosts Window

The mouse buttons across the top of the Hosts window are use to access the available functions. The buttons are:

- **Open** - Retrieves the current hosts table from the PortMaster and displays it in the scrollable text window.
- **Save** - Saves the hosts entries shown in the text window as the new hosts table for the PortMaster.
- **Done** - removes the Hosts Window from view.

To edit the PortMaster hosts table use the following general procedure:

1. Select **Open** with the left mouse button. The Hosts table will be retrieved from the PortMaster, sorted in IP address order and will be displayed in the scrollable text window.

2. Make additions, deletions, and changes. All entries should have the Internet address (in the conventional '.' notation) followed by the official host name. A '#' indicates the beginning of a comment; characters up to the end of the line are ignored. This convention is identical to the /etc/hosts file on your UNIX Workstation. Therefore, the /etc/hosts file can be pasted directly into the text window.

3. After making all modifications, select "**Save**". This will store the entries in the text window in the non-volatile storage of the PortMaster.

Managing the Locations Table

The Locations table is used to manage dial-out network connections. The management of this table is described in the Dialnet User's Guide.

Managing the Passwords Table

The Passwords Table provides login security for users to establish login sessions or for incoming Dialnet network connections. This sections covers normal user security. Consult the Dialnet User's manual for information on "network" users.

Serial ports configured to accept login sessions initially prompt for a login user name. After receiving the login name, the PortMaster checks the name against the list of names in the local Passwords Table. If found, the PortMaster initiates password authentication of the user. If successfully validated (the password received matches the password stored in the Passwords Table) the PortMaster begins the session which has been defined for the user.

Two types of login users can be created; Normal and Dialback. Normal users are allowed to immediately begin an active session on a host computer somewhere on the network. Dialback users are disconnected by the PortMaster. The PortMaster then automatically dials to the users remote modem using a predefined telephone number. This feature allows for enhanced security or for simple telephone charge-back.

If the login name does not match an entry in the Passwords Table and the port is configured to support Pass-Thru Login it automatically forwards the session to the designated host on the local network for password authentication.

To view or edit the PortMaster Passwords Table, log in to the PortMaster and select the "**Tables**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "**Passwords**" from the menu.

The following window will be displayed:

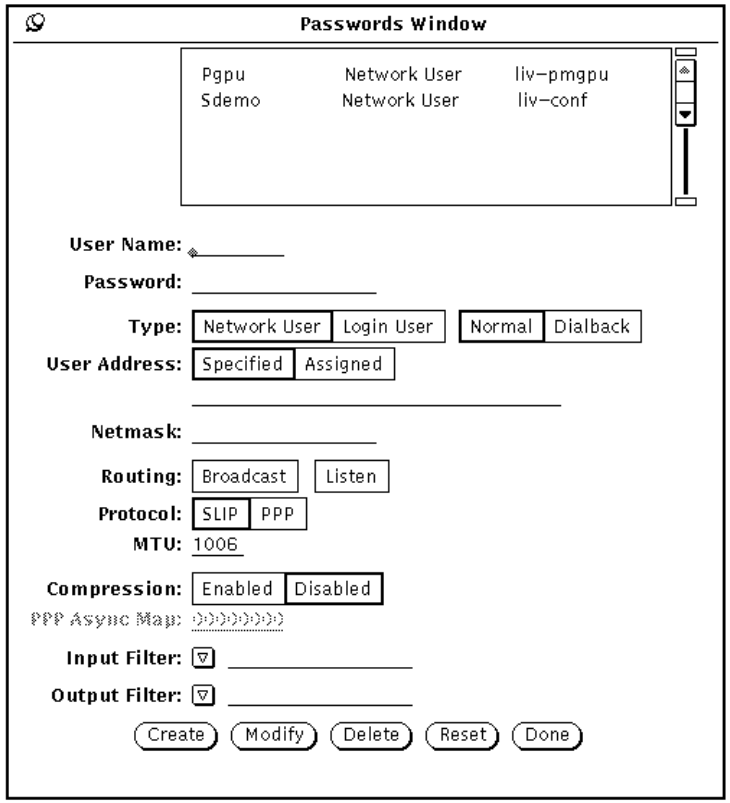

Figure 3-11. Passwords Window

The mouse buttons across the bottom of the Passwords window are use to access the available functions. The buttons are:

- **Create** - Adds the currently displayed user to the PortMaster Passwords Table.
- **Modify** - Applies modifications to the user displayed on the Passwords Window.
- **Delete** - Deletes the currently displayed user from the PortMaster Passwords Table.
- **Reset** - Clears the Passwords Window to allow the entry of a new user.
- **Done** - Removes the Passwords Window from the display.

Password Parameters

The Passwords table has 5 fields for each normal login user and 6 fields for dialback users. These fields are:

User Name

The login name of the user. This name can be up to 8 characters in length and is the user name to be supplied at the "login:" prompt from the PortMaster.

Password

The password for the user. This is a string of up to 16 ASCII characters.

Type

All login users should be set to a type of "Login User". "Network User" is specifically for Dialnet use. Consult the Dialnet User's manual for complete information. Login users can be set to "Normal" or "Dialback". Normal users will be allowed to immediately begin a login session after properly entering their user name and password. Dialback users will be disconnected by the PortMaster and then re-dialed at their pre-defined telephone number.

Host

This field defines which network host the users session will be forwarded to. The three options and their meanings are:

Default - Connect the user to the defined host for this serial port. Consult the serial port edit window for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session with.

Specified - Connect the user to the host specifically entered on the line below the Host selection. A valid hostname or IP address should be entered on here.

Login Service

The user can be set to use any of the available PortMaster Login Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual.

Telephone No

This field is only displayed for Dialback Login Users. The telephone number which should be dialed to reach the users modem must be entered in this field. Dialback only supports modems with the Hayes "AT" command set.

Access Filter

An optional access control filter can be specified for the user. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the users connection will be allowed. If not, access will be denied.

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster do not have the ability to run the RIP protocol. The static routing table contains three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. This would be the number of gateways through which the packet must traverse to reach its destination.

To view or edit the PortMaster routes table, log in to the PortMaster and select the "**Tables**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "Routes" from the menu.

The following window will be displayed:

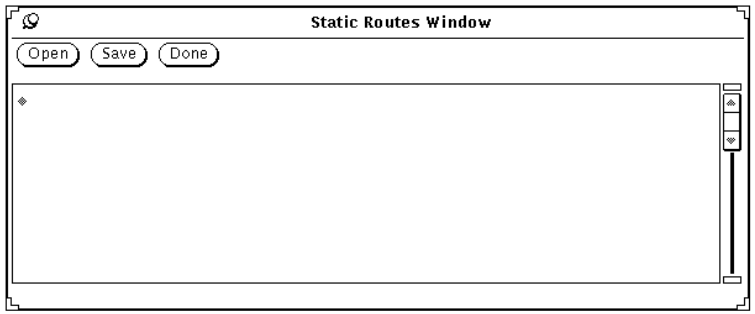

Figure 3-12. Routes Window

The mouse buttons across the top of the Routes window are use to access the available functions. The buttons are:

- **Open** - Retrieves the current routes table from the PortMaster and displays it in the scrollable text window.
- **Save** - Saves the routes entries shown in the text window as the new routes table for the PortMaster.
- **Done** - Remove the Routes Window from the display.

To edit the PortMaster routes table use the following general procedure:

1. Select **Open** with the left mouse button. The Routes table will be retrieved from the PortMaster, sorted in destination name order and will be displayed in the scrollable text window.

2. Make additions, deletions, and changes. All entries should have the destination host name, network name, or Internet address (in the conventional '.' notation or the name from the /etc/hosts file or the /etc/networks file) followed by the gateway name (in the same format). A '#' indicates the beginning of a comment; characters to the end of the line are ignored.

3. After making all modifications, select "**Save**". This will store the entries in the text window in the permanent configuration of the PortMaster.

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying the passage of packets through network interfaces. By designing appropriate filters, administrators can control access to specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allow the packet to pass freely through the interface (and on to its destination in the network) or cause the packet to be discarded without forwarding.

The Livingston packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- **Input** and **Output** Filters - Each interface can be assigned both an input-packet filter and an output-packet filter. This is especially useful in routers with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface for its

destination and the mix of inbound and outbound traffic desired for the interface. This capability also has the potential to decrease the number of rules contained in the filter because fewer network numbers need to be included.

- **Source** and **Destination Address Filtering** - Both source and destination IP addresses can be evaluated in the rule list. Also, the number of significant bits to use in the address comparison can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- **Protocol Filtering** - Specific protocols can be handled separately in the packet filters. These include TCP, UDP, and ICMP.

- **Source and Destination Port Filtering** - The source and destination port numbers can be used in the rule set to control availability of specific network services. This includes evaluation base on whether the port number is less than, equal to, or greater than a specific value.

- **Established Session Filtering** - The status of TCP connections can be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access to the local network.

- **Unlimited Number of Rules** - Each filter can have a large number of rules specified. This is only limited by available memory within the router.

- **Simple Rule Creation** - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example if the rule is not based on specific source and destination IP address, these addresses can be omitted from he specification of the rule.

- **In-line Rule Processing** - Rules are processed in the order in which they are specified in the rule set. This eliminates ambiguity about how a specific packet would be handled, and allows more flexibility in the creation of a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

Packet filters are "attached" to interfaces as either input filters or output filters. For serial interfaces, the packet filter is enabled at the time it transitions to the UP state (i.e. after a reset on the physical port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Managing the Filter Table

From the "**Tables**" pop-up menu, select "**Filters**". The screen shown below will be shown:

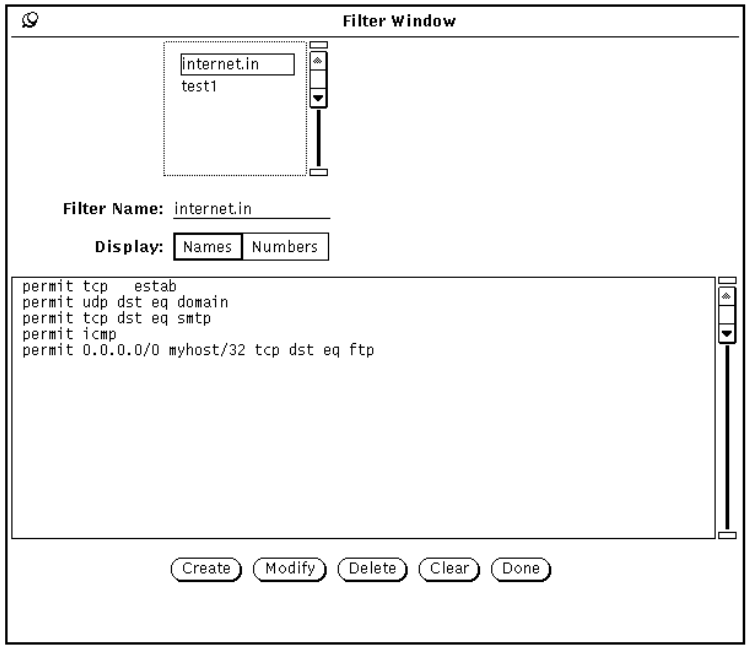

Figure 3-13 Filter Window

The mouse buttons across the bottom of the Filter window are use to access the available functions. The buttons are:

- **Create** - Adds the currently displayed filter to the PortMaster Filter Table.
- **Modify** - Applies modifications to the filter displayed on the Filter Window.
- **Delete** - Deletes the currently displayed filter from the PortMaster Filter Table.
- **Clear** - Clears the Filter Window to allow the entry of a new filter.
- **Done** - Removes the Filter Window from the display.

Filter Name

This field displays the name of the current packet filter being edited or the name of the new filter being created. Selecting a name from the scrolling list above will fill in the Filter Name.

Display

The display field can be changed at any time. When set to Names, the rules will convert IP Address to host names and port numbers to service names. When set to Numbers, IP Addresses will be displayed in standard dot notation and services will be displayed numerically.

Filter Rule Syntax

The rule set for the filter is entered on a scrollable text window. Entries can be inserted, deleted, and moved around within this window. Because packets are evaluated starting at the first rule, the most common packets which will be handled by the router should be specified first. As soon as a packet matches a rule the action specified by the rule will be immediately taken. If the packet does not match any rule, the action will be to deny the packet from traveling through the interface.

The syntax for specifying a rule is:

action [source_address/bits destination_address/bits] protocol options

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Source_address/bits - specifies the comparison with the source IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet (i.e. if 24 bits is specified, a packet with the source address of 192.9.200.1 would become 192.9.200.0 since 24 bits are used to represent the first 3 bytes of the address). The most common bit counts would be:

0 - To match packets with any source IP Address.

16 - To look at only the network number of a class B IP Address.

24 - To look at only the network number of a class C IP Address.

32 - To look at the entire IP Address.

The resulting value is then compared with the source address in the rule.

Destination_address/bits - specifies the comparison with the destination IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet. The resulting value is then compared with the destination address in the rule.

Protocol - The protocol of the packet may be specified. Valid values are TCP, UDP or ICMP.

Options - Each protocol supports a specific list of options:

TCP - This type of rule supports filtering on source and destination port numbers as well as the established state of the connection. The syntax for TCP options is:

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

Where:

src - indicates a comparison should be made with the source TCP port number.

dst - indicates a comparison should be made with the destination TCP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

estab - indicates that the packet should be tested to see if it is for an established TCP network connection. If this key word is specified packets being sent to start new TCP connections would not match this rule.

UDP - This type of rule supports filtering on source and destination port numbers. The syntax for UDP options is:

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

Where:

src - indicates a comparison should be made with the source UDP port number.

dst - indicates a comparison should be made with the destination UDP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

ICMP - This type of rule supports filtering on type of ICMP message. The syntax for ICMP options is:

[type icmp_message_type]

Where a comparison is made with the ICMP message type contained in the packet.

Examples

In figure 3-14, Rule 1 says we permit tcp packets from any foreign host if the packet is for an already established connection.

Rule 2 says we permit udp Domain Name Service packets from any foreign host.

Rule 3 says we permit Sendmail packets.

Rule 4 says we permit ftp from any foreign host but only to "myhost".

For examples of other filter rules, please refer to the "Command Prompt Interface" section of this manual.

This page intentionally left blank.

Configuring SNMP

The PortMaster provides support for using the Simple Network Management Protocol (SNMP) for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are fully described in the Livingston MIB distributed with the standard Livingston software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the software. pmconsole provides a window for configuring and enabling the SNMP facilities of the PortMaster. The SNMP edit window can be displayed by using the "Edit" button pop-up menu from the main console window. After selecting "SNMP" from this menu, the following window will be displayed:

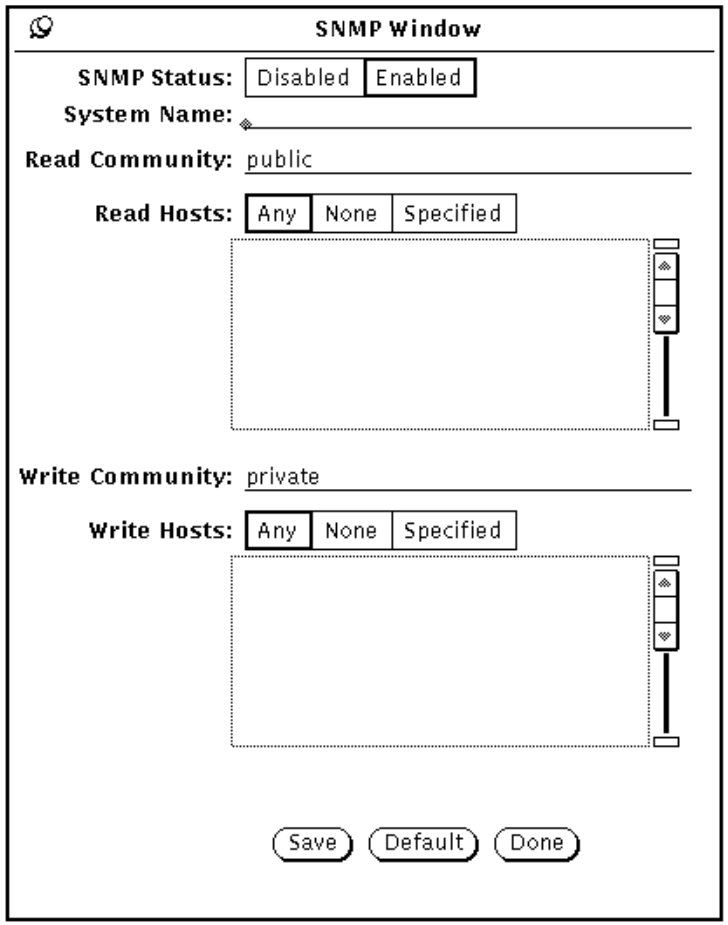

Figure 3-14. SNMP Window

This window has the following buttons:

- Save - The currently displayed configuration values will be saved in the non-volatile storage of the PortMaster.
- Default - The configuration values will be set to the factory default.
- **Done** - The SNMP window will be removed from the display.

The parameters which can be set on this window are:

SNMP Status

This field enables the SNMP capabilities of the PortMaster. If "Enabled", SNMP gets and sets will be allowed on the PortMaster. If "Disabled", SNMP queries will be ignored.

System Name

This field sets the global SNMP system name. It is used as a system identifier independent of protocols. In addition, it is used as the system identifier in PPP PAP and CHAP requests.

Read Community

The SNMP read community is generally used to segregate administrative management communities. This should be set to match the read community setting of your SNMP management software. The default is "public".

Read Hosts

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The options are:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

Specified - A specific list of hosts can perform SNMP gets from the PortMaster. The specific list must be entered in the read hosts window. To edit the list of hosts place your mouse pointer anywhere in the scrolling window. Press and hold the right mouse button to bring up the scrolling list pop-up menu. Select "Edit List". When the scrolling list pop-up menu is accessed again, use the selections to insert, change or delete entries.

Write Community

The SNMP write community is generally used to segregate

administrative management communities. This should be set to match the write community setting of your SNMP management software. The default is "private".

Write Hosts

For security purposes, the hosts which are allowed to perform SNMP sets can be set on the PortMaster. The options are:

Any - All hosts using the correct write community will be allowed to set SNMP data on the PortMaster.

None - No SNMP writes will be allowed by the PortMaster.

Specified - A specific list of hosts can perform SNMP sets on the PortMaster. The specific list must be entered in the write hosts window. To edit the list use the same procedure described for "Read Hosts".

RADIUS

The PortMaster supports RADIUS (Remote Authentication Dial In User Service). This service support authentication of users and remote routers from a centrally managed database maintained on an authentication server somewhere on the network. For information on implementing a RADIUS authentication server, see the RADIUS User's Guide. Pmconsole allows the administrator to configure the PortMaster as a RADIUS client. In this configuration, the PortMaster will first consult its local Password Table (See Password Table Maintenance earlier in this chapter), it will then consult the RADIUS server if the user is not locally defined.

From the PortMaster Console Window, select the Edit pop-up menu and select **RADIUS**. The following window will be displayed:

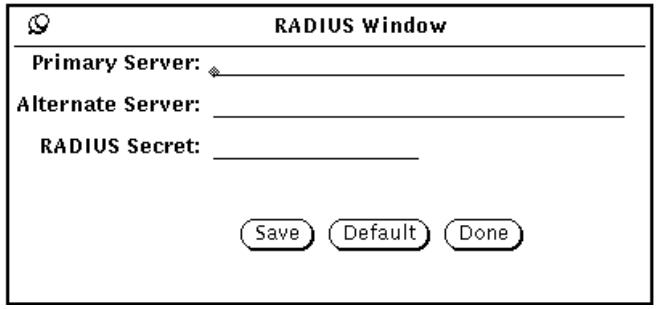

Figure 3-15. RADIUS Window

Primary Server - Enter the hostname or the IP address of the Primary Authentication Server.

Alternate Server - Enter the name of the Secondary Authentication Server.

RADIUS Secret - enter the secret used to encrypt users passwords and for verification of the responding RADIUS server. Note that when entering the RADIUS secret from **pmconsole** it is passed over the network in clear text. Alternately this secret may be entered using the command line interface directly through the asynchronous serial port on the router.

pmconsole with an ASCII Terminal

The ASCII terminal interface provides several screens through which you can configure the PortMaster ports, monitor the performance, and install other PortMasters on your network. This can be run from any ASCII terminal logged onto a UNIX Workstation which supports full screen addressing and has an entry in the termcap or terminfo database. Before running **pmconsole** verify that your TERM environment variable matches your terminals entry in the termcap database. If the screen display is unreadable, the wrong terminal type has probably been specified. Press the "Control" key and the letter "C" to exit the program and consult with your system administrator on the proper setting of your terminal type.

When **pmconsole** is started, the screen in Figure 3-16 will be displayed.

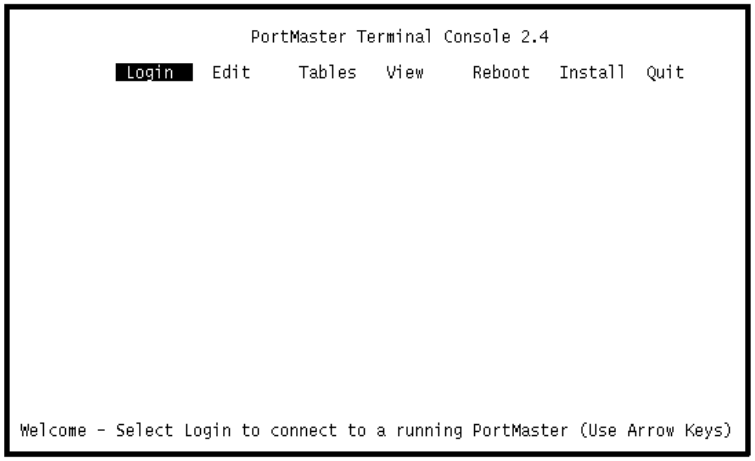

Figure 3-16. PortMaster Console login display

This is the primary screen in the PortMaster Console program. From this screen all other screens and functions of the software are accessible. The list of commands across the top of the screen are used to access the various functions. A function is selected by using the arrow keys or by

typing the first letter of one of the commands. Once the command has been highlighted, pressing the <RETURN> key will cause it to be executed. The PortMaster Console screen has the following commands:

- **Login** - to access any PortMaster
- **Edit** - to set the port configurations, network configurations and administration password
- **Tables** - to view and edit Dial-out Locations, User Passwords, the Hosts Table, or the Static Routing Table
- **View** - to view all port configurations and data traffic for the PortMaster
- **Reboot** - to remotely reboot the PortMaster
- **Install** - to install a PortMaster onto the network or to install new software releases
- **Quit** - to exit the PortMaster Console program

A detailed description of each of these functions is described below.

PortMaster Login

To communicate with any PortMaster which has already been installed onto the network you must use the Login function. This function establishes a link with the PortMaster and allows you to utilize all other functions. To Login, use the following steps:

1. Move the reverse video box over the LOGIN command and press <RETURN>.

2. The Password prompts will be displayed. Enter the PortMaster name which was assigned during the installation procedure. Then press <RETURN>. For example enter:

PortMaster Name: portmaster1

3. Enter the password, if any, and press <RETURN>. When the PortMaster is initially installed there is no password. Then, a message stating the connection is being attempted will appear. With a successful connection, the main PortMaster screen (Figure 3-17) will be displayed.

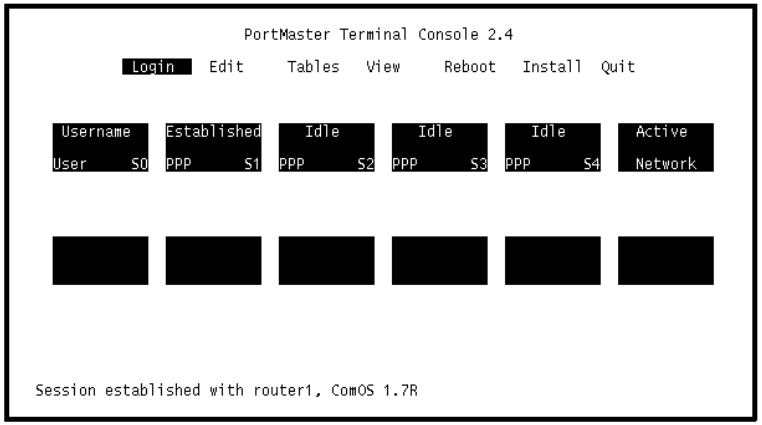

Figure 3-17. PortMaster Console screen

The PortMaster Console screen displays the port statuses for the serial port and for the network (Ethernet and Global Configuration).

Global Configuration

After the **pminstall** program has been run, or if the PortMaster is moved to a new network, you will need to tell it about the network internet addresses and the global configuration parameters. In addition, the global configuration screen is used to change the PortMaster Administration password. From the PortMaster Console, do the following:

1. Select the **EDIT** command. A new menu listing all of the ports and the Network will be displayed. Highlight the "**NETWORK**" command using the arrow keys and press <RETURN>.

2. The screen in Figure 3-18 will be displayed.

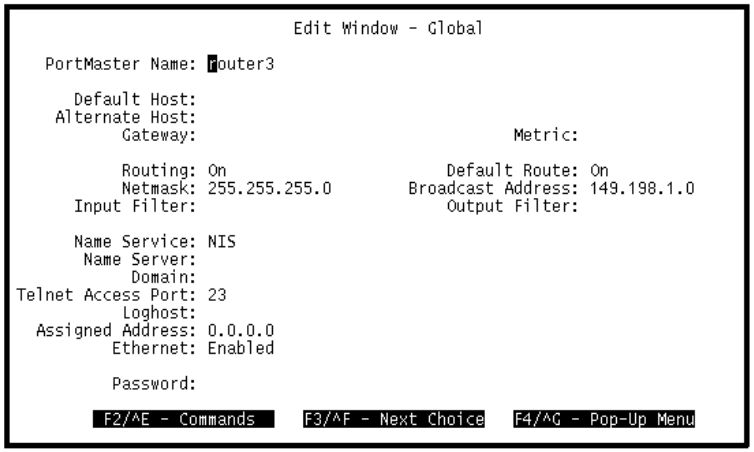

Figure 3-18. Edit screen - Global

3. Enter the following information, terminated by pressing RETURN:

- **PortMaster Name** - name of PortMaster as entered during the installation procedure.
- **Default Host** - This is left blank on the IRX.
- **Alternate Hosts** - This is left blank on the IRX.

- **Gateway Name** - If the PortMaster is being connected to a network with gateway systems, then the name of the default gateway on the same network should be entered. The PortMaster automatically routes network packets through gateways which are running the Routing Information Protocol (RIP), but will use the default gateway if no RIP gateways are found.
- **Gateway Metric** - If the Gateway field above is being used, this value (from 1-15) is the cost associated with using the default gateway route. This is useful if the PortMaster is configured to listen for default routes coming from other routers. Otherwise, this field can be left blank.
- **Routing** - This indicates whether the PortMaster should use the RIP protocol through the Ethernet Interface. The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

On - The PortMaster will send RIP information to other computers attached to the local Ethernet and will accept RIP information from other routers on the local Ethernet.

Broadcast - The PortMaster will send RIP information to other computers attached to the local Ethernet.

Listen - The PortMaster will accept RIP information from other routers on the local Ethernet.

Off - The PortMaster will not send RIP information to the local Ethernet and it will ignore all RIP messages it receives on the local Ethernet.

- **Default Route** - This option works in conjunction with the "Routing" field above. The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

On - The PortMaster will send default route information as part of its normal RIP messages and will accept default route information coming from other routers on the local Ethernet.

Broadcast - The PortMaster will send default route information as part of its normal RIP messages.

Listen - The PortMaster will accept default route information coming

from other routers on the local Ethernet.

Off - The PortMaster will not send default route information to the local Ethernet and it will ignore all default route messages it receives on the local Ethernet.

- **Netmask** - defaults to 255.255.255.0. This should only be modified if your site uses subnetting or Class A or B IP addresses. Consult you network administrator for this information.
- **Broadcast Address** - This is the IP address which the PortMaster will interpret and use as the local broadcast address. This is used primarily by the RIP protocol and some diagnostic protocols. This value should match other computers on the same local Ethernet. This can be selected by using the "Next Choice" function key.
- **Input Filter** - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Input Filters" toward the end of this chapter.
- **Output Filter** - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Output Filters" toward the end of this chapter
- **Name Service** - For networks which use the Network Information Service (NIS), also known as YP, the PortMaster can be configured to use this service for host name matching. Select DNS if your network is configured for Domain Name Service.
- **Name Server** - Enter the name of the server providing the name service selected above.
- **Telnet Admin Port** - The PortMaster allows the system administrator to access all of the PortMaster administration functions through a command line interface. These functions can be reached by logging

onto the PortMaster with a telnet session. This field identifies the specific TCP port number for the PortMaster to listen on for incoming telnet administration sessions. The default value is "23". Any number from 0 to 65536 may be used. If 0 is selected, the PortMaster will disable the telnet administration function.

- **Loghost** - The PortMaster supports the "syslog" network accounting function. If a host is entered in this field, the PortMaster will log user authentication information to this host using the system facility "auth" and the priority of "info" (auth.info). Consult your system's syslogd and /etc/syslog.conf manual pages for more information on these services.
- **Assigned Address** - This field is used in conjunction with Dialnet. It is only used for network login users using the PPP protocol who are being assigned a temporary IP address for their active session. Consult the Dialnet User's Manual for complete information.
- **Ethernet** - This field enables the Ethernet interface of the PortMaster. It should only be disabled when the PortMaster is not being attached directly to the local Ethernet. This can be selected by using the "Next Choice" function key.
- **Password** - PortMaster administration password.

As each of the first three items is entered, it will be validated against your systems global host table (/etc/hosts or Yellow Pages). These were established by pminstall if this is a stand-alone installation, or by your network administrator. The Netmask should not be changed unless you are using sub-nets and understand their operation. Refer to your workstation documentation for more information on sub-nets.

4. You will notice a function key label at the bottom of the screen. This indicates that by pressing function key F2 or by pressing down the "Control" key and typing the letter "E" the commands menu will be displayed. To save the configuration data in the PortMaster, press F2 and select SAVE from the command list. At the bottom of the screen will be a message:

Configuration parameters successfully saved.

5. Select the DONE command. At this point, the PortMaster has all the information necessary to begin normal serial communications with its host.

Installation from PortMaster Console

To install a PortMaster from the PortMaster Console, instead of using the program pminstall as described in Chapter 2, select the INSTALL command. The screen in Figure 3-18 will appear. The option commands in this screen are the same options available with pminstall (See Chapter 2, Running pminstall):

- New PortMaster
- New Host
- Upgrade PortMaster
- Upgrade Host

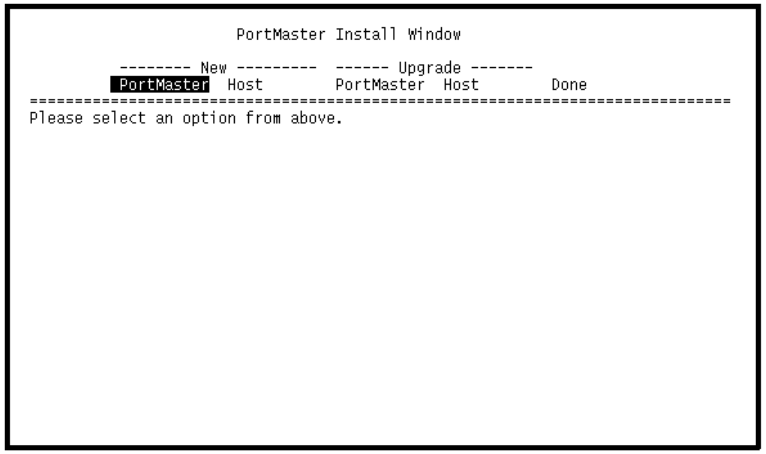

Figure 3-19. PortMaster Install screen

Asynchronous Port Configuration

To set the configuration of port s0, use the following general procedure:

1. Select the **EDIT** command. A new menu listing all of the ports and the Network will be displayed. Highlight the Serial Port using the arrow keys and press <RETURN>.

2. The Edit screen for all ports (Figure 3-20) will appear. From this screen you can modify the serial port configuration parameters.

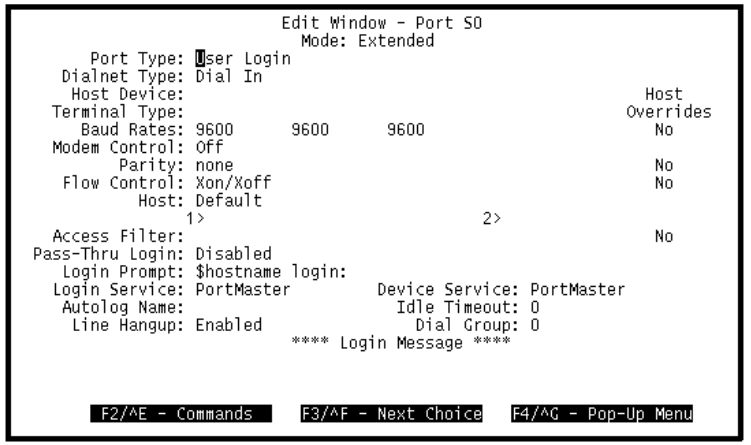

Figure 3-20. Edit screen - Serial Port

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time. . When the F2 or "Control-E" key is pressed, the function key is replaced by a menu of commands which can be executed. The available commands are:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **REMOTE RESET**. These values are temporary until you select **SAVE**. If power is removed from the

PortMaster, the new parameter values will no longer be stored in the PortMaster.

- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster permanent configuration.
- **RESET** - reset the serial port using the values stored by the **APPLY** or **SAVE** selection.
- **GENERIC** - set the on-screen values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **EDIT** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **DONE** - return to the PortMaster Console screen.

Serial Port Parameters

This screen displays the serial port parameters and the current values. Some selections have menus. To use the menu, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. Alternately the selections can be rotated through with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The serial port edit screen supports two modes of operation; "Standard" and "Extended". Many users will find that the "Standard" mode will meet all of their needs. "Extended" mode is for users who wish to customize the operation of the serial port more extensively. The desired mode can be selected by choosing a **Mode** option at the top of the edit screen.

Standard Mode Parameters

These are the parameters that can be selected from this screen:

Port Type *(menu field)*

User Login - (default) the specified port will display a login prompt to the user. After successful baud rate matching and receiving a login

name, the user will be transferred directly to a login session on the host workstation.

Host Device - the port will operate as a host controlled device on the host workstation. The Host Device field described below must be entered.

Two-Way - (or bidirectional) the port will operate in User Login mode if carrier is detected on pin 8 of the RS-232 connector. Otherwise it can be accessed as a host controlled device on the workstation. The Host Device field described below must be entered.

Dialnet - This option will be displayed only if Dialnet has been enabled from the Global Configuration Window. This option can be selected in combination with the other Port Types if the "Dialnet Type" field is set to a value other than "Hardwired". Consult the Dialnet User's Manual for more information on this field and the "Dialnet Type" field.

Host Device *(keyboard entry field)*

This is field will be displayed (and is required) in either the Host Device or Two-Way modes. The Host Device name is the name of a pseudo tty device in the workstation directory /dev. Standard device entries are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

There is a utility included with the PortMaster software called lstty. This program lists only the pseudo-tty devices that are in /dev, sorted in numerical order. It is a quick way to check on what pseudo-tty devices you have in your /dev directory. This program resides in the /usr/portmaster directory. Simply use the command:

lstty

Since other programs on the host computer use these same pseudo tty devices, care should be taken in selecting the devices for the PortMaster. Each PortMaster port which binds to a specific device should be allocated a unique device name. In addition, since most dynamically allocated

devices are taken from the beginning of the above list, it is recommended that devices at the end of the list be used for the PortMaster.

See Appendix A for discussion of device drivers.

Terminal Type *(keyboard entry field)*

This optional field is used in either the User Login or Two-Way modes. When a new session is established on the host workstation, this terminal type will automatically be set in the user's environment. A valid entry from the termcap file should be entered. If this field is left blank, the host computer will assume a "dumb" terminal.

Baud Rates *(menu field)*

Three different baud rates may be specified. These baud rates are used for speed matching with the device being attached to the PortMaster. Speeds are sequentially matched from the first baud rate (left side) through the third baud rate (right side). In Host Device mode, only the first baud rate is used.

- First baud - the first baud rate that PortMaster uses to synchronize with the attached device. (default = 9600 baud)
- Second baud - the second baud rate that PortMaster uses to synchronize with the attached device. (default = 2400 baud)
- Third baud - the third baud rate that PortMaster uses to synchronize with the attached device. (default = 1200 baud)

Modem Control *(menu field)*

On or off may be selected. The default is "off". If "on" is selected the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted.

Parity *(menu field)*

Even, odd, or none may be selected. The default is "none". This value should be set to match the device being attached to the PortMaster. When even or odd is selected, 7 databits and 1 stopbit are assumed. When none is selected, 8 databits and 1 stopbit are assumed. See the

"Extended Mode Parameters" section if another combination is required.

Login Message *(keyboard entry field)*

The message to be displayed to the user prior to the login prompt. Up to 255 characters can be in the message.

Extended Mode Parameters

In addition the the parameters described above in "Standard Mode Parameters", the following parameters may be set when Extended Mode is selected.

Flow Control *(menu field)*

PortMaster supports two types of flow control:

Xon/Xoff - This is a software flow control which is supported by most devices. By using ASCII control characters DC1 and DC3 the PortMaster communicates with the attached device to start and stop the flow of data.

RTS/CTS - This is for devices where hardware flow control is required. When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.

Host *(menu field)*

The port can be configured to support three different ways of determining the host to establish a session on:

Default - In this mode, the host entries entered in the global (network) edit screen are used for this port.

Prompt - In this mode, the user is given a host prompt (before the standard login prompt). The user then is required to enter a valid host name or internet address for a host on the network.

Specified - In this mode a primary host and up to three alternate hosts may be entered for this specific port. In this way each port can be

independently assigned to a specific host computer. When this option is selected, the additional fields will appear on the display for the entry of the host names. Ports which are configured for User Login will automatically switch to an alternate host if the Primary Host is unavailable (i.e. host 1 is down or network is unreachable). Login connections are attempted in the order in which the host names are entered. The first (or primary) host is required. The remaining hosts are optional and may be left blank.

Login Service *(menu field)*

The port can be configured to use one of four different network services for establishing login sessions.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either pminstall or the install window of pmconsole. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. In addition it is the most efficient and highest performance service available.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, where it is impractical to utilize the PortMaster service, Rlogin should be selected.

Telnet - This service is generally supported by a most TCP/IP computers. Therefore, in a network where mixed hardware and operating systems will be used by this port, Telnet should be selected. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used to create a virtual connection between this port and another serial port on a different PortMaster. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. The serial port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

Device Service *(menu field)*

The port can be configured to use one of four different network device services.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either pminstall or the install window of pmconsole. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. When selected, the port is accessed through a /dev/tty device on the host workstation.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, this service can be utilized to allow UNIX based workstations on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" indication.

Telnet - This service is generally supported by a most TCP/IP computers. Therefore, this service can be utilized to allow many different types of computers on the network to initiate a telnet session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" indication. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or a similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port

operating parameters are set with pmconsole. The application can then open the socket connection and immediately begin reading and writing data to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. If multiple ports on the PortMaster are configured to use this service with the same TCP port number, it will automatically create a "pool" of ports which can be accessed by other hosts.

Login Prompt *(keyboard entry field)*

This field allows the administrator to customize the login prompt the user will see. Any valid ASCII characters may be entered. The default is to display the Sun Host Name followed be the word "login:". If the string "$hostname" is included in the login prompt, the active Sun hostname is substituted for the string.

Autolog Name *(keyboard entry field)*

If this field is filled in, the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the Sun Workstation as if the user had typed the **Autolog Name** in response to the login prompt.

Idle Timeout

The idle timeout specifies how long the PortMaster should wait after the activity on the port stops before disconnecting the session. The idle timeout is specified in minutes and can be any value from 0 to 240. If set to 0, no timeout will be used.

Line Hangup

If this field is enabled, the DTR signal on the RS-232 connector will be momentarily dropped to cause a hangup after the termination of a user session. If disabled, DTR will not drop after the session terminates.

Pass-Thru Login *(menu field)*

If this field is enabled, user's whose names do not match the local

PortMaster passwords file will automatically be forwarded to the Host specified in the "Host" field above. If this field is disabled, only users who are in the local password file will be able to logon.

Dial Group *(keyboard entry field)*

This field is used by Dialnet for creating dial-out pools when establishing remote network connections. Consult the Dialnet User's Manual for complete information.

Host Overrides *(menu field)*

The PortMaster allows host overrides to be selected for Baud Rate, Parity, Databits, and Flow Control. This feature allows the host to alter the active parameters via software control (i.e. system ioctl calls). Parameters which have a check mark in the box opposite them can be overridden. The default is that the Host can only turn Xon/Xoff flow control on and off. This is useful for many UNIX utilities like uucp and tip. If the parameter is not checked it cannot be overridden. In this case system requests to change these parameters will be ignored.

Access Filter

If the PortMaster is set to prompt the user for a host on this port, an optional access control filter can be specified. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the users connection will be allowed. If not, access will be denied. In addition, if the Access Override field is checked, and access has been denied, the user will be prompted for a username and password. The user's access filter from the Password Table will then be used to determine if the users private access filter provides sufficient additional capability to allow access to the designated host.

Enabling Serial Port Parameters

If you would like to try a new port configuration, without saving to the PortMaster permanent configuration:

1. Select F2 (or Control-E) to view the Commands Menu.

Select **APPLY** from this menu.

2. Select **REMOTE RESET** from the Commands Menu.

The new port configuration will now be in effect, until the PortMaster is rebooted, the power is removed from the PortMaster or the parameters are changed again and applied.

If you want to save the new configuration in the permanent PortMaster configuration, select **SAVE** from the Commands Menu.

Synchronous Port Configuration

To set the configuration of the synchronous ports, use the following general procedure:

1. Select the **EDIT** command. A new menu listing all of the ports and the Network will be displayed. Highlight the Synchronous Port using the arrow keys and press <RETURN>.

2. The Edit screen for all ports (Figure 3-21) will appear. From this screen you can modify the synchronous port configuration parameters.

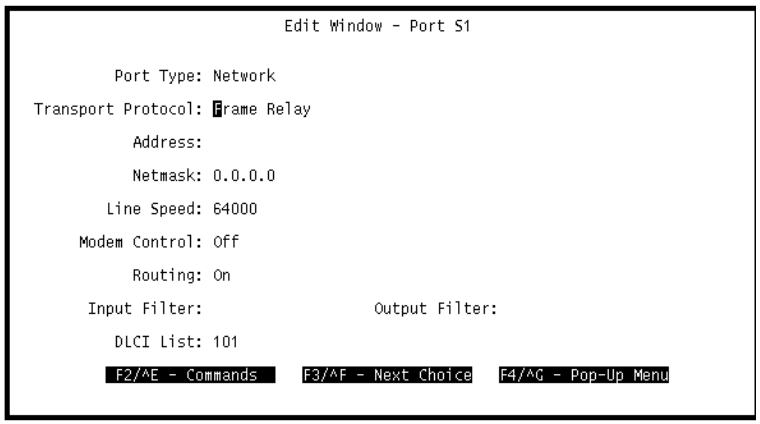

Figure 3-21. Synchronous Port Edit Window

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time. The function keys and their meanings are:

When the F2 or "Control-E" key is pressed, the function key is replaced by a menu of commands which can be executed. The available commands are:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **REMOTE RESET**. These values are temporary until you select **SAVE**. If power is removed from the PortMaster, the new parameter values will no longer be stored in the PortMaster.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster non-volatile storage.
- **REMOTE RESET** - reset the port using the values stored by the **APPLY** or **SAVE** selection.
- **DEFAULT** - set the on-screen values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **DONE** - return to the PortMaster Console window**.**

Synchronous WAN Port Parameters

This window shows the synchronous port parameters and the current values. Some selections have a small box with a triangle. Point to the box, click and hold the right mouse button. A menu of choices will be displayed, with the current value highlighted. As you move the cursor through the menu, each item, in turn, will become reverse video. When you are positioned at the value you wish to select, release the mouse button.

Some selections show all options in a horizontal line. The option which is selected has a bold box surrounding it. To select an alternate option, simply click your left mouse button on the desired option.

Port Type

This value is always wet to Network for synchronous ports and is not configurable.

Transport Protocol

PPP - Point to Point Protocol. This protocol should be used for direct leased line connections between routers.

Frame Relay - Frame Relay should be selected when attaching the router to a Frame Relay network via a Frame Relay Switch.

Address

Un-numbered - This option may be selected for use with the PPP protocol. When selected an IP Address is not assigned directly to the port. Instead, the router's Ethernet IP Address is used to identify the router. This option eliminates the need to use extra network or subnet numbers for the Point-to-Point link.

Specified - This option must be selected for Frame Relay connections and is optional for PPP connections. When selected, an IP Address should be entered in the line below. This IP Address is used as the address of the port on the router.

Destination - This option is only used for PPP connections. It allows you to specify the IP Address of the remote router when Specified is selected, or to Negotiate (or learn) the address of the remote router automatically via the PPP protocol option negotiation.

Netmask - This is the netmask to be used for the IP network of this port.

Line Speed - Speeds from 9600bps up 2048K (E1 for Europe) can be selected.

Modem Control - On or off may be selected. The default is "off". If "on" is selected, the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted.

Routing - This indicates whether the PortMaster should use the RIP

protocol through the WAN Interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected the PortMaster will send RIP information to other computers attached to the WAN Interface. If "Listen" is selected, the PortMaster will accept RIP information from other routers on the WAN Interface. The default is to both Broadcast and Listen.

Input Filter - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received by this interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Output Filter - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to this interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" toward the end of this chapter.

DLCI List - When using Frame Relay, a row is provided for entering the list of DLCI's which are accessible through the Frame Relay network by this port. The PortMaster IRX will automatically use ARP and Inverse ARP requests to learn the IP Addresses of routers attached to the permanent virtual circuits represented by these DLCI's. Alternately the IP Addresses can be specified directly opposite their corresponding DLCIs. If an address is specified, the router will statically configure these entries into its ARP table.

Monitoring the PortMaster

pmconsole allows the monitoring of traffic and errors through the serial and parallel ports, as well as monitoring statistics for each of its network interfaces. The View command on the main console screen allows selection of either "Ports" or "Netstats".

Port View Window

From the PortMaster Console screen, select the VIEW command. Then select "Ports" from the menu. A screen similar to Figure 3-22 will be displayed.

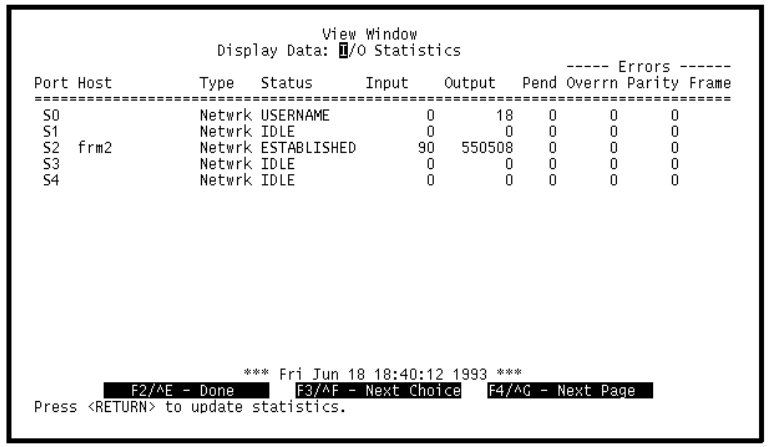

Figure 3-22. View Ports screen

This screen allows you to view the configuration and Status of each port. These values are refreshed each time you press the <RETURN> key.

Three sets of data can be displayed in the view screen. These are the "Active Configuration", "I/O Statistics" and "Session All three display the port, the port type, and the current status of the port.

When "**Active Configuration**" is selected (using F3 or F4 function keys), the screen displays data communications parameters such as baud rate, databits and parity.

When "**I/O Statistics**" is selected the screen displays input and output information. There are three columns labeled: Input, Output, and Pending. These relate to the number of bytes transferred in or out the port and the number of bytes in the PortMaster output buffer which are pending to be output. There are also three error counts displayed: Over-

run, Parity and Framing errors.

When "**Sessions**" is selected the window displays active users (if the session was started by a dial-up process) the direction in which the connection was started, the time since the active session was started, how long the port has been idle, and the idle timeout if one has been set.

Network Statistics

After selecting "Netstats" from the VIEW menu, the screen in figure 3-23 will be displayed.

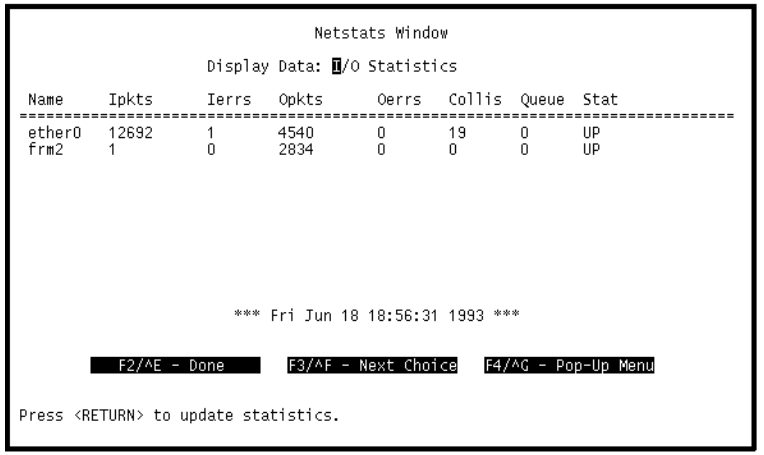

Figure 3-23. Netstats Screen

This screen allows you to view the Status of each network interface in the PortMaster. These values are refreshed each time you press <RETURN>.

The values which are displayed are:

- **Name** - The name of the network interface. The Ethernet interface is named "ether0" and each interface through the serial ports are named "ptp", followed by a uniquely assigned number.

- **Ipkts** - The number of input packets received by the interface.
- **Ierrs** - The number of input packets received by the interface which were dropped due to errors.
- **Opkts** - The number of output packets sent by the interface.
- **Oerrs** - The number of output packets which were not sent by the interface due to errors.
- **Collis** - The number of collisions experienced while trying to send packets out the interface.
- **Queue** - The number of packets currently queued for transmission on the interface.
- **Stat** - Either "NIS" or "DOWN" indicating whether the interface is active.
- **inet/dest** - For the Ethernet interface, the internet address of the PortMaster. For the ptp interfaces, the internet address of the remote system.
- **netmask** - The netmask of the inet/dest field.
- **Routing** - "Routing", "Sending", Listen", or "Quiet" indicating whether RIP protocol packets are being transmitted or received by the interface.

Managing the Hosts Table

Each device attached to the Ethernet (with uses TCP/IP) is assigned a unique internet address. Internet addresses are four byte numerical values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique and easy to remember name. This is done on the Sun Workstation (and other UNIX systems) in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

The PortMaster hosts table should be used when any of the ports are set to prompt the user for a host name on the network. This table is then consulted to determine the correct internet address of the host.

If the hostname specified by the user is not found in the hosts table, then

the PortMaster will attempt to match the hostname using the Network Information Service (NIS), also known as "NIS". See the section "Global Configuration" for more information on setting the NIS server and NIS domain.

To view or edit the PortMaster hosts table, log in to the PortMaster and select the "Hosts" command from the main console menu.

The hosts table stored in the PortMaster will be automatically retrieved into a working file on the Workstation. pmconsole will then start an editor running to allow modifications to this file. As a default, pmconsole will run the "vi" editor. To choose an alternate editor, set the environment variable PM_EDITOR to the editor name.

Once edits or viewing have been completed, save the file and exit the editor. pmconsole will automatically download the file to the local hosts file in the PortMaster.

Managing the Passwords Table

The Passwords Table provides login security for users to establish login sessions or for incoming Dialnet network connections. This sections covers normal user security. Consult the Dialnet User's manual for information on "network" users.

Serial ports configured to accept login sessions initially prompt for a login user name. After receiving the login name, the PortMaster checks the name against the list of names in the local Passwords Table. If found, the PortMaster initiates password authentication of the user. If successfully validated (the password received matches the password stored in the Passwords Table) the PortMaster begins the session which has been defined for the user.

Two types of login users can be created; Normal and Dialback. Normal users are allowed to immediately begin an active session on a host computer somewhere on the network. Dialback user's are disconnected by the PortMaster. The PortMaster then automatically dials to the users remote modem using a predefined telephone number. This feature allows for enhanced security or for simple telephone charge-back.

If the login name does not match an entry in the Passwords Table and the port is configured to support Pass-Thru Logins it automatically forwards the session to the designated host on the local network for password authentication.

To view or edit the PortMaster Passwords Table, log in to the PortMaster and select the "Tables" item from the main console menu. A pop-up menu will be displayed. Select "Passwords" from the menu. The following screen will be displayed:

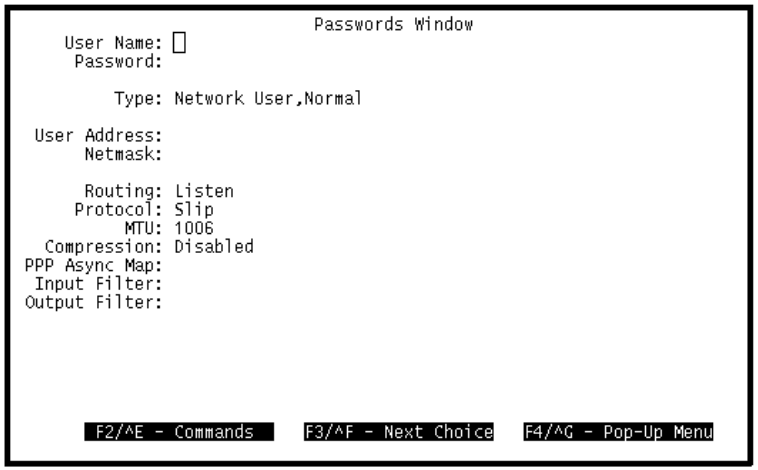

Figure 3-24. Passwords Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

When this key is pressed, the function keys will be replaced by a menu of commands which can be executed. The available commands are:

- **Create** - Adds the currently displayed user to the PortMaster Passwords Table.

- **Modify** - Applies modifications to the user displayed on the Passwords Window.
- **Purge** - Deletes the currently displayed user from the PortMaster Passwords Table.
- **Reset** - Clears the Passwords Screen to allow the entry of a new user.
- **Edit** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **Done** - return to the PortMaster Console screen.

Password Parameters

This screen displays the password table parameters and the current values. Some selections have menus. To use the menu, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. Alternately the selections can be rotated through with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The Passwords table has 5 fields for each user normal login user and 6 fields for dialback users. These fields are:

User Name *(menu and keyboard entry field)*

The login name of the user. This name can be up to 8 characters in length and is the user name to be supplied at the "login:" prompt from the PortMaster.

Password *(keyboard entry field)*

The password for the user. This is a string of up to 16 ASCII characters.

Type *(menu field)*

All login users should be set to a type of "Login User". "Network User" is specifically for Dialnet use. Consult the Dialnet User's manual for complete information. Login users can be set to "Normal" or "Dialback". Normal users will be allowed to immediately begin a login session after properly entering their user name and password. Dialback users will be

disconnected by the PortMaster and then re-dialed at their pre-defined telephone number.

Host *(menu field)*

This field defines which network host the users session will be forwarded to. The three options and their meanings are:

Default - Connect the user to the defined host for this serial port. Consult the serial port edit window for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session with.

Specified - Connect the user to the host specifically entered on the line below the Host selection. A valid hostname or IP address should be entered here.

Login Service *(menu field)*

The user can be set to use any of the available PortMaster Login Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual.

Telephone No *(keyboard entry field)*

This field is only displayed for Dialback Login Users. The telephone number which should be dialed to reach the users modem must be entered in this field. Dialback only supports modems with the Hayes "AT" command set.

Access Filter

An optional access control filter can be specified for the user. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the users connection will be allowed. If not, access will be denied.

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster do not have the ability to run the RIP protocol. The static routing table contains three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. This would be the number of gateways through which the packet must traverse to reach its destination.

To view or edit the PortMaster routes table, log in to the PortMaster and select the "Tables" item from the main console menu. A pop-up menu will be displayed. Select "Routes" from the menu.

The routes table stored in the PortMaster will be automatically retrieved into a working file on the Workstation. pmconsole will then start an editor running to allow modifications to this file. As a default, pmconsole will run the "vi" editor. To choose an alternate editor, set the environment variable PM_EDITOR to the editor name.

Once edits or viewing have been completed, save the file and exit the editor. pmconsole will automatically download the file to the local routes file in the PortMaster.

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying the passage of packets through network interfaces. By designing appropriate filters, administrators can control access to

specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allow the packet to pass freely through the interface (and on to its destination in the network) or cause the packet to be discarded without forwarding.

The Livingston packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- **Input** and **Output** Filters - Each interface can be assigned both an input-packet filter and an output-packet filter. This is especially useful in routers with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface for its destination and the mix of inbound and outbound traffic desired for the interface. This capability also has the potential to decrease the number of rules contained in the filter because fewer network numbers need to be included.

- **Source** and **Destination Address Filtering** - Both source and destination IP addresses can be evaluated in the rule list. Also, the number of significant bits to use in the address comparison can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- **Protocol Filtering** - Specific protocols can be handled separately in the packet filters. These include TCP, UDP, and ICMP.

- **Source and Destination Port Filtering** - The source and destination port numbers can be used in the rule set to control availability of specific network services. This includes evaluation base on whether the port number is less than, equal to, or greater than a specific value.

- **Established Session Filtering** - The status of TCP connections can be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access

to the local network.

- **Unlimited Number of Rules** - Each filter can have a large number of rules specified. This is only limited by available memory within the router.

- **Simple Rule Creation** - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example if the rule is not based on specific source and destination IP address, these addresses can be omitted from he specification of the rule.

- **In-line Rule Processing** - Rules are processed in the order in which they are specified in the rule set. This eliminates ambiguity about how a specific packet would be handled, and allows more flexibility in the creation of a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

Packet filters are "attached" to interfaces as either input filters or output filters. For serial interfaces, the packet filter is enabled at the time it transitions to the UP state (i.e. after a reset on the physical port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Managing the Filter Table

From the "**Tables**" pop-up menu, select "**Filters**". The screen shown below will be shown:

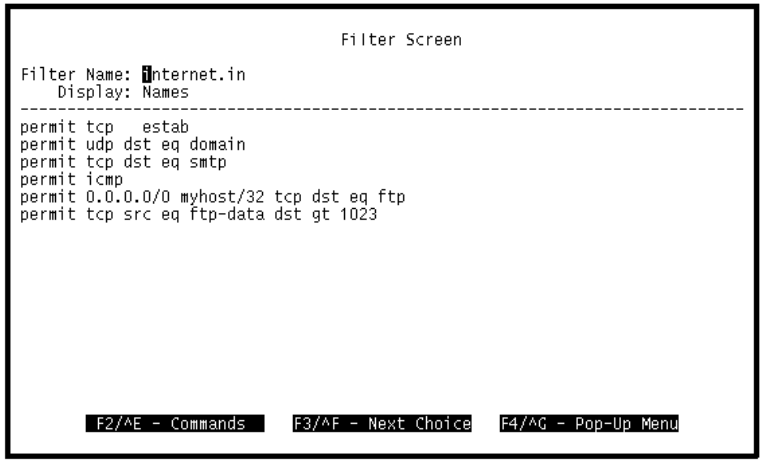

Figure 3-25 Filter Window

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

When this key is pressed, the function keys will be replaced by a menu of commands which can be executed. The available commands are:

- **Create** - Adds the currently displayed filter to the PortMaster Filter Table.
- **Modify** - Applies modifications to the filter displayed on the Filter Window.
- **Purge** - Deletes the currently displayed filter from the PortMaster Filter Table.
- **Reset** - Clears the Filter Window to allow the entry of a new filter.

- **Edit** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **Done** - Removes the Filter Window from the display.

Filter Name

This field displays the name of the current packet filter being edited or the name of the new filter being created. Selecting a name from the pop-up list above will fill in the Filter Name.

Display

The display field can be changed at any time. When set to Names, the rules will convert IP Address to host names and port numbers to service names. When set to Numbers, IP Addresses will be displayed in standard dot notation and services will be displayed numerically.

Edit

Upon entering the Edit area of the screen the F3 (or "Control-F" key) places you into your editor of choice (the PM_EDITOR environment variable) which will allow you to edit the Filter. Exiting the editor places you back into the Edit area and refreshes the area to include the information added from within your editor.

Filter Rule Syntax

The rule set for the filter is entered on the screen or from within an editor as described above. Entries can be inserted, deleted, and moved around within this window. Because packets are evaluated starting at the first rule, the most common packets which will be handled by the router should be specified first. As soon as a packet matches a rule the action specified by the rule will be immediately taken. If the packet does not match any rule, the action will be to deny the packet from traveling through the interface.

The syntax for specifying a rule is:

action [source_address/bits destination_address/bits] protocol options

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Source_address/bits - specify the comparison with the source IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet (i.e. if 24 bits is specified, a packet with the source address of 192.9.200.1 would become 192.9.200.0 since 24 bits are used to represent the first 3 bytes of the address). The most common bit counts would be:

0 - To match packets with any source IP Address.

16 - To look at only the network number of a class B IP Address.

24 - To look at only the network number of a class C IP Address.

32 - To look at the entire IP Address.

The resulting value is then compared with the specific source address.

Destination_address/bits - specify the comparison with the destination IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet. The resulting value is then compared with the specific destination address.

Protocol - The protocol of the packet may be specified. Valid values are TCP, UDP or ICMP.

Options - Each protocol supports a specific list of options:

TCP - This type of rule supports filtering on source and destination port numbers as well as the established state of the connection. The syntax for TCP options is:

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

Where:

src - indicates a comparison should be made with the source TCP port number.

dst - indicates a comparison should be made with the destination TCP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

estab - indicates that the packet should be tested to see if it is for an established TCP network connection. If this key work is specified packets being sent to establish new TCP connections would not match this rule.

UDP - This type of rule supports filtering on source and destination port numbers. The syntax for UDP options is:

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

Where:

src - indicates a comparison should be made with the source UDP port number.

dst - indicates a comparison should be made with the destination UDP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

ICMP - This type of rule supports filtering on type of ICMP message. The syntax for ICMP options is:

[src eq icmp_message_type]

Where a comparison is made with the ICMP message type contained in the packet.

Examples

In figure 3-14, Rule 1 says we permit tcp packets from any foreign host if the packet is for an already established connection.

Rule 2 says we permit udp Domain Name Service packets from any foriegn host.

Rule 3 says we permit Sendmail packets.

Rule 4 says we permit ftp from any foreign host but only to "myhost".

For examples of other filter rules, please refer to the "Command Prompt Interface" section of this manual.

Configuring SNMP

The PortMaster provides support for using the Simple Network Management Protocol (SNMP) for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are fully described in the Livingston MIB distributed with the standard Livingston software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the software. pmconsole provides a screen for configuring and enabling the SNMP facilities of the PortMaster. The SNMP edit screen can be displayed by using the "Edit" pop-up menu from the main console screen. After selecting "SNMP" from this menu, the following screen will be displayed:

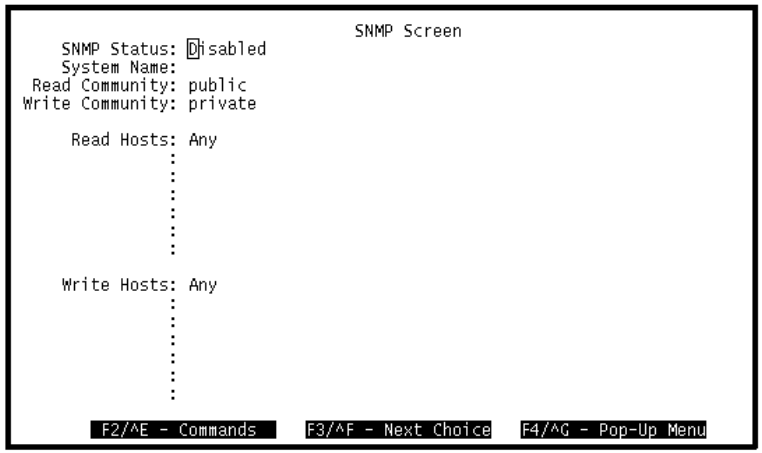

Figure 3-26. SNMP Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

When F2 (or "Control-E") key is pressed, the function key is replaced by a menu of commands which can be executed. The available commands are:

- Save - Stores the currently displayed values to the non-volatile storage in the PortMaster.
- Reset - Sets all values to their factory default configuration.
- Edit - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- Done - return to the PortMaster Console screen.

SNMP Parameters

This screen displays the SNMP parameters and the current values. Some selections have menus. To use the menu, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. Alternately the selections can be rotated through with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The SNMP screen has 5 fields. These fields are:

SNMP Status *(menu field)*

This field enables the SNMP capabilities of the PortMaster. If "Enabled", SNMP gets and sets will be allowed on the PortMaster. If "Disabled", SNMP queries will be ignored.

System Name *(keyboard entry field)*

This field sets the global SNMP system name. It is used as a system identifier independent of protocols. In addition, it is used as the system identifier in PPP PAP and CHAP requests.

Read Community *(keyboard entry field)*

The SNMP read community is generally used to segregate administrative

management communities. This should be set to match the read community setting of your SNMP management software. The default is "public".

Read Hosts *(menu field)*

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The options are:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

Specified - A specific list of hosts can perform SNMP gets from the PortMaster. A set of input fields will be displayed on the screen for the entry of a list of hosts.

Write Community *(keyboard entry field)*

The SNMP write community is generally used to segregate administrative management communities. This should be set to match the write community setting of your SNMP management software. The default is "private".

Write Hosts *(menu field)*

For security purposes, the hosts which are allowed to perform SNMP sets can be set on the PortMaster. The options are:

Any - All hosts using the correct write community will be allowed to set SNMP data on the PortMaster.

None - No SNMP writes will be allowed by the PortMaster.

Specified - A specific list of hosts can perform SNMP sets on the PortMaster. A set of input fields will be displayed on the screen for the entry of a list of hosts.

RADIUS

The PortMaster supports RADIUS (Remote Authentication Dial In User Service). This service support authentication of users and remote routers from a centrally managed database maintained on an authentication server somewhere on the network. For information on implementing a RADIUS authentication server, see the RADIUS User's Guide. Pmconsole allows the administrator to configure the PortMaster as a RADIUS client. In this configuration, the PortMaster will first consult its local Password Table (See Password Table Maintenance earlier in this chapter), it will then consult the RADIUS server if the user is not locally defined.

From the PortMaster Console Window, select the Edit pop-up menu and select **RADIUS**. The following window will be displayed:

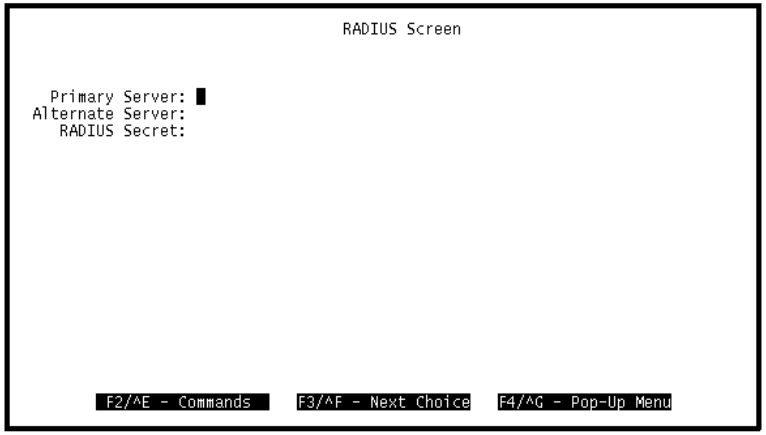

Figure 3-27 RADIUS Screen

Primary Server - Enter the hostname or the IP address of the Primary Authentication Server.

Alternate Server - Enter the name of the Secondary Authentication Server.

RADIUS Secret - enter the secret used to encrypt users passwords and for verification of the responding RADIUS server. Note that when entering the RADIUS secret from **pmconsole** it is passed over the network in clear text. Alternately this secret may be entered using the command line interface directly through the asynchronous serial port on the router.

Command Prompt Interface

Any of the previously described administration activities of the PortMaster can be performed using an ASCII terminal connected to a PortMaster serial port or remotely using the telnet protocol to establish an administrative session on the PortMaster. When using an ASCII terminal, set the communication parameters of the terminal to match the ones which have been previously set for that port or the default parameters if no settings have been made (Default: 9,600 baud, 8 data bits, 1 stop bit, and no parity).

The User Commands

The following commands are available:

● **SET** Command - set the port and global parameters. Set values for entries in several tables.

● **SHOW** Command - shows the status of each port , all ports and global data, or entries in several tables.

● **REBOOT** Command - reboot the PortMaster to the currently saved configuration.

● **RESET** Command - reset a port to the currently stored configuration.

● **VERSION** Command - displays the version number of the PortMaster software.

● **QUIT, DONE, EXIT** Commands - leave the Command mode.

● **SAVE** Command - save the current configuration to the PortMaster permanent configuration.

● **HELP** Command - provides information on each of the PortMaster commands including usage and syntax.

● **ADD** Command - adds entries to one of the local PortMaster tables.

● **DELETE** Command - deletes entries from one of the local PortMaster tables.

● **DIAL** Command - begins dialing to one of the Dialnet Locations.

● **IFCONFIG** Command - Similar to the ifconfig command on UNIX systems, this provides configuration values for all active interfaces. It also allows modification of active values on the fly.

● **TELNET** Command- Allows you to telnet from the COMMAND prompt to another host on the network.

● **TRACEROUTE** Command- Allows you to trace network routes when attempting to debug a problem.

● **PING** Command- Allows you to send and receive ICMP packets from the COMMAND prompt.

● **PMLOGIN** Command- Allows you to establish a login using the PortMaster login service to a node on your network.

● **PTRACE** Command- Allows you to watch network traffic after setting up a filter (See "Filters", later in this chapter).

● **RLOGIN** Command- Allows you to establish a login using the UNIX rlogin service to a node on your network.

Using the Commands

To use the ASCII Command Interface, you must login to the PortMaster using a special administrators user name and password. This login can be initiated from the async diagnostic port or through a telnet session to the TCP port number specified in the Global Telnet Access Port (default 23). At the login prompt enter:

```
login: !root
```

The PortMaster will request that you enter a password. This is the PortMaster administration password. After initial installation, there is no password. Upon entering the correct password, the PortMaster will display the prompt:

```
Command>
```

It is at this point that you can begin to use the PortMaster commands. Each command responds to the minimum number of characters, at least

two, that are unique to that command. Command entry is not case sensitive.

SET Command

The SET command is used to set each of the configuration parameters, including global parameters, and port parameters.

Setting Global Parameters

The syntax for setting global parameters is:

SET *parameter value [options]*

Any values which require an IP address should use the format:

```
XXX.XXX.XXX.XXX
```

where the XXX is a decimal number between 0 and 255.

Valid *parameters* and their associated values and options are:

ADDRESS - The PortMaster network internet address. Enter an IP address as the value.

GATEWAY - The default gateway (router) internet address. A metric value between 1 and 15 may be entered after the gateway address to be used as the metric for the default route.

NETMASK - The subnetting IP address mask for the Ethernet interface.

DEBUG - The debugging mask for the PortMaster. Most values are reserved for use by Livingston technical support. However, if the administrator is logged on to one of the serial ports, the debug value of 0x71 will show messages for every packet handled by the PortMaster. This output will be sent to the defined system console. The console can be set using the command "set port_name console" where port_name is the name of the serial port. Setting debug to 0 will disable this output.

NAMESVC - The type of service (NIS or DNS) to use for resolving host names.

NAMESERVER - The name server IP address.

DOMAIN - The domain name to use on the name server. *The value* is the domain name.

ROUTING - The routing options for the Ethernet interface. Valid values are:

On - The PortMaster will send RIP information to other computers attached to the local Ethernet and will accept RIP information from other routers on the local Ethernet.

Broadcast - The PortMaster will send RIP information to other computers attached to the local Ethernet.

Listen - The PortMaster will accept RIP information from other routers on the local Ethernet.

Off - The PortMaster will not send RIP information to the local Ethernet and it will ignore all RIP messages it receives on the local Ethernet.

DEFAULT - The default routing options for the all interfaces. Valid values are:

On - The PortMaster will send default route information as part of its normal RIP messages and will accept default route information coming from other routers.

Broadcast - The PortMaster will send default route information as part of its normal RIP messages.

Listen - The PortMaster will accept default route information coming from other routers.

Off - The PortMaster will not send default route information to other routers and it will ignore all default route messages it receives.

ETHERNET - Whether to Enable the Ethernet interface of the PortMaster. Valid values are "Up" to enable Ethernet and "Down" to disable Ethernet.

BROADCAST - The broadcast address for the Ethernet interface. Valid values are "high" to use a host part of all ones and "low" to use a host

port of all zeros. The actual broadcast address is constructed from the IP address of the PortMaster and the Netmask.

SNMP - Whether to enable SNMP or to set the community name. Valid values are:

On - To enable SNMP.

Off - To Disable SNMP.

Readcommunity - To set the read community for SNMP on the PortMaster.

Writecommunity - To set the write community for SNMP on the PortMaster.

ASSIGNED - The first assigned IP address for Dialnet Users. See the Dialnet User's guide for complete information.

TELNET - The telnet access port for the PortMaster. This values allows the administrator to use the telnet protocol to access the administration features of the PortMaster. The value can be any number from 0 - 65536. If "0" is used, telnet administration will be disabled. The value "23" is the default TCP port number for telnet.

IFILTER - Set the Input Filter for the Ethernet Interface. When specified, all packets received from the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Input Filters" toward the end of this chapter.

OFILTER - Set the Output Filter for the Ethernet Interface. When specified, all packets being sent to the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Output Filters" toward the end of this chapter.

AUTHENTIC - Set the primary RADIUS authentication server.

ALTERNATE - Set the alternate RADIUS authentication server.

SECRET - Set the RADIUS encryption secret.

SYSNAME - Set the Global SNMP system name.

PASSWORD - The PortMaster administration password. The *value* is a string of up to 16 characters to be used for the administration password.

Setting the Asynchronous Port Type

The syntax for setting the port type is:

SET S0 *type [device] [* NETWORK *dialnet_type]*

Where *Type* is one of:

LOGIN - (default) the specified port will display a login prompt to the user. After successful baud rate matching and receiving a login name, the user will be transferred directly to a login session on the host workstation.

DEVICE - the port will operate as a host controlled device on the workstation. The Host Device field described below must be entered.

TWOWAY - (or **BIDIRECTIONAL**) the port will operate in User Login mode if carrier is detected on pin 8 of the RS-232 connector. Otherwise it can be accessed as a host controlled device on the workstation. The Host Device field described below must be entered.

DISABLED - can be used for port P0 to disable the /dev entry. When reset, the P0 port will go to an idle (unused) state.

device is of the form:

/dev**/**<*tty_device*>

This is required in either the Host Device or Two-Way modes. The Host Device name is the name of a pseudo tty device in the workstation directory /dev. Standard device entries are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

There is a utility included with the PortMaster software called lstty. This program lists only the pseudo-tty devices that are in /dev, sorted in numerical order. It is a quick way to check on what pseudo-tty devices you have in your /dev directory. This program resides in the /usr/portmaster directory. Simply use the command:

lstty

See Appendix A for discussion of device drivers.

If NETWORK is used, one of four dialnet types may be selected: HARDWIRED, DIALIN, DIALOUT, TWOWAY. For a complete description of these options refer to the Dialnet User's Manual.

Setting Port Parameters

The syntax for setting port parameters is:

SET *port parameter value*

Where *port* is one of: S0 - S4

Parameter and *value* is one of:

SPEED - The baud rate for the port.

An extra value is entered after the "SPEED" key word to indicate which of the three optional baud rates is being set. Valid values are: 1, 2, or 3. This is followed by the actual baud rate. Valid async values are: 115200,57600,38400,19200, 9600, 4800, 2400, 1200, 300. Valid sync values are: 2048K, 1536K, 1344K, 115200, 64000, 57600, 56000, 38400, 19200, 9600.

ADDRESS - The local IP Address of the port. If set to 0.0.0.0 for PPP or SLIP connections, the IP Address of the Ethernet interface will be used. If set to 0.0.0.0 for Frame Relay connections, the port will be disabled.

DESTINATION [NETMASK] - The IP Address of the remote router and the netmask for the port. If destination is set to 255.255.255.255 for PPP connections, the PortMaster will

attempt to negotiate the remote IP Address. If set to 0.0.0.0 for PPP connections, the port will be disabled. The destination address is not used for Frame Relay connections, however the netmask should be set for all types of connections.

PROTOCOL - Sets the transport protocol for the port. Async ports support SLIP or PPP. Sync ports support PPP or Frame Relay. Valid values are: SLIP, PPP, FRAME.

ROUTING - The routing options for the interface. Valid values are:

On - The PortMaster will send RIP information to other computers attached to the port and will accept RIP information from other routers on the port.

Broadcast - The PortMaster will send RIP information to other on the port.

Listen - The PortMaster will accept RIP information from other routers on port.

Off - The PortMaster will not send RIP information to the remote routers and it will ignore all RIP messages it receives from remote routers.

MTU - Set the desired maximum transmission unit for the port. Valid values are 100 - 1500.

COMPRESSION - Sets the status of VJ Header compression (async only). Valid values are ON or OFF.

MAP - Sets the PPP async map (async only). A 32 bit hexadecimal number should be specified.

IFILTER - Set the Input Filter for the Interface. When specified, all packets received from the interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Input Filters" toward the end of this chapter.

OFILTER - Set the Output Filter for the Interface. When specified, all packets being sent to the interface will be evaluated against the

rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Output Filters" toward the end of this chapter.

PARITY - The parity checking to be used for the port (async only).
Valid values are: **EVEN**, **ODD**, or **NONE**

DATABITS - The number of databits per byte (async only).

Valid values are: 8, 7, 6, or 5

STOPBITS - The number of stop bits in the data frame (async only).

Valid values are: 1 or 2

MODEM - Whether to use the carrier detect signal.

Valid values are: ON or OFF

XON/XOFF - Whether to use Xon/Xoff flow control (async only).

This is a software flow control which is supported by most devices. By using ASCII control characters DC1 and DC3 the PortMaster communicates with the attached device to start and stop the flow of data.
Valid values are: ON or OFF.

RTS/CTS - Whether to use RTS/CTS flow control (async only).

This is for devices where hardware flow control is required. When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.
Valid values are: ON or OFF.

HOST - The host for this specific port (async only).

This option determines which host the port will connect to during an active session. Valid values are:
DEFAULT - In this mode the port will not be assigned to a host..

PROMPT - In this mode, the user is given a host prompt (before the standard login prompt). The user then is required to enter a valid host name or internet address for a host on the network.
Host Name or **Internet Address** - The port is assigned to a specific Host during an active session. An optional value may be inserted before the internet address to specify alternate hosts. This extra value is a number between 1 and 4. "1" is the primary host and "2" through "4" are the alternate hosts. Alternate host connections are only attempted of the primary host is unavailable (i.e. host is down or network is unreachable). Alternate host entries are optional.

SERVICE_LOGIN - The port can be configured to use one of four different network services for establishing login sessions (async only). Valid values are:

PORTMASTER - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either pminstall or the install window of pmconsole. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. In addition it is the most efficient and highest performance service available.
RLOGIN - This service is generally supported by a large number of mixed UNIX based computers. Therefore, where it is impractical to utilize the PortMaster service, Rlogin should be selected.
TELNET - This service is generally supported by a most TCP/IP computers. Therefore, in a network where mixed hardware and operating systems will be used by this port, Telnet should be selected. The default TCP port number for telnet is 23, however an alternate port number may be entered following the TELNET parameter.

NETDATA - This service can be used to create a virtual connection between this port and another serial port on a different PortMaster. The default TCP port number for netdata is 6000, however an alternate port number may be entered following the NETDATA parameter. The serial port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

SERVICE_DEVICE - The port can be configured to use one of four different network device services (async only). Valid values are:

PORTMASTER - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either pminstall or the install window of pmconsole. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. When selected, the port is accessed through a /dev/tty device on the host workstation.

RLOGIN - This service is generally supported by a large number of mixed UNIX based computers. Therefore, this service can be utilized to allow UNIX based workstations on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" indication.

TELNET - This service is generally supported by a most TCP/IP computers. Therefore, this service can be utilized to allow many different types of computers on the network to initiate a telnet session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will

automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" indication. The default TCP port number for telnet is 23, however an alternate port number may be entered following the TELNET parameter.

NETDATA - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or a similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port operating parameters are pre-set by the administrator. The application can then open the socket connection and immediately begin reading and writing data to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, however an alternate port number may be entered following the NETDATA parameter. If multiple ports on the PortMaster are configured to use this service with the same TCP port number, it will automatically create a "pool" of ports which can be accessed by other hosts.

TERMTYPE - Sets the terminal type in the users environment (async only). This optional field is used in either Login or Two-Way modes. When a new session is established on the host workstation, this terminal type will automatically be set in the user's environment. A valid entry from the termcap database should be entered. If this field in not entered, the host workstation will assume a "dumb" terminal.

PROMPT - Customized user login prompt (async only).

This field allows the administrator to customize the login prompt the user will see. Any valid ASCII characters may be entered. The default is to display the Host Name followed by the word "login:". If the string "$hostname" is included in the login prompt, the active hostname is substituted for the string.

OVERRIDE - Sets which configuration parameters can be overridden by the host (async only). The PortMaster allows overrides to be

set for Baud Rate, Parity, Databits, and Flow Control. This feature allows the host to alter the active parameters via software control (i.e. system ioctl calls). The default is that the Host can only turn Xon/Xoff flow control on and off. Two values are specified after the OVERRIDE parameter. The first one is the item to set. Valid values are: XON/XOFF, BAUD, DATABITS, or PARITY. The second value is either ON or OFF. "ON" means the host can override the value. "OFF" means the PortMaster configuration value is used and host attempts to change these values are ignored.

EXTENDED - Sets extended mode on or off.

Valid values are: ON or OFF. When Extended mode is "ON" more detailed output will be displayed in the "SHOW" command.

USERNAME or **AUTOLOG** - Sets the Autolog name (async only).

If this field is entered, the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the Host Workstation as if the user had typed the Autolog Name in response to the login prompt.

SECURITY - Sets the security level for this port (async only). Valid values are "on" which disables Pass-Thru logins and "Off" which enables Pass-Thru logins. If Pass-Thru logins are enabled (security set to off) any username which does not match the local password table will automatically be forwarded to the designated host for login and authentication.

CONSOLE - Sets this port to the PortMaster system console (async only).

MESSAGE - The login message to be displayed to the user prior to receiving the login prompt (async only). The value for this parameter is a string of up to 255 characters. New-lines are designated by using the carat symbol (^).

IDLETIME - The idle timeout specifies how long the PortMaster

should wait after the activity on the port stops before disconnecting the session (async only). The idle timout is specified in minutes and can be any value from 0 to 240. If set to 0, no timeout will be used.

GROUP - This field is used by Dialnet for creating dial-out pools when establishing remote network connections (async only). Consult the Dialnet User's Manual for complete information

ENCODE - This specifies the data encoding for the synchronous WAN ports. Valid values are NRZ and NRZI. The most common setting for synchronous data encoding is NRZ. NRZ is the default.

ACCESS - This sets the access override for async ports and is used in conjunction with the ACCESS FILTER. Valid values are ON or OFF. The default is OFF. When set to ON, users in the Password table will be allowed to override the port's Access Filter with their own Access Filter by providing the correct username and password.

HANGUP - This controls whether the DTR signal on the RS-232 connector will be momentarily dropped to cause a hangup after the termination of a user session (async only). If set to OFF, DTR will not drop after the session terminates. If set to ON, DTR will drop. The default is ON.

DLCI LIST - For Frame Relay connections this identifies the physical addresses of the enabled permanent virtual circuits. Active DLCI numbers should be provided by the Frame Relay Service Provider. Multiple DLCI's can be defined for each port. In addition, the IP addresses associated with each DLCI can be specified. If the IP address for a DLCI is not specified the router will automatically attempt to learn the remote IP address using the Inverse ARP protocol. DLCI entries must all be entered at the same time. Each entry should be seperated by a space. Entries are either the DLCI number or the DLCI number followed by a colon (:) followed by an IP address.

Examples of the **SET** command are:

set s1 speed 2 4800

sets the second baud rate to use for speed matching to 4800 baud.

set s1 login

sets the Device Type on serial port S1 to User Login.

set s1 twoway /dev/ttyr0

sets serial port S1 to a two-way device using /dev/ttyr0 as the device name on the host Sun Workstation.

set s1 message Welcome to the PortMaster

displays the login message: "Welcome to the PortMaster" on serial port S1.

The **SET** command stores the values and instructions in the PortMaster memory. No new changes take effect until you enter a RESET command.

SHOW Command

The **SHOW** command allows you to look at the current settings for any of the serial ports. It also lets you list the contents of the local hosts table.

The syntax for the show commands are:

port **-** Input/output, active & default configuration for the port.

ALL - Show global configuration and summary of all ports.

table - Show summary of the specified table. Valid values are: hosts, location, filter, or password.

memory - Show system memory usage.

netconns - Show system wide TCP and UDP network connections.

routes - Show the active and static routing table. Fields displayed include; destination - the remote host or network, gateway - the next hop system, metric - the hop count to the destination, interface - which

network interface to use, flags -

"H" - A host route

"N" - A network or subnet route

"S" - A static route

"L" - A route to a directly attached network or host

"D" - A dynamic route

"C" - A route which has recently changed

"O" - An obsolete route (scheduled for deletion)

netstat - Input/output statistics summary for all network interfaces.

user - The configuration settings for a user in the password table.

location - The configuration settings for a dialnet location.

For example:

show all

Shows the settings of all global parameters and a summary of each of the individual ports. This display is similar to the VIEW command in pmconsole described earlier in this chapter.

show s1

Displays the full set of configuration values for serial port S1. If "Extended" mode is turned on (described above), a more detailed set of information will be displayed.

show table hosts

Displays the currently stored hosts table.

IFCONFIG Command

When the IFCONFIG command is entered, the active configuration of each network interface is displayed. Each interface is displayed in two lines. The first line has the name of the interface (ie ether0, ptp1) and various flags for that interface. Possible flags are:

UP - The interface is UP and running.

DOWN - The interface is DOWN, it is not in use.

BROADCAST - The network is a broadcast network (ie. ethernet).

POINT_TO_POINT - The network is a point to point connection.

FRAME_RELAY - The network is a Frame Relay connection.

PRIVATE - No routing information will be transmitted on this interface. If private is not shown as a flag, routing information will be transmitted to the interface.

SUSPENDED - This On-Demand Dialnet interface is available for use, but does not have an active telephone connection to the remote site.

The second line will show:

inet - the internet address of the interface.

dest - the destination internet address if it is a point to point connection.

netmask - The netmask for the "inet" or "dest".

broadcast - The broadcast address if it is an ethernet interface.

mtu - The maximum transmission unit for the interface.

PING Command

The ping command allows the administrator to verify that the PortMaster can communicate with another host or router on the network. This is accomplished by sending an ICMP echo request to the remote host and listening for the corresponding echo reply from that host. The ping command takes a host name or IP Address as its argument.

PMLOGIN Command

Pmlogin initiates a login session to a host on the network using the portmaster network connection service. This command is only available from an administrative session on an asynchronous port.

PTRACE Command

The ptrace command allows the administrator to monitor specific network traffic received by the PortMaster. The ptrace command takes the name of a packet filter as its argument. When enabled, packets received by the PortMaster are evaluated against the packet filter. If the packet is "permitted" through the filter, a user readable message indicating the source and destination, protocol, and other protocol specific information are displayed to the administrator. By using a defined packet filter, the administrator can narrow the output down to the specific traffic they are interested in monitoring. By specifying the ptrace command with no filter, packet tracing is disabled.

When accessing the PortMaster via a telnet session, care should be taken to filter out the administrative telnet packets. Otherwise, ptrace will report packets from the administrators own ptrace output, causing a large amount of unusable packet tracing information.

REBOOT Command

Reboots the PortMaster, reloading the currently saved parameters. All ports will be set to the state of the last saved configuration. The syntax is:

REBOOT

RESET Command

Reset a port to it's currently stored values. Any terminal that is logged in through the PortMaster will be disconnected. You will need to log in again. The syntax is:

RESET port

- or -

RESET ALL

Where port is one of S0 - S4

RLOGIN Command

Rlogin initiates a login session to a host on the network using the rlogin

network connection service. This command is only available from an administrative session on an asynchronous port.

TELNET Command

Telnet initiates a login session to a host on the network using the telnet network connection service. This command takes a host name or IP address as its argument. In addition, a TCP port number for the connection can be specified on the command line.

TRACEROUTE Command

The traceroute command allows the administrator to identify all of the routers (and the path) to a remote host. This is accomplished by sending an special UDP frames to the host and listening for ICMP messages from the routers which handle the frames. The traceroute command takes a host name or IP Address as its argument and returns a list of routers.

QUIT, DONE, EXIT Command

These commands will log you out of the PortMaster command mode and will return you to login mode.

SAVE Command

Saves the current configurations in the PortMaster non-volatile storage. The syntax is:

SAVE ALL

- or -

SAVE port

Where port is one of S0 - S4. Using SAVE ALL will store all global parameters, port parameters, and tables in the PortMaster.

HELP Command

Provides information on the usage and syntax of the PortMaster commands. For example:

```
Command> help set
                              SET OPTIONS
General Parameters                      Entries in Tables
------------------------------------------------------------------------------
s0-s4     - Set configuration for a port   location - Set value for a location
default   - Set the use of default routes  user     - Set value for a user
dialnet   - Enable or disable Dialnet      snmp     - Set value for SNMP
domain    - Set the NIS or DNS domain      filter   - Set rule for a filter
gateway   - Set the default route
loghost   - Set the network syslog host    Ethernet Interface Parameters
password  - Set the admin password         -----------------------------------
telnet    - Set the TCP port for admin     routing  - Set the routing options
nameserver- Set the NIS or DNS server      address  - Set the Internet Address
namesvc   - Set NIS or DNS service         broadcast- Set the broadcast address
assigned  - Set pooled IP address          ifilter  - Set the input filter
sysname   - System Name                    ofilter  - Set the output filter
                                           netmask  - Set the ethernet netmask
Authentication Parameters                  ethernet - Enable or disable
----------------------------------------
authentic - Set the primary auth server
alternate - Set the alternate auth server
secret    - Set the encryption secret

Use "help set option" for further assistance
Command> quit
```

Managing the Hosts Table

Each device attached to the Ethernet (with uses TCP/IP) is assigned a unique internet address. Internet addresses are four byte numerical

values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique and easy to remember name. This is done on UNIX systems in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

The PortMaster hosts table should be used when any of the ports are set to prompt the user for a host name on the network. This table is then consulted to determine the correct internet address of the host.

If the hostname specified by the user is not found in the hosts table, then the PortMaster will attempt to match the hostname using the Network Information Service (NIS), also known as "NIS". See the section "Setting Global Parameters" for more information on setting the NIS server and NIS domain.

Three commands have been established for managing the local hosts table:

- ADD Command - adds entries to the local hosts table.
- DELETE Command - deletes entries from the local hosts table.
- SHOW Command - shows the entries in the local hosts table.

ADD Command

Add an entry to the local hosts table. The syntax is:

ADD host internet_address hostname

Where:
internet_address - is a valid host internet address in the form:

XXX.XXX.XXX.XXX

where XXX is a decimal number between 0 and 255.

hostname - is a character string of printable characters.

DELETE Command

Delete an entry from the local hosts table. The syntax is:

DELETE host internet_address

- OR -

DELETE host hostname

Where:
internet_address - is a valid host internet address in the form:

XXX.XXX.XXX.XXX

where XXX is a decimal number between 0 and 255.

hostname - is a character string of printable characters.

SHOW Command

List the contents of the local hosts table.

The syntax for the show command is:

SHOW table hosts

Managing the Passwords Table

The Passwords Table provides login security for users to establish login sessions or for incoming Dialnet network connections. This sections covers normal user security. Consult the Dialnet User's manual for information on "network" users.

Serial ports configured to accept login sessions initially prompt for a login user name. After receiving the login name, the PortMaster checks the name against the list of names in the local Passwords Table. If found, the PortMaster initiates password authentication of the user. If successfully validated (the password received matches the password stored in the Passwords Table) the PortMaster begins the session which has been defined for the user.

Two types of login users can be created; Normal and Dialback. Normal users are allowed to immediately begin an active session on a host computer somewhere on the network. Dialback user's are disconnected by the PortMaster. The PortMaster then automatically dials to the users remote modem using a predefined telephone number. This feature

allows for enhanced security or for simple telephone charge-back.

If the login name does not match an entry in the Passwords Table and the port is configured to support Pass-Thru Logins it automatically forwards the session to the designated host on the local network for password authentication.

Five commands have been established for managing the local passwords table:

- ADD Command - adds new users.
- DELETE Command - deletes existing users.
- SET Command - sets parameters for existing users.
- SAVE Command - saves changes to the passwords table to non-volatile storage.
- SHOW Command - shows settings for users.

ADD Command

Add an entry to the local passwords table. The syntax is:

ADD user User_Name password User_Password

Where:
User_Name - is a 1-8 character name for the new user.
User_Password - is a 0-16 character password for the new user.

DELETE Command

Delete a user from the passwords table. The syntax is:

DELETE user User_Name

Where:

User_Name is a 1-8 character name of an existing user.

SHOW Command

List a summary of the Passwords Table or show the specific configuration values for a single user.

The syntax for the show command is:

SHOW table passwords

- or -

SHOW user User_Name

SET Command

The set command can be used to configure specific values for Login Users. The syntax of the command is:

SET user User_Name parameter value [parameter value ...]

Where User_Name is the name of an exiting Login User. Several parameters may be set in each command by specifying the next parameter after the proceeding value. Valid parameters are:

Password

The password for the user. The value is a string of up to 16 ASCII characters.

Dialback

The dialback telephone number for the user. This is the string of characters which would follow the Hayes compatible "ATDT" command. If a telephone number is entered, the user will be automatically changed to a dialback user. If the word "none" is entered as the dialback value, the user will be changed into a normal Login User.

Host

This field defines which network host the users session will be forwarded to. The three values and their meanings are:

Default - Connect the user to the defined host for this serial port. Consult the serial port setting for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session with.

IP Address - Connect the user to the host specifically entered. A valid hostname or IP address should be entered here.

Service

The user can be set to use any of the available PortMaster Login Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual. Valid values are: PortMaster, Rlogin, Telnet, or Netdata. The TCP port number may also be specified after the name of the service.

Ifilter

An access control filter can be set for the user if they have been set to be prompted for a host to connect to. The Ifilter can be any valid filter name from the Packet Filter Table.

SAVE Command

Stores the Passwords Table in the PortMaster's non-volatile storage.

The syntax for the save command is:

SAVE passwords

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster do not have the ability to run the RIP protocol. The static routing table contains three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet

through the above gateway. Generally metric is the HOP count to the remote network. This would be the number of gateways through which the packet must traverse to reach its destination.

Three commands have been established for managing the static routes:

- **ADD** Command - adds new static route.
- **DELETE** Command - deletes existing static route.
- **SAVE** Command - saves changes to the static routes table to non-volatile storage.

ADD Command

Add an entry to the static routes table. The syntax is:

ADD route Destination Gateway Metric

Where:
Destination - is the destination IP address.
Gateway - is the gateway IP address.
Metric - is the hop count to the remote destination.

DELETE Command

Delete a static route. The syntax is:

DELETE route Destination

Where:

Destination - is the destination IP address.

SAVE Command

Stores the Routes Table in the PortMaster's non-volatile storage.

The syntax for the save command is:

SAVE routes

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying the passage of packets through network interfaces. By designing appropriate filters, administrators can control access to specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allow the packet to pass freely through the interface (and on to its destination in the network) or cause the packet to be discarded without forwarding.

The Livingston packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- Input and Output Filters - Each interface can be assigned both an input-packet filter as well as an output packet filter. This is especially useful in routers with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface, where its destination is, and the mix of traffic both inbound and outbound desired for the interface. This capability also has the potential to decrease the number of rules contained in the filter because fewer network numbers need to be included.

- Source and Destination Address Filtering - Both the source and destination IP addresses can be evaluated in the rule list. In addition, the number of significant bits to use in the address comparison can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- Protocol Filtering - Specific protocols can be handled separately in the packet filters. These include TCP, UDP, and ICMP.

- Source and Destination Port Filtering - The source and destination port numbers can be used in the rule set to control availability of specific

network services. This includes evaluation base on whether the port number is less than, equal to, or greater than a specific value.

- Established Session Filtering - The status of TCP connections can be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access to the local network.

- Unlimited Number of Rules - Each filter can have a large number of rules specified. This is only limited by available memory within the router.

- Simple Rule Creation - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example if the rule is not based on specific source and destination IP address, these addresses can be omitted from he specification of the rule.

- In-line Rule Processing - Rules are processed in the order in which they are specified in the rule set. This eliminates ambiguity about how a specific packet would be handled, and allows more flexibility in the creation of a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

Packet filters are "attached" to interfaces as either input filters or output filters. For serial interfaces, the packet filter is enabled at the time it transitions to the UP state (i.e. after a reset on the physical port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Filter Creation

New packet filters are created with the "add filter" command. It is recommended that a specific naming convention be used to differentiate the uses of various filters. For example, the following names could be used:

internet.in - The input filter to be used for the link to the Internet.
internet.out - The output filter to be used for the link to the Internet.
s1.in - The input filter for serial port S1.
ether.out - The output filter for the ethernet interface.
project1.out - The output filter to be used during a special project.

The syntax of the "**add filter**" command is:

add filter Filter_Name

Filter_Name is the name to be assigned to a filter.

Setting Filter Rules

Once a filter has been created, the "set filter" command is used to add, modify or delete specific rules. The syntax of this command is:

set filter Filter_Name Rule_no [*permit|deny* **]**

[S*ource_Addr/Source_Bits Dest_Addr/Dest_Bits* **]**

[*Protocol* **[** *src lt|eq|gt Value* **] [** *dst lt|eq|gt Value* **]**

[*established* **]**

Filter_Name - is the name of an existing filter.

Rule_no - is a number up to the highest previously set Rule_no plus 1 (i.e. if there are 4 existing rules, Rule_no can be from 1 to 5). If an existing rule number is specified, it is replaced by the new rule. If no parameters are specified for the rule, that rule is deleted.

permit|deny - indicates whether the packet should be forwarded (permit) or discarded (deny).

Source_Addr - The Source Address to look for in the Packet's IP header.

Source_Bits - The number of bits to use when comparing the **Source_Addr** to the actual address in the packet. Valid values are from 0 to 32.

Dest_Addr - The Destination Address to look for in the Packet's IP header.

Dest_Bits - The number of bits to use when comparing the Dest_Addr to the actual address in the packet. Valid values are from 0 to 32.

Protocol - The protocol to look for in the packet's IP header. Valid values are: tcp, udp, and icmp.

src - Evaluate the Source Port in TCP or UDP packets.

lt|eq|gt - The type of comparison to perform with the TCP or UDP port number.

Where "**lt**" means Less-Than, "**eq**" means Equal-To and "**gt**" means Greater-Than.

Value - The decimal value to use in the TCP or UDP port number comparison.

dst - Evaluate the Destination Port in TCP or UDP packets.

established - Evaluates whether the packet is for an established TCP connection.

Deleting Filters

The "**delete filter**" command is used to remove a packet filter from the table. The syntax of the command is:

delete filter Filter_Name

Filter_Name - is the name of an existing filter.

Viewing Filters

The "**show**" command can be used to view the list of packet filters and

the contents of each filter. To view the list of all packet filters use the command:

show table filter

To view the contents of a specific filter use the command:

show filter Filter_Name

Saving Filters

To save the table of packet filters use the command:

save filter

Filter names for specific interfaces are saved through the normal configuration save commands (i.e. "**save all**" or "**save s1**").

Packet Processing

When packets are received on an interface the active input filter for that interface is evaluated before forwarding the packet through the PortMaster.

Before packets are transmitted on an interface the active output filter for that interface is evaluated before transmitting.

Each rule is evaluated in the order the rules are specified. As soon as the packet matches one rule, that rules action is immediately taken and no further processing is performed on the packet. If no rules match the specific packet, the packet is "denied" and it is discarded. Whenever a packet is discarded, the PortMaster automatically generates and ICMP Host Unreachable message back to the originator.

It is recommended that packets which represent the highest volume of traffic through an interface be specified early in the list of rules. This

will decrease the overhead of processing these packets and therefore increase overall performance.

Ethernet Interface Filters

The "set" command is used to establish specific input and output packet filters for the Ethernet interface. To set an input filter use the command:

set ifilter Filter_Name

Where **Filter_Name** is the name of an entry in the filter table. To set an output filter use the command:

set ofilter Filter_Name

If no name is specified, or if the named filter does not exist, packet filtering is disabled. Packet filtering is enabled or disabled on the ethernet interface immediately after executing the above set command.

Hardwired Serial Interface Filters

The "**set**" command is used to establish specific input and output packet filters for hardwired serial ports. To set an input filter use the command:

set Port_Name ifilter Filter_Name

Port_name - is the name of a port on the PortMaster (i.e. S1, S2...)

Filter_Name - is the name of an entry in the filter table.

To set an output filter use the command:

set Port_Name ofilter Filter_Name

If no name is specified, or if the named filter does not exist, packet filtering is disabled. Packet filtering is enabled or disabled on serial interfaces when the port is reset, and the network connection is re-established.

Dial-In User Filters

For the PortMaster Communications Servers which support dial-up SLIP and PPP access, input and output filters are assigned to the "user" rather than to the serial port. When a user establishes a PPP or SLIP

connection with the PortMaster the designated filters are attached to the port through which the user is attached. The "set user" command is used to assign filters to specific users. To set an input filter for a user use the following command:

set user User_Name ifilter Filter_Name

User_Name - is the name of a user in the PortMaster passwords table

Filter_Name - is the name of an entry in the filter table.

To set an output filter for a user use the following command:

set user User_Name ofilter Filter_Name

User_Name - is the name of a user in the PortMaster passwords table

Filter_Name - is the name of an entry in the filter table.

Dial-Out Location Filters

For the PortMaster Communications Servers which support dial-out SLIP and PPP, input and output filters are assigned to the "location" rather than to the serial port. When a PPP or SLIP connection is established to a remote site the designated filters are attached to the port through which the connection is attached. The "set" command is used to assign filters to specific locations. To set an input filter for a location use the following command:

set Location_Name ifilter Filter_Name

Location_Name - is the name of a location in the PortMaster location table

Filter_Name - is the name of an entry in the filter table.

To set an output filter for a location use the following command:

set user Location_Name ofilter Filter_Name

Location_Name - is the name of a location in the PortMaster location table

Filter_Name - is the name of an entry in the filter table.

Examples

Because of the flexibility provided through the PortMaster packet filtering system, it is possible to specify filters which do not achieve the desired results. Great care should be taken to evaluate the types of traffic which

a specific filter allow to pass through an interface. If possible, testing should be performed from both sides of the filtering interface to verify that the filter is operating correctly.

The following example could be used at a site which has an Internet connection and wishes to gain access to the Internet through a PortMaster serial port without exposing their site (and its network) to outside people and organizations. This filter would designate one system on the local network for all Electronic Mail communications with the Internet. It would also designate one system for all FTP access from the Internet. In addition, it will allow local users to Telnet and FTP to remote sites. Finally, it will allow DNS (Domain Name Service) to work between the Internet and the local site. For the purposes of this example, the local site will use network number 192.9.200.0, the E-mail server will be at address 192.9.200.1 and the FTP server will be at address 192.9.200.2.

```
#
#               Allow our users to open Telnet sessions with the Internet
#
set filter s1.in  1 permit tcp src eq 23 estab
set filter s1.out 1 permit tcp dst eq 23
#
#               Allow our users to open an FTP session with the Internet
#
set filter s1.in  2 permit tcp src eq 21 estab
set filter s1.out 2 permit tcp dst eq 21
set filter s1.in  3 permit tcp src eq 20 dst gt 1023
set filter s1.out 3 permit tcp dst eq 20
#
```

```
#               Allow DNS to pass through
#
set filter s1.in  4 permit udp dst eq 53
set filter s1.out 4 permit udp dst eq 53
#
#               Allow the Internet to open an SMTP session with our
server
#
set filter s1.in  5 permit 0.0.0.0/0 192.9.200.1/32 tcp dst eq 25
set filter s1.out 5 permit 192.9.200.1/32 0.0.0.0/0 tcp src eq 25 estab
#
#               Allow our server to open an SMTP session with the
Internet
#
set filter s1.in  6 permit 0.0.0.0/0 192.9.200.1/32 tcp src eq 25 estab
set filter s1.out 6 permit 192.9.200.1/32 0.0.0.0/0 tcp dst eq 25
#
#Allow the Internet to open an FTP and FTP-data session with our server
#
set filter s1.in  7 permit 0.0.0.0/0 192.9.200.2/32 tcp dst eq 21
set filter s1.out 7 permit 192.9.200.2/32 0.0.0.0/0 tcp src eq 21 estab
set filter s1.in  8 permit 0.0.0.0/0 192.9.200.2/32 tcp dst eq 20 estab
set filter s1.out 8 permit 192.9.200.2/32 0.0.0.0/0 tcp src eq 20
#
#               Allow ICMP for debugging
#
set filter s1.in  9 permit icmp
set filter s1.out 9 permit icmp
#
#
#               Save It and Set It
#
#
save filter
set s1 ifilter s1.in
set s1 ofilter s1.out
```



```
save s1
reset s1
```

Configuring SNMP

The PortMaster provides support for using the Simple Network Management Protocol (SNMP) for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are fully described in the Livingston MIB distributed with the standard Livingston software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the software. Several commands have been established for setting SNMP parameters.

Enabling SNMP

To enable or disable SNMP use for the PortMaster use to command:

set SNMP on

- or -

set SNMP off

Setting Community Names

The read and write communities to be used by the PortMaster can be set to any value. The SNMP community names are generally used to segregate administrative management communities. This should be set to match the read and write community settings of your SNMP management software. To set the SNMP read community use the command:

set SNMP readcommunity Community_Name

Where Community_Name is the name of the SNMP read community. To set the SNMP write community use the command:

set SNMP writecommunity Community_Name

Where Community_Name is the name of the SNMP write community.

Setting Read Hosts

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The syntax for this command is:

ADD snmphost reader Host_Name

Where Host_Name is one of the following:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

IP Address - The IP address of the host to add to the list of valid SNMP readers.

Setting Write Hosts

For security purposes, the hosts which are allowed to perform SNMP sets can be set on the PortMaster. The syntax for this command is:

ADD snmphost writer Host_Name

Where Host_Name is one of the following:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

IP Address - The IP address of the host to add to the list of valid SNMP readers.

Saving SNMP Configurations

After modifying SNMP configuration values, the SNMP table should be saved to non-volatile storage. This can be done by using the command:

SAVE snmp

Viewing SNMP Configurations

Current SNMP setting may be viewed by using the command:

SHOW table snmp

Using /dev Entries _____APPENDIX A

On the UNIX systems there is a directory called /dev. This directory contains a list of devices. Some devices are pseudo devices called pseudo tty's. A pseudo tty device is a process that acts like a serial device, such as a terminal. Most UNIX systems support at least 255 of these. Each connection to the PortMaster requires a pseudo tty device. In addition, other software programs use pseudo tty devices. These include; workstation shelltool windows, rlogin, rsh or other network processes.

First, to use a device, the operating system has to have support for that device. The second thing you need to access a device is an entry in /dev which is the name of that device. The name entry in /dev cross references to a major device number and a minor device number. The major device number is used for a single type of device in the operating system. For example pseudo ttys use the major device number 20 on Sun Workstations. Then each of the devices which acts like a pseudo tty is assigned a minor device number. For example, the entry, /dev/ttyr0, is a pseudo-tty entry in /dev. The device 'name' is ttyr0. If the command:

ls -l /dev/ttyr0

is performed, the following entry would be displayed:

```
crw-rw-rw-  1 root      20,  32 Sep  2 08:20 /dev/ttyr0
```

This indicates that /dev/ttyr0 has major device number 20 (a pseudo tty) and minor device 32 (the 33'rd minor device number).

Using Default /dev Entries

To use the default /dev devices, simply use the path and name of the device, for example:

/dev/ttyr0

The port types Device and TwoWay require a device name, which is found in the /dev directory. Some UNIX releases allow the number of pseudo tty's configured into the kernel to be customized. For example, the generic Sun Workstation operating system has support for 48 pseudo devices. To go beyond the 48 devices, you must modify your UNIX

kernel. Check your system documentation for instructions on adding pseudo tty devices.

Modifying your UNIX kernel

This section describes the steps necessary to modify the kernel of a system run the SunOS version of UNIX. This can be used as a reference for other UNIX systems. Refer your systems installation documentation for more complete descriptions of these steps. For the Sun, the System and Network Administration Guide, has a chapter on Re-configuring the System Kernel. In the generic configuration file, in the /sys/<*arch*>/conf directory (where <*arch*> is the machine architecture - sun3, sun4, sun4c), there is a line dealing with pseudo-tty devices. This line sets the default number of pseudo-tty devices to 48:

```
pseudo-device  pty    #pseudo-tty's, also needed for SunView
```

Change the entry from 'pty' to 'pty64' and you will set the number of pseudo-tty devices to 64. Append any number you wish, up to 255 to the 'pty' entry. No number defaults to 48 devices. You will then need to re-build your kernel, as described in the Sun documentation.

Using MAKEDEV

The last step is to make entries in /dev to match the operating system support. The first 64 are created using a program called MAKEDEV. During a standard installation the first 48 device entries will be automatically created. They are:

/dev/ttyp0 - /dev/ttypf

/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

An additional 16 may be created using MAKEDEV which is located in the /dev directory. Use the command:

MAKEDEV pty3

and /dev/ttys0 - /dev/ttysf will be created.

There is a utility included with the PortMaster software called lstty. This

program lists only the pseudo-tty devices that are in /dev, sorted in numerical order. It is a quick way to check on what pseudo-tty devices you have in your /dev directory. This program resides in the /usr/portmaster directory. Simply use the command:

lstty

Utilities _____ APPENDIX B

PMcommand

The pmcommand utility allows the administrator to download an ASCII command file to the PortMaster. The syntax of this command is:

pmcommand [-nostop] PM_Name PM_Password Command_File

Where:

-nostop - tells pmcommand not to stop executing if there is an error in the command script. Without this option, any errors detected in commands will cause the script to immediately stop executing.

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Command_File - is the name of the file containing portmaster commands. All commands described in the "Command Prompt Interface" can be placed in this file.

PMdial

The pmdial utility allows manual or scheduled Dialnet connections to be initiated by the PortMaster from a host on the network. The syntax of this command is:

pmdial [-v] PM_Name PM_Password Location_Name

Where:

-v - tells pmdial to display the execution of the dial script as it proceeds on the PortMaster.

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Location_Name - is the name of a Dialnet Location in the PortMaster Location Table.

For more information on Dialnet locations and dialing to those locations, consult the Dialnet User's Manual.

PMreset

The pmreset utility allows the system administrator to reset any or all ports on the PortMaster from a remote host. This can be embedded in a shell script or called directly by the administrator. The syntax of this command is:

pmreset PM_Name PM_Password Port_Name

Where:

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Port_Name - is the symbolic name of the port (ie. S0) or the word "ALL" to reset all ports on the PortMaster.

Specifications _____ APPENDIX C

Network Interface

10-Mbps Baseband IEEE 802.3 compatible interface utilizing TCP/IP protocol.

Connector Type	Cable Type	Transmission Distance
15 Pin DIX for connection to external transceiver	RG-11 50 Ω coaxial	Trunk segment 1640 ft/500 m max Transceiver cable - 164 ft/50 m max Network trunk - 8200 ft/2500 m max
BNC T-Connector	RG-58 A/U 50 Ω coaxial	Trunk segment - 984 ft/300 m max Station distance - 1.5 ft/0.5 m min Network trunk - 3035 ft/925 m max
RJ-45 for 10BaseT	Unshielded Twisted Pair	Hub distance - 328 ft/100 m max Repeaters - 4 max

Communications Interface

1 RS-423 (RS-232 compatible) asynchronous serial port.
1 - 4 RS-423/RS-232/V.35 synchronous serial ports
Data Rates selectable up to 2048Kbps.
Software flow control XON/XOFF.
Hardware flow control RTS/CTS.
DB-25, DTE pinout female connectors.
Terminal, Host, Modem support:
DTR, DSR, DCD, TXC, RXC, RTS, CTS

Physical Dimensions

Length: 11.5 in/29.2 cm

Width: 16.8 in/42.7 cm

Height: 3.2 in/8.1 cm

Weight: 12.4 lb/5.7 kg

Power Requirements

110 VAC +-10%, 47 to 63 Hz, 1.0A

220 VAC +-10%, 47 to 63 Hz, .6A

Environmental Operating Range

Temperature: 41° to 113° F/5° to 45° C

Humidity: 20% to 80%

Glossary _____ APPENDIX D

ASCII

American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.

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.

bps

bits-per-second

button

In this manual, this refers to outlined selections in a window display that can be activated by pointing and clicking the mouse.

byte

8 binary bits

Device Type

For the PortMaster there are three device types: Device, User Login, and TwoWay. Both Device and TwoWay require a device name assignment.

Ethernet

An effective means of interconnecting large numbers of computers and related devices. Uses coaxial cable to carry the data between components on the network.

file

A method of organizing and storing or retrieving data, on a disk or in memory.

icon

A visual image, on the display, of a shape denoting the purpose of a program function.

interface

The connection or communication between various system elements.

modem

A device to allow computer communication using ordinary telephone lines. This device connects to the PortMaster through a serial port.

mouse

A pointing device, usually with at least two functional buttons. In this document, the left mouse button selects buttons in a window. The right mouse button causes pop-down menus to be displayed, on some windows.

port

The channel through which data flows. The physical connection to the CPU, such as a parallel printer port or a serial port.

printer

A device for putting computer-generated information on paper or other media. This device can have either a serial or parallel interface, or both.

RS-232 interface

A standard of data communication using serial data and control signals.

serial port

A bi-directional channel through which data flows one bit at a time, most often 10-bits to a character of data: start bit, 8 data bits, 1 stop bit.

TCP/IP

A standard communications protocol developed by the U.S. Department of Defense.

terminal

In this manual, this refers to a device with a keyboard and a display for communicating with a computer. This is an ASCII device with an RS-232 serial interface.

Thick Ethernet

An Ethernet connection using a multi-pin D-shell connector and a cable to a transceiver. Generally using RG-11 50Ω coaxial cable.

Thin Ethernet

An Ethernet connection where the transceivers are built in to the device and a BNC connector and cable are used for the Ethernet connection. Generally using RG-58 50Ω coaxial cable.

TwoWay Mode

A device that is used either as a User Login or a Host Device, to which the system sends information. A device name must be assigned.

UNIX

A multi-user, multi-tasking operating system.

User Login Mode

A PortMaster mode that communicates with an ASCII terminal, with someone logging in through the PortMaster.

window

An area of the workstation display dedicated to a particular function or process.

workstation

A system, usually a desktop unit, that contains a computer, display, keyboard, mouse and, perhaps, a disk drive or drives.

Command Reference _____ APPENDIX E

Command List

add	- Add an entry to one of the PortMaster tables
delete	- Remove and entry from one of the PortMaster tables
dial	- Initiate dialing to one of the Dialnet Locations
done	- End administration session with the PortMaster
exit	- End administration session with the PortMaster
help	- provide a brief listing of commands
ifconfig	- View or configure values for the active interfaces
ping	- Similar to the UNIX ping command
pmlogin	- Login to remote host using PortMaster login service
ptrace	- Trace network traffic using a filter
quit	- End administration session with the PortMaster
reboot	- Terminate all sessions, and restart the operating system
rlogin	- Login to remote host using rlogin service
reset	- Terminate a session on a port and restart the port
save	- Save configuration parameters or tables
set	- Set configuration values and parameters in tables
show	- Show active and configured values
telnet	- Establish a telnet session with another host
traceroute	- Trace routes to destination hosts or gateways
version	- Display the current version of the operating system

Command Options

add

filter	- Add a packet filter definition to the filter table
host	- Add a host to the local hosts table
route	- Add a route to the static routing table
location	- Add a new Dialnet dialout location
snmphost	- Add a host to the SNMP access list
netuser	- Add a SLIP or PPP user to the password table
user	- Add a login user to the password table

delete

filter	- Delete a packet filter from the filter table

host - Delete a host from the local hosts table
route - Delete a route from the static routing table
location - Delete a Dialnet dialout location
snmphost - Delete a host from the SNMP access list
netuser - Delete a SLIP or PPP user from the password table
user - Delete a login user from the password table

reset

all - Reset all PortMaster ports
s0-s4 - Reset a PortMaster serial port
console - Stop sending console messages to any of the ports
nic - Reset the PortMaster ethernet controller
dialer - Checks all active interfaces against the location table

save

s0-s4 - Save configuration values for a serial port
all - Save all configuration values
filter - Save the entire filter table
global - Save global configuration values
location - Save the entire location table
snmp - Save the SNMP configuration table
password - Save the entire password table
host - Save the entire hosts table
console - Save the currently active system console
routes - Save the static routing table

set - global values

password - Set the PortMaster administration password
gateway - Set the default route for the PortMaster
address - Set the PortMaster's Internet Address
netmask - Set the netmask of the ethernet interface
debug - Set the console message debugging level
domain - Set the NIS or DNS domain for the Portmaster
nameserver - Set the NIS or DNS server for the PortMaster
namesvc - Set the type of Name Service (DNS or NIS)
routing - Set the routing options for the ethernet interface

ethernet - Enable or disable the ethernet interface
broadcast - Set the broadcast Internet Address
snmp - Enable or disable SNMP, or set community names
loghost - Set the network host to receive syslog messages
assigned - Set the first assigned address for dialin network users
telnet - Set the TCP port for telnet access
namesvc - Set type (NIS or DNS) of name resolving service
nameserver - Set nameserver IP address
default - Set default routing options for all interfaces
ifliter - Set input filter for the Ethernet interface
ofilter - Set output filter for the Ethernet interface
authentic - Set primary RADIUS authentication server IP address
alternate - Set alternate RADIUS authentication server IP address
secret - Set RADIUS encryption secret
sysname - Set the name of the global SNMP system name

set - port values

speed - Set the port speed
parity - Set the parity
databits - Set the number of databits
stopbits - Set the number of stopbits
device - Set the port to be used as an outbound device
login - Set the port to be used for login sessions
twoway - Set the port for both inbound and outbound connections
username - Set the Autolog username
modem - Enable or disable hardware carrier detect
xon/xoff - Enable or disable Xon/Xoff flow control
rts/cts - Enable or disable RTS/CTS flow control
message - Set the welcome message
console - Set the system console
disabled - Disable the parallel port
host - Set the login host for the port (async only)
termtype - Set the terminal type for the user's environment
prompt - Set the login prompt for the port
override - Enable or disable host overrides of datacomm parameters
extended - enable or disable extended port features
autolog - Set the automatic login name for the port
service_login - Set the default login service to use for the port
service_device - Set the default device service to use for the port

network - Enable or disable SLIP or PPP use of the port
routing - Set type of routing for hardwired network connection
address - Set the IP address for hardwired network connection
group - Set the Dialnet group number for the port
compress - Enable or disable header compression for connection
protocol - Set the network protocol for hardwired connection
map - Set the PPP async map for hardwired connection
mtu - Set the Maximum transmisson unit for connection
security - Enable or disable pass-through login access
destination - Set IP address of the remote router
ifilter - Set input filter for the interface
ofilter - Set the output filter for the interface
idletime - Set idle timer for auto-disconnect
encode - Set data encoding for WAN ports
access - Set access filter override for async ports
hangup - Set DTR to toggle on or off on disconnect

set - password table values

address - Internet address for the network user
netmask - Netmask for the network user
protocol - Protocol (ie. SLIP or PPP) for the network user
routing - Type of routing for the network user
mtu - Maximum transmission unit for the network user
map - PPP async map for the network user
compression - Enable or disable header compress for the network user
password - Set the user's password
dialback - Set the dialback location or telephone number
host - Set the login host for the user
service - Set the login service for the user
ifilter - Set the input packet filter or the User access filter
ofilter - Set the output packet filter for the user

set - location table values

idletime - Set the idle timeout (in minutes) for the location
routing - Set the type of routing to use for this location
address - Set the Internet address of this location
script - Set the Chat script for dialing to this location

manual - Set this to a manual dial location
continuous - Set this location to auto redial if the connection drops
on_demand - Set this location to be dialed On-Demand
netmask - Set the netmask for this location
group - Set the dial group for this location
maxports - Set the maximum number of connections to this location
high_water - Set the high water mark for dialing additional lines
protocol - Set the protocol to use for this location (SLIP or PPP)
compression - Enable or disable header compression for this location
mtu - Set the maximum transmission unit for this location
map - Set the PPP async map for this location
ifilter - Set the input packet filter for this location
ofilter - Set the output packet filter for this location

set - filter table values

permit - Allows packets which match this rule to proceed
deny - Prevent packets which match this rule from proceeding
tcp - Apply this rule to TCP packets
udp - Apply this rule to UDP packets
icmp - Apply this rule to ICMP packets
src - Apply this rule to packets based on its source port
dst - Apply this rule to packets based on its destination port
established - Apply this rule to TCP packets from established connections

show

s0-s4 - Show input/output, active and default configuration
all - Show summary status for all ports
table - Show summary listing of a data table
memory - Show system memory utilization
netconns - Show all TCP and UDP network connections
routes - Show active and static routing table
netstat - Show network interface statistics
user - Show configuration for a user in the password table
location - Show the configuration values for a dialnet location
filter - Show the rule list for a filter

Index

A

About This Manual, 1-5
ADD Command, 3-86, 3-106, 3-108
Administration, 1-1
Asynchronous Port Configuration, 3-55

C

Command Prompt Interface, 3-86
Configuration Switch Settings, 2-2
Configuring SNMP, 3-82, 3-120
Connecting Devices to the Diagnostic/Async Port, 2-5
Connecting Serial Communications Devices, 2-5
Connecting the Ethernet, 2-7

D

DELETE Command, 3-86, 3-106, 3-108, 3-111
Deleting Filters, 3-115
Diagnostic Light, 2-2
DIAL Command, 3-86
Dial-In User Filters, 3-117
Dial-Out Location Filters, 3-118

E

Enabling Serial Port Parameters, 3-20, 3-64
Enabling SNMP, 3-121
Established Session Filtering, 3-77
Ethernet, 2-2
Ethernet Activity Light, 2-2
Ethernet Configuration, 2-3
Ethernet Connection, 2-4
Ethernet Interface Filters, 3-116
Ethernet Link Status, 2-2
Extended Mode Parameters, 3-15, 3-60

F

Filter Creation, 3-113
Filter Organization, 3-35, 3-77, 3-113

G

General, 1-2
Global Configuration, 3-4, 3-49

H

Hardware, 1-1
Hardware Installation, 2-1
Hardwired Serial Interface Filters, 3-117
HELP Command, 3-86, 3-105
Host Software Installation, 2-12

I

IFCONFIG Command, 3-87, 3-101
In-line Rule Processing, 3-77
Industry Standards, 1-4
Input and Output Filters, 3-76
Installation from PortMaster Console, 3-8, 3-54
IRX Internet Address Setup, 2-11

L

Loading from Tape or Floppy Diskette, 2-9

M

Managing the Filter Table, 3-36, 3-78
Managing the Hosts Table, 3-27, 3-70, 3-105
Managing the Passwords Table, 3-29, 3-71, 3-107
Managing the Routes Table, 3-32, 3-75, 3-110
Monitoring the PortMaster, 3-24, 3-68

N

Network Booting, 2-3

O

Operating Modes, 1-4

P

Packet Filters, 3-34, 3-76, 3-111
Packet Processing, 3-116
Password Parameters, 3-31, 3-73
PING Command, 3-87, 3-102
Pmconsole with X Windows, 3-2
PMLOGIN Command, 3-87, 3-102
PortMaster Console, 3-1
PortMaster Login, 3-3, 3-48
Power, 2-2
Power Selection and Connection, 2-3
Protocol Filtering, 3-77
PTRACE Command, 3-87, 3-102

Q

QUIT, DONE, EXIT, 3-86, 3-104

R

RADIUS, 3-46, 3-84
Rear Panel Layout, 2-1
REBOOT Command, 3-86, 3-103
Requesting Assistance, 1-6
RESET Command, 3-86, 3-103
RLOGIN Command, 3-87, 3-103
Routing, 1-3
Running pmconsole, 3-1
Running pminstall, 2-10

S

SAVE Command, 3-86, 3-104, 3-110, 3-111
Saving Filters, 3-116
Saving SNMP Configurations, 3-122
Security, 1-2
Self-Test and Diagnostic Messages, 2-3

Serial Port Parameters, 3-12, 3-57
Serial Ports, 2-2
SET Command, 3-86, 3-88, 3-108
Setting Community Names, 3-121
Setting Filter Rules, 3-114
Setting Global Parameters, 3-88
Setting Port Parameters, 3-92
Setting Read Hosts, 3-121
Setting the Asynchronous Port Type, 3-91
Setting Write Hosts, 3-122
SHOW Command, 3-86, 3-100, 3-107, 3-108
Simple Rule Creation, 3-77
Smart Features, 1-5
SNMP Parameters, 3-83
Source and Destination Address Filtering, 3-76
Source and Destination Port Filtering, 3-77
Standard Mode Parameters, 3-13, 3-57
Synchronous Port Configuration, 3-64
Synchronous WAN Port Configuration, 3-20
Synchronous WAN Port Parameters, 3-22, 3-66

T

TELNET Command, 3-87, 3-103
The User Commands, 3-86
Thick Ethernet, 2-4
Thin Ethernet, 2-4, 2-7
TRACEROUTE Command, 3-87, 3-104
Twisted Pair Ethernet, 2-4, 2-8

U

Unlimited Number of Rules, 3-77
Using the Commands, 3-87

V

VERSION Command, 3-86

Viewing Filters, 3-115
Viewing SNMP Configurations, 3-122

W

WAN Ports, 2-4
WAN Protocols, 1-3
Workstation Software Installation, 2-9