

PortMaster®

Configuration Guide

Lucent Technologies

Remote Access Business Unit

4464 Willow Road

Pleasanton, CA 94588

925-737-2100

800-458-9966

May 1998

950-1182D

Copyright and Trademarks

© 1995, 1997, 1998 Lucent Technologies. All rights reserved.

PortMaster, ComOS, and ChoiceNet are registered trademarks of Lucent Technologies. RADIUS ABM, PMVision, PMconsole, and IRX are trademarks of Lucent Technologies, Inc. ProVision is a service mark of Lucent Technologies, Inc. All other marks are the property of their respective owners.

Disclaimer

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

Contents

About This Guide

Audience	xvii
PortMaster Documentation	xvii
Additional References	xix
RFCs	xix
ITU-T Recommendations	xxi
Books	xxi
Document Conventions	xxii
Document Advisories	xxiii
Contacting Lucent Remote Access Technical Support	xxiii
For the EMEA Region	xxiv
For North America, Latin America, and the Asia Pacific Region	xxiv
PortMaster Training Courses	xxiv
Subscribing to PortMaster Mailing Lists	xxv

1. Introduction

PortMaster Software	1-1
Preconfiguration Planning	1-2
Configuration Tips	1-3
Basic Configuration Steps	1-4

2. How the PortMaster Works

Booting the PortMaster	2-1
PortMaster Initialization	2-3

On-Demand Connections	2-4
PortMaster Security Management	2-4
Port Status and Configuration	2-5
3. Configuring Global Settings	
Setting the System Name	3-2
Setting the Administrative Password	3-2
Setting the Dynamic Host Control Protocol (DHCP) Server	3-2
How the Cable Modem Telephone Return System Works	3-3
Setting the Default Route Gateway	3-5
Configuring Default Routing	3-6
Configuring Name Resolution	3-6
Using the Host Table	3-7
Setting the Name Service	3-7
Setting the Name Server	3-8
Setting the Domain Name	3-8
Setting the Telnet Port	3-9
Using the Telnet Port as a Console Port	3-9
Setting the Number of Management Application Connections	3-9
Setting System Logging	3-9
Setting the Loghost	3-10
Disabling and Redirecting Syslog Messages	3-10
Setting Administrative Logins to Serial Ports	3-12
Configuring an IP Address Pool	3-12
Setting the Reported IP Address	3-13
Configuring SNMP	3-13
About the livingston.mib Definition File	3-14
Examining the MIB Structure	3-14

PortMaster Modem Table	3-20
Setting SNMP Monitoring	3-21
Setting SNMP Read and Write Community Strings	3-21
Adding SNMP Read and Write Hosts	3-22
Viewing SNMP Settings	3-23
Monitoring SNMP Alarms	3-23
Displaying the Routing Table	3-23
Setting Static Routes	3-24
Adding and Deleting a Static Route for IP	3-24
Adding and Deleting a Static Route for IPX	3-25
Modifying the Static Netmask Table	3-26
Enabling NetBIOS Broadcast Packet Propagation	3-29
Setting Authentication for Dial-In Users	3-29
Setting Call-Check Authentication	3-30
Setting the ISDN Switch	3-30

4. Configuring the Ethernet Interface

Setting General Ethernet Parameters	4-1
Configuring RIP Routing	4-1
Applying Filters	4-2
Setting IP Parameters	4-3
Setting the IP Address	4-3
Setting the Subnet Mask	4-4
Setting the Broadcast Address	4-4
Enabling or Disabling IP Traffic	4-4
Setting Ethernet IPX Parameters	4-5
Setting the IPX Network Address	4-5
Enabling or Disabling IPX Traffic	4-5
Setting the IPX Frame Type	4-6

Configuring Ethernet Subinterfaces	4-7
Setting OSPF on the Ethernet Interface	4-8
5. Configuring an Asynchronous Port	
Asynchronous Port Uses	5-1
General Asynchronous Port Settings	5-3
Overriding Certain Port Settings	5-3
Setting the Port Speed	5-3
Parity Checking	5-4
Setting Databits	5-4
Setting Flow Control	5-4
Setting the Dial Group	5-5
Displaying Extended Port Information	5-5
Setting the Login Prompt	5-5
Setting the Login Message	5-6
Setting an Optional Access Filter	5-6
Setting Port Security	5-6
Allowing Users to Connect Directly to a Host	5-6
Setting a Port as the Console	5-7
Setting the Port Idle Timer	5-7
Configuring a PortMaster for Login Users	5-8
Setting the Port Type	5-9
Setting the Login Service	5-10
Setting the Login Host	5-11
Setting the Terminal Type	5-11
Configuring a Port for Access to Shared Devices	5-11
Setting the Device Service	5-14
Configuring a Port for Network Access	5-15
Network Dial-In-Only Access	5-16

Network Dial-Out-Only Access	5-17
Network Dial-In-and-Out (Two-Way) Access	5-18
Configuring a Port for a Dedicated Connection	5-20
Setting the Protocol	5-22
Setting the MTU Size	5-22
Setting the Destination IP Address and Netmask	5-22
Setting the IPX Network Number	5-22
Configuring RIP Routing	5-23
Configuring Compression	5-23
Setting the PPP Asynchronous Map	5-24
Setting Input and Output Filters	5-25
Connecting without TCP/IP Support	5-25
6. Configuring a Synchronous WAN Port	
Synchronous Port Uses	6-1
Configuring WAN Port Settings	6-4
General Synchronous Settings	6-4
Settings for Hardwired Connections	6-7
7. Configuring Dial-In Users	
Configuring the User Table	7-1
Displaying User Information	7-2
Adding Users to the User Table	7-2
Deleting Users from the User Table	7-3
User Types	7-3
Network Users	7-3
Login Users	7-3
Configuring Settings for Network and Login Users	7-4
Setting a Password	7-4

Setting the Idle Timer	7-4
Setting the Session Limit	7-4
Configuring Network Users	7-4
Setting the Protocol	7-5
Setting the User IP Address	7-5
Setting the Subnet Mask	7-6
Setting the IPX Network Number	7-6
Configuring RIP Routing	7-6
Setting the Asynchronous Character Map	7-7
Setting the MTU Size	7-7
Setting the Maximum Number of Dial-In Ports	7-8
Setting Compression	7-8
Setting Filters	7-9
Specifying a Callback Location	7-10
Configuring Login Users	7-10
Setting the Login Host	7-10
Applying an Optional Access Filter	7-11
Setting the Login Service Type	7-12
Specifying a Callback Telephone Number	7-13
8. Configuring Dial-Out Connections	
Configuring the Location Table	8-1
Creating a Location	8-3
Setting the Connection Type	8-3
Setting the Telephone Number	8-5
Setting the Username and Password	8-5
Setting the Protocol	8-5
Setting the Destination IP Address	8-6
Setting the Destination Netmask	8-6
Setting the IPX Network Number	8-6

Setting RIP Routing	8-7
Setting the Dial Group	8-8
Setting the MTU Size	8-8
Configuring Compression	8-8
Setting the Idle Timer	8-10
Setting Data over Voice	8-10
Setting CHAP	8-10
Setting the Asynchronous Character Map	8-11
Setting Multiline Load Balancing	8-11
Setting the Maximum Number of Dial-Out Ports	8-12
Setting Bandwidth-on-Demand	8-12
Setting Filters	8-13
Input Filters	8-13
Output Filters	8-13
Testing Your Location Configuration	8-14
9. Configuring Filters	
Overview of PortMaster Filtering	9-1
Filter Options	9-2
Filter Organization	9-3
How Filters Work	9-4
Creating Filters	9-5
Creating IP Filters	9-6
Filtering TCP and UDP Packets	9-7
Creating IPX Filters	9-7
Displaying Filters	9-8
Deleting Filters	9-8
Example Filters	9-9
Simple Filter	9-9

Input Filter for an Internet Connection	9-10
Input and Output Filters for FTP Packets	9-11
Rule to Permit DNS into Your Local Network	9-12
Rule to Listen to RIP Information	9-12
Rule to Allow Authentication Queries	9-13
Rule to Allow Networks Full Access	9-13
Restrictive Internet Filter	9-13
Restricting User Access	9-15
10. Using Modems	
Null Modem Cable and Signals	10-1
Modem Functions	10-2
Using Automatic Modem Configuration	10-2
Displaying Modem Settings and Status	10-2
Adding a Modem to the Modem Table	10-3
Associating a Modem with a Port	10-6
Configuring Ports for Modem Use	10-7
Setting the Port Speed	10-7
Setting Modem Control	10-8
Setting Parity	10-8
Setting the Flow Control	10-8
Hanging Up a Line	10-9
11. Configuring the PortMaster 3	
Configuring General Settings	11-1
Displaying Line Status	11-2
Configuring Line Use	11-2
Setting Channel Groups	11-2
Setting the Channel Rate	11-3
Setting the Inband Signaling Protocol for T1	11-3

Setting the Inband Signaling Protocol for E1	11-4
Configuring ISDN PRI Settings	11-5
Setting the ISDN PRI Switch	11-5
Setting the Framing Format	11-5
Setting the Encoding Method	11-6
Setting the Pulse Code Modulation	11-7
Setting the Loopback	11-7
Setting the Directory Number	11-7
Using True Digital Modems	11-8
Setting Digital Modems	11-8
Hot-Swapping Digital Modem Cards	11-9
Setting Digital Modems to Analog Service	11-9
Using Channelized T1	11-10
Why Use Channelized T1?	11-10
How to Order DS-1 Service from the Telephone Company	11-10
Configuring the PortMaster 3 for Channelized T1	11-11
Example Channelized T1 Configuration	11-11
Using the T1 Expansion Card	11-12
Clocking	11-12
Configuring the T1 Expansion Card for Fractional T1	11-13
Troubleshooting the T1 Expansion Card	11-14
Using Multichassis PPP	11-15
Setting Multichassis PPP	11-15
Displaying Multichassis PPP Addresses	11-15
Disconnecting a User from a Virtual Port	11-15
Troubleshooting the PortMaster 3	11-16

12. Using ISDN BRI

Overview of ISDN BRI Connections	12-1
--	------

Provisioning	12-3
Configuring ISDN	12-4
ISDN BRI Switch Types	12-4
Setting the Switch Type	12-5
Service Profile Identifier (SPID) for ISDN BRI	12-5
Terminal Identifier (TID) for ISDN BRI	12-6
Directory Number	12-6
Information Elements (IEs)	12-6
Multilink PPP	12-7
Multiple Subscriber Network for an S/T Interface	12-8
Port Limits	12-8
Data over Voice	12-8
ISDN Port Configuration Tips	12-9
ISDN BRI Unnumbered IP Configuration Example	12-9
Configuration Steps	12-9
Configuring the PortMaster in Denver	12-11
Configuring the PortMaster in San Francisco	12-15
Testing the Setup	12-20
Troubleshooting an ISDN BRI Connection	12-21
Interpreting ISDN BRI Port Status	12-22
 13. Using Frame Relay	
Overview of Frame Relay	13-1
PVCs and DLCIs	13-2
Line Speed	13-2
Port Speed	13-2
CIR and Burst Speed	13-2
Discarding Frames	13-3
Ordering Frame Relay Service	13-3

LMI Types	13-3
Frame Relay Configuration on the PortMaster	13-4
Enabling LMI	13-5
Enabling Annex-D	13-6
Listing DLCIs for Frame Relay Access	13-6
Configuration Steps for a Frame Relay Connection	13-7
Configuring the PortMaster in Bangkok	13-8
Configuring the PortMaster in New York	13-9
Troubleshooting a Frame Relay Configuration	13-11
Frame Relay Subinterfaces	13-12
Configuring Subinterfaces	13-12
Troubleshooting Subinterfaces	13-14
Example: Configuring a Frame Relay Subinterface	13-15
14. Using Synchronous V.25bis Connections	
Overview of Synchronous V.25bis Dial-Up Connections	14-1
Configuration Steps for a Synchronous V.25bis Connection	14-3
Configuring the PortMaster in Boston	14-3
Configuring the PortMaster in Miami	14-7
Testing the Configuration	14-12
Troubleshooting a Synchronous V.25bis Connection	14-13
15. Using Office-to-Office Connections	
Overview of Example Configuration	15-1
Configuration Steps for an Office-to-Office Connection	15-3
Configuring the Office Router in London	15-4
Configuring the PortMaster in Paris	15-8
Testing the Setup	15-12
Setting the Console Port for Multiline Load Balancing	15-13

Using ISDN for On-Demand Connections	15-15
16. Using Internet Connections	
Overview of Continuous Internet Connections	16-3
Configuration Steps for an Internet Connection	16-3
Configuring Global Settings	16-4
Configuring Port Settings	16-4
Configuring a Dial-Out Location	16-7
Testing the Continuous Dial-Out Setup	16-8
Testing the Network Hardwired Setup	16-9
Providing Network Filtering	16-10
Using ISDN for Internet Connections	16-11
17. Providing User Dial-In Access	
Overview of Dial-In Configuration	17-1
Example Configuration	17-3
Configuration Steps for Dial-In Access	17-4
Connecting Modems	17-5
Configuring Global Settings	17-5
Configuring Ports	17-6
Configuring Users	17-8
Dial-In Login Users	17-9
Dial-In Network Users	17-9
Testing the User Dial-In Setup	17-10
18. Accessing Shared Devices	
Overview of Shared Device Access Methods	18-1
Host Device Configuration	18-1
Network Device Configuration	18-2
Configuration Steps for Shared Device Access	18-4

Configuring Global Settings	18-4
Configuring Port Settings	18-5
Configuring a Network Device for Telnet Access	18-8
19. Using Synchronous Leased Lines	
Overview of Leased Line Connections	19-1
Configuration Steps for Leased Line Connections	19-3
Configuring the PortMaster Office Router in Rome	19-4
Configuring the PortMaster Office Router in Florence	19-6
Troubleshooting a Leased Line Connection	19-8
A. Networking Concepts	
Network Addressing	A-1
IP Addressing	A-1
IP Address Notation	A-2
Reserved IP Addresses	A-5
Private IP Networks	A-5
IP Address Conventions	A-6
IPX Addressing	A-6
Netmasks	A-7
Using Naming Services and the Host Table	A-8
Managing Network Security	A-9
RADIUS	A-10
ChoiceNet	A-10
B. TCP and UDP Ports and Services	
Glossary	
Command Index	
Subject Index	

About This Guide

The *PortMaster® Configuration Guide* provides general information about networking and network configuration as well as specific information needed to configure PortMaster products. Review this guide thoroughly before configuring your PortMaster. This guide provides the settings required for the most commonly used PortMaster configurations.

To use this guide you must have successfully installed your PortMaster according to the instructions provided in the relevant installation guide. This guide provides configuration information only.

You can use either of two interfaces to configure the PortMaster:

- **Command line interface**—use this guide and the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.
- **PMVision™ graphical user interface (GUI).**

This guide assumes you are using the command line interface and provides examples of command line usage.

Audience

This guide is designed for qualified system administrators and network managers, and for persons with a working knowledge of networking and routing. Appendix A, “Networking Concepts,” provides an overview of network address conventions but is intended as a quick refresher and should not be used as a substitute for careful study of these principles.

Refer to “Additional References” in this Preface for appropriate RFCs and other suggested reading. See the *PortMaster Routing Guide* for advanced information on routing protocols and routing with PortMaster products.

PortMaster Documentation

The following manuals are available from Lucent Technologies. The hardware installation guides are included with most PortMaster products; other manuals can be ordered through your PortMaster distributor or directly from Lucent.

The manuals are also provided as PDF and PostScript files on the *PortMaster Software CD* shipped with your PortMaster.

In addition, you can download PortMaster information and documentation from **<http://www.livingston.com>**.

- *ChoiceNet® Administrator's Guide*

This guide provides complete installation and configuration instructions for ChoiceNet server software.

- *PortMaster Command Line Reference*

This guide provides the complete description and syntax of each command in the ComOS command set.

- *PortMaster Configuration Guide*

This guide provides a comprehensive overview of networking and configuration issues related to PortMaster products.

- PortMaster hardware installation guides

These guides contain complete hardware installation instructions. An installation guide is available for each PortMaster product line—IRX™, Office Router, Communications Server, and Integrated Access Server.

- *PMconsole™ for Windows Administrator's Guide*

This guide covers PMconsole Administration Software for Microsoft Windows, a graphical tool for configuring the PortMaster. The majority of the material in this guide also applies to the UNIX version of PMconsole. Lucent recommends that you use the Java GUI PMVision rather than PMconsole to configure and manage a PortMaster.

- *PortMaster Routing Guide*

This guide describes routing protocols supported by PortMaster products, and how to use them for a wide range of routing applications.

- *PortMaster Troubleshooting Guide*

This guide can be used to identify and solve software and hardware problems in the PortMaster family of products.

- *RADIUS Administrator's Guide*

This guide provides complete installation and configuration instructions for Lucent Remote Authentication Dial-In User Service (RADIUS) software.

Additional References

RFCs

Use any World Wide Web browser to find a Request for Comments (RFC) online.

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specification*

RFC 950, *Internet Standard Subnetting Procedure*

RFC 1058, *Routing Information Protocol*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1166, *Internet Numbers*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1256, *ICMP Router Discovery Messages*

RFC 1321, *The MD5 Message-Digest Algorithm*

RFC 1331, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*

RFC 1334, *PPP Authentication Protocols*

RFC 1349, *Type of Service in the Internet Protocol Suite*

RFC 1413, *Identification Protocol*

RFC 1490, *Multiprotocol Interconnect Over Frame Relay*

RFC 1541, *Dynamic Host Configuration Protocol*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 1552, *The PPP Internet Packet Exchange Control Protocol (IPXCP)*

RFC 1587, *OSPF NSSA Options*
RFC 1597, *Address Allocations for Private Internets*
RFC 1627, *Network 10 Considered Harmful (Some Practices Shouldn't be Codified)*
RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*
RFC 1661, *The Point-to-Point Protocol (PPP)*
RFC 1700, *Assigned Numbers*
RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
RFC 1812, *Requirements for IP Version 4 Routers*
RFC 1814, *Unique Addresses are Good*
RFC 1818, *Best Current Practices*
RFC 1824, *Requirements for IP Version 4 Routers*
RFC 1825, *Security Architecture for the Internet Protocol*
RFC 1826, *IP Authentication Header*
RFC 1827, *IP Encapsulating Payload*
RFC 1828, *IP Authentication Using Keyed MD5*
RFC 1829, *The ESP DES-CBC Transform*
RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1878, *Variable Length Subnet Table for IPv4*
RFC 1918, *Address Allocation for Private Internets*
RFC 1965, *Autonomous System Confederations for BGP*
RFC 1966, *BGP Route Reflection, An Alternative to Full Mesh IBGP*
RFC 1974, *PPP Stac LZS Compression Protocol*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 1997, *BGP Communities Attribute*
RFC 2003, *IP Encapsulation within IP*
RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
RFC 2125, *The PPP Bandwidth Allocation Protocol (BAP), The PPP Bandwidth Allocation Control Protocol (BACP)*
RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*
RFC 2139, *RADIUS Accounting*
RFC 2178, *OSPF Version 2*

ITU-T Recommendations

The following documents are recommendations of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), formerly known as CCITT:

- Recommendation V.25bis (1988)—*Automatic calling and/or answering equipment on the general switched telephone network (GSTN) using the 100-series interchange circuits*
- Recommendation V.120 (09/92)—*Support by an ISDN of data terminal equipment with V-series type interfaces for statistical multiplexing*

Books

The Basics Book of ISDN. Motorola Codex. Reading, MA: Addison-Wesley Publishing Company, 1991. (ISBN 0-201-56368-1)

Building Internet Firewalls. D. Brent Chapman and Elizabeth D. Zwicky. Sebastopol, CA: O'Reilly & Associates, Inc., 1995. (ISBN 1-56592-124-0)

DNS and BIND, 2nd ed. Paul Albitz and Cricket Liu. Sebastopol, CA: O'Reilly & Associates, Inc., 1992. (ISBN 1-56592-236-0)

Firewalls and Internet Security: Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Reading, MA: Addison-Wesley Publishing Company, 1994. (ISBN 0-201-63357-4) Japanese translation is available (ISBN 4-89052-672-2). Errata are available from **ftp://ftp.research.att.com/dist/internet_security/firewall.book**.

Internetworking with TCP/IP Volume 1: Principles, Protocols, and Architecture, 3rd ed. Douglas E. Comer. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1995. (ISBN 0-13-216987-8)

The ISDN Consultant. Robert E. Lee. Upper Saddle River, NJ: Prentice-Hall, Inc. 1996. (ISBN 0-13-259052-2)

ISDN: How to Get a High-Speed Connection to the Internet. Charles Summers and Bryant Dunetz. New York, NY: John Wiley and Sons, Inc. 1996. (ISBN 0-47-113326-4)

TCP/IP Network Administration. Craig Hunt. Sebastopol, CA: O'Reilly & Associates, Inc., 1992. (ISBN 0-937175-82-X)

Routing in the Internet. Christian Huitema. Prentice Hall PTR, 1995.
(ISBN 0-13-132192-7)

TCP/IP Illustrated, Volume 1: The Protocols. W. Richard Stevens. Addison-Wesley Publishing Company. 1994. (ISBN 0-201-63346-9)

Internet Routing Architectures. Bassam Halabi. Cisco Press, 1997.

Document Conventions

The following conventions are used in this guide:

Convention	Use	Examples
Bold font	Indicates a user entry—a command, menu option, button, or key—or the name of a file, directory, or utility, except in code samples.	<ul style="list-style-type: none"> Enter version to display the version number. Press Enter. Open the permit_list file.
<i>Italic font</i>	Identifies a command-line placeholder. Replace with a real name or value.	<ul style="list-style-type: none"> set <i>Ether0</i> address <i>Ipaddress</i> Replace <i>Area</i> with the name of the OSPF area.
Square brackets ([])	Enclose optional keywords and values in command syntax.	<ul style="list-style-type: none"> set nameserver [2] <i>Ipaddress</i> set <i>S0</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	set syslog <i>Logtype</i> {[disabled] [<i>Facility.Priority</i>]}

Convention	Use	Examples
Vertical bar ()	Separates two or more possible options in command syntax.	<ul style="list-style-type: none">• set S0 W1 ospf on off• set S0 host default prompt IpAddress

Document Advisories



Note – means take note. Notes contain information of importance or special interest.



Caution – means be careful. You might do something—or fail to do something—that results in equipment failure or loss of data.



Warning – means danger. You might do something—or fail to do something—that results in personal injury or equipment damage.

Contacting Lucent Remote Access Technical Support

The PortMaster comes with a 1-year hardware warranty.

For all technical support requests, record your PortMaster ComOS version number and report it to the technical support staff or your authorized sales channel partner.

New releases and upgrades of PortMaster software are available by anonymous FTP from **ftp://ftp.livingston.com.pub/le/**.

In North America you can schedule a 1-hour software installation appointment by calling the technical support telephone number listed below. Appointments must be scheduled at least one business day in advance.

For the EMEA Region

If you are an Internet service provider (ISP) or other end user in Europe, the Middle East, Africa, India, or Pakistan, contact your local Lucent Remote Access sales channel partner. For a list of authorized sales channel partners, see the World Wide Web at <http://www.livingston.com/International/EMEA/distributors.html>.

If you are an authorized Lucent Remote Access sales channel partner in this region, contact the Lucent Remote Access EMEA Support Center Monday through Friday between the hours of 8 a.m. and 8 p.m. (GMT+1), excluding French public holidays.

- By voice, dial +33-4-92-92-48-88.
- By fax, dial +33-4-92-92-48-40.
- By electronic mail (email) send mail to **emea-support@livingston.com**

For North America, Latin America, and the Asia Pacific Region

Contact Lucent Remote Access Monday through Friday between the hours of 6 a.m. and 6 p.m. (GMT -8).

- By voice, dial 800-458-9966 within the United States (including Alaska and Hawaii), Canada, and the Caribbean, or +1-925-737-2100 from elsewhere.
- By fax, dial +1-925-737-2110.
- By email, send mail as follows:
 - From North America and Latin America to **support@livingston.com**.
 - From the Asia Pacific Region to **asia-support@livingston.com**.
- Using the World Wide Web, see <http://www.livingston.com/>.

PortMaster Training Courses

Lucent Remote Access offers hands-on, technical training courses on PortMaster products and their applications. For course information, schedules, and pricing, visit the Lucent Remote Access website at <http://www.livingston.com>, click **Services**, and then click **Training**.

Subscribing to PortMaster Mailing Lists

Lucent maintains the following Internet mailing lists for PortMaster users:

- **portmaster-users**—a discussion of general and specific PortMaster issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-users** in the body of the message.

The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-users-digest** in the body of the message.

- **portmaster-radius**—a discussion of general and specific RADIUS issues, including configuration and troubleshooting suggestions. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-radius** in the body of the message.

The mailing list is also available in a daily digest format. To receive the digest, send email to **majordomo@livingston.com** with **subscribe portmaster-radius-digest** in the body of the message.

- **portmaster-announce**—announcements of new PortMaster products and software releases. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-announce** in the body of the message. All announcements to this list also go to the portmaster-users list. You do not need to subscribe to both lists.

This chapter discusses the following topics:

- “PortMaster Software” on page 1-1
- “Preconfiguration Planning” on page 1-2
- “Configuration Tips” on page 1-3
- “Basic Configuration Steps” on page 1-4

PortMaster Software

All PortMasters are shipped with the following software:

- **ComOS®**—The communication software operating system already loaded in Flash RAM on each PortMaster. You can use the ComOS command line interface to configure your PortMaster through a console.
- **PMVision**—A GUI companion to the ComOS command line interface for Microsoft Windows, UNIX, and other platforms that support the Java Virtual Machine (JVM). Because PMVision also supports command entry, you can use a combination of GUI panels and ComOS commands to configure, monitor, and debug a PortMaster. When connected to one or more PortMaster products, PMVision allows you to monitor activity and edit existing configurations. PMVision replaces the PMConsole interface to ComOS.
- **pmd** or **in.pmd**—The optional PortMaster daemon software that can be installed on UNIX hosts to allow the host to connect to printers or modems attached to a PortMaster. The daemon also allows the PortMaster to multiplex incoming users onto the host using one TCP stream instead of multiple streams like rlogin. The daemon is available for SunOS, Solaris, AIX, HP-UX, and other platforms.

For installation and configuration instructions, copy the PortMaster software to the UNIX host as described in the *PortMaster Software CD* booklet.

- RADIUS—The RADIUS server, **radiusd**, runs as a daemon on UNIX systems, providing centralized authentication for dial-in users. The **radiusd** daemon is provided to customers in binary and source form for SunOS, Solaris, Solaris/X8.6, AIX, HP-UX, IRIX, Alpha OSF/1, Linux, and BSD/OS platforms.

For installation and configuration instructions, see the *RADIUS Administrator's Guide*.

- ChoiceNet—ChoiceNet is a security technology invented by Lucent to provide a traffic filtering mechanism for networks using dial-up remote access, synchronous leased-line, or Ethernet connections. When used with RADIUS, ChoiceNet provides exceptional flexibility in fine-tuning the level of access provided to users.

For installation and configuration instructions, see the *ChoiceNet Administrator's Guide*.

Preconfiguration Planning

Before the PortMaster can be used to connect wide area networks (WANs), you must install the hardware using the instructions in the installation guide for your system.

This configuration guide is designed to introduce the most common configuration options available for PortMaster products. Review this material before you configure your PortMaster and, if possible, answer the following questions:

- What general configuration do you want to implement?
- Do you want to use a synchronous connection to a high-speed line?
- Will your high-speed lines use Frame Relay, ISDN, switched 56Kbps, or PPP?
- If you want dial-on-demand routing, do you want multiline load-balancing?
- Do you want multilink PPP (RFC 1717)?
- Do you want packet filtering for Internet connections?
- Do you want packet filtering for connections to other offices?
- Do you want dial-in users to use SLIP, PPP, or both?
- If you use PPP, do you want PAP or CHAP authentication?
- Are you using a name service—DNS or NIS?
- Have you obtained the necessary network addresses?

- Are you running IP, IPX, or both?
- Do you want to enable SNMP for network monitoring?
- Do you want dial-in only, dial-out only, or two-way communication on each port?
- What characteristics do you want to assign to the dial-out locations?
- How do you want to configure dial-in users?
- Do you want to use RADIUS to authenticate dial-in users, or the internal user table on the PortMaster?
- Do you want to use ChoiceNet to filter network traffic?
- Do you want to use the console port for administration functions, or do you want to attach an external modem to the port?
- For dial-in uses, do you receive service on analog lines, ISDN BRI, ISDN PRI, channelized T1, or E1?

Many other decisions must be made during the configuration process. This guide discusses the various configuration options and their implications.

Configuration Tips

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

If You Are Configuring...	Then Configure Settings on...
A network hardwired port or hardwired multiline load balancing	The port
One or more ports for dial-out operation	Dial-out locations using the location table
One or more ports for dial-in operation	Dial-in users using the user table or RADIUS
A callback network user	The callback location in the location table, and refer to the location name in the user table

Basic Configuration Steps

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

1. **Install the PortMaster hardware and assign an IP address and a password as described in the installation guide shipped with your PortMaster.**



Note – This guide assumes that you have completed Step 1 and does not give details on hardware installation or IP address assignment.

2. **Boot the system and log in with the administrative password.**

You can configure the PortMaster from a terminal attached to the console port, by an administrative Telnet session, or by a network connection.

3. **If you want to use PMVision software to configure your PortMaster, install it on a workstation anywhere on your network.**

See the PMVision online help for more information.

4. **Configure the global settings.**

PortMaster global settings are described in Chapter 3, “Configuring Global Settings.”

5. **Configure the Ethernet settings, and configure the IP and IPX protocol settings for your network.**

PortMaster Ethernet settings are described in Chapter 4, “Configuring the Ethernet Interface.”

6. **Configure the asynchronous port(s).**

PortMaster asynchronous port settings are described in Chapter 6, “Configuring a Synchronous WAN Port.”

7. **Configure the synchronous port(s), if available.**

PortMaster synchronous port settings are described in Chapter 6, “Configuring a Synchronous WAN Port.”

8. **Configure ISDN BRI connection(s), if available.**

ISDN PRI connection configuration is described in Chapter 11, “Configuring the PortMaster 3.” ISDN BRI connection configuration is covered in Chapter 12, “Using ISDN BRI.”

9. Configure dial-in users in the user table, or configure RADIUS.

The user table is described in Chapter 7, “Configuring Dial-In Users.” If you are using RADIUS security instead of the user table, see the *RADIUS Administrator's Guide*.

10. Configure ChoiceNet, if you are using it.

ChoiceNet is a traffic filtering mechanism for networks using dial-up remote access, synchronous leased-line, or Ethernet. Refer to the *ChoiceNet Administrator's Guide* for more information.

11. Configure dial-out locations in the location table.

The location table is described in Chapter 8, “Configuring Dial-Out Connections.”

12. Configure filters in the filter table.

Once the filters are created, they can be assigned as input or output filters for the Ethernet interface, users, locations, or hardwired ports. Filters are described in Chapter 9, “Configuring Filters.”

13. Configure OSPF, if you are using this protocol.

OSPF is described in the *PortMaster Routing Guide*.

14. Configure BGP, if you are using this protocol.

BGP is described in the *PortMaster Routing Guide*.

15. Troubleshoot your configuration, if necessary, and back it up.

See the *PortMaster Troubleshooting Guide* for instructions.

Once you have correctly configured all the settings necessary for your circumstances, your PortMaster is ready to provide communication service and routing for your network.

This chapter summarizes PortMaster operation and capabilities so you can choose how to configure your system. Consult the glossary for definitions of unfamiliar terms.

This chapter discusses the following topics:

- “Booting the PortMaster” on page 2-1
- “PortMaster Initialization” on page 2-3
- “On-Demand Connections” on page 2-4
- “PortMaster Security Management” on page 2-4
- “Port Status and Configuration” on page 2-5

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Booting the PortMaster

When you start up the PortMaster, it carries out the following functions during the booting process:

1. Self-diagnostics are performed. The results are displayed to asynchronous console port C0 or S0 if the console DIP switch (first from the left, also known as DIP 1) is up.
2. ComOS is loaded.
 - If the netboot DIP switch (second from the left, also known as DIP 2) is down, the PortMaster boots from the ComOS stored in nonvolatile Flash RAM. The PortMaster uncompresses and loads the ComOS into dynamic RAM (DRAM). If a valid ComOS is not found in Flash, the PortMaster attempts to boot from the network as described in the next paragraph.
 - If the netboot DIP switch is up, or if a valid ComOS is not found in Flash, the PortMaster sends a Reserve Address Resolution Protocol (RARP) message to the Ether0 Ethernet interface to find its IP address. If it gets a reply, the PortMaster

then attempts to boot itself across the network using the Trivial File Transfer Protocol (TFTP) to download a netbootable ComOS image from the host that replied to the RARP.

The TFTP process begins by transferring the **/tftpboot/address.typ** file, replacing *address* with the uppercase 8-character hexadecimal expression of the IP address of the PortMaster and *typ* with the 3-character boot extension describing the model of PortMaster, as shown in Table 2-1. If **/tftpboot/address.typ** is not found, the PortMaster requests **/tftpboot/GENERIC.OS**.

Table 2-1 Boot Extensions

Boot Extension	PortMaster Model
PM3	PM3
PM2	PM-2, PM-2E, PM-2R, PM-2ER, PM-2i, PM-2Ei
IRX	IRX, any model
P25	PM-25
PMO	PortMaster Office Router, any model

The netbootable ComOS can also be downloaded via serial cable through the console port. Refer to the *PortMaster Troubleshooting Guide* for details.

- 3. The user configuration is loaded from Flash RAM.
- 4. The IP address is located.

If no address is configured for the Ethernet interface and no address was obtained from netbooting, the PortMaster sends a RARP message to discover its IP address. If the PortMaster receives a reply to the RARP message, its IP address is set in dynamic memory.

At this point the PortMaster is fully booted with its configuration loaded into DRAM. This process takes less than a minute. After the PortMaster boots successfully, the status LED is on, blinking off once every 5 seconds. Refer to the hardware installation guide for your PortMaster for the location of the status LED and for troubleshooting procedures if the LED is not behaving as described.

PortMaster Initialization

Once the PortMaster has successfully booted, it does the following:

1. Ethernet interfaces are started.
2. Modem initialization strings are sent to asynchronous ports that have modem table entries defined.
3. Network hardwired ports are initiated.
4. Continuous dial-out connections are initiated.
5. On-demand dial-out connections for locations that have routing enabled are initiated, and routing information is exchanged between the PortMaster and those locations.
6. Broadcasting and listening for routing packets are initiated on interfaces configured for routing.
7. TCP connections to PortMaster hosts are established.
8. TCP connections are established to ports configured as host devices by means of the PortMaster device service.
9. The PortMaster listens for TCP connections to any ports configured as network devices.
10. The PortMaster listens for activity on TCP and UDP ports, such as for administrative Telnet sessions on TCP port 23, PMconsole connections on TCP port 1643, and SNMP requests on UDP port 161.
11. Syslog starts, if configured.
12. RADIUS starts, if configured.
13. ChoiceNet starts, if configured.

The PortMaster is now ready to begin providing service.

On-Demand Connections

The PortMaster establishes on-demand connections in the following way:

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

PortMaster Security Management

The PortMaster provides security through the user table, or if configured, RADIUS security. When a dial-in user attempts to authenticate at the login prompt, or via PAP or CHAP authentication, the PortMaster refers to the entry in the user table that corresponds to the user. If the password entered by the user does not match, the PortMaster denies access with an “Invalid Login” message. If no user table entry exists for the user and port security is off, the PortMaster passes the user on to the host defined for that port using the selected login service. In this situation, the specified host is expected to authenticate the user.

If port security is on and the user was not found in the user table, the PortMaster queries the RADIUS server if one has been configured. If the username is not found in the user table, port security is on, and no RADIUS server is configured in the global configuration of the PortMaster, access is denied with an “Invalid Login” message. If the RADIUS server is queried and does not respond within 30 seconds (and neither does the alternate RADIUS server), access is denied with an “Invalid Login” message.

If security is set to **off**, any username that is not found in the user table is sent to the port’s host for authentication and login. If security is set to **on**, the user table is checked first. If the username is not found and a RADIUS server is configured, RADIUS is consulted. When you are using RADIUS security, you must use the **set security S0** command to set security to **on**.

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

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

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

Port Status and Configuration

Use the following command to display the current status, active configuration, and default configuration of each port:

```
Command> show s0|W1|P0
```

Table 2-2 describes each possible status. Refer to the *PortMaster Troubleshooting Guide* for verification information.

Table 2-2 PortMaster Port Status

Status	Description
IDLE	The port is not in use.
USERNAME	<p>The data carrier detect (DCD) signal has been asserted and observed on the port.</p> <ul style="list-style-type: none">• On older PortMaster expansion cards (ports S10 through S29) and system cards (ports S0 through S9), DCD floats high when nothing is attached to the port.• On newer cards, in two-way and device environments, DCD is high when the device is busy. When terminals are attached to the device port and modem control is set to off, USERNAME status indicates that the login: prompt has been sent to the port and should be displayed on the terminal. The PortMaster is waiting for a login request.
HOSTNAME	The host: prompt has been sent to the port. The PortMaster is waiting for a reply.
PASSWORD	The Password: prompt has been sent to the port. The PortMaster is waiting for a reply.
CONNECTING	A network connection is attempting to become established on the port.
ESTABLISHED	A connection is active on the port.
DISCONNECTING	The connection has just ended, and the port is returning to the IDLE state.
INITIALIZING	The modem attached to the port is being initialized by the modem table.
COMMAND	The command line interface is being used on the port.
NO-SERVICE	An ISDN port is not receiving service from the telephone company.

This chapter describes how to configure settings that the PortMaster uses across all its ports and interfaces.

This chapter discusses the following topics:

- “Setting the System Name” on page 3-2
- “Setting the Administrative Password” on page 3-2
- “Setting the Dynamic Host Control Protocol (DHCP) Server” on page 3-2
- “Setting the Default Route Gateway” on page 3-5
- “Configuring Default Routing” on page 3-6
- “Configuring Name Resolution” on page 3-6
- “Setting the Telnet Port” on page 3-9
- “Setting the Number of Management Application Connections” on page 3-9
- “Setting System Logging” on page 3-9
- “Setting Administrative Logins to Serial Ports” on page 3-12
- “Configuring an IP Address Pool” on page 3-12
- “Setting the Reported IP Address” on page 3-13
- “Configuring SNMP” on page 3-13
- “Displaying the Routing Table” on page 3-23
- “Setting Static Routes” on page 3-24
- “Enabling NetBIOS Broadcast Packet Propagation” on page 3-29
- “Setting Authentication for Dial-In Users” on page 3-29
- “Setting Call-Check Authentication” on page 3-30
- “Setting the ISDN Switch” on page 3-30

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Setting the System Name

The system name is the name that identifies the PortMaster for SNMP queries, IPX protocol routing, and CHAP authentication. Enter a name that is valid for your network. The system name can have up to 16 characters, and appears in place of the **Command>** prompt on PortMaster products that have it set.

To set the system name, use the following command:

```
Command> set sysname String
```

Setting the Administrative Password

The PortMaster is shipped without a password. Press **Enter** at the **password** prompt when accessing the PortMaster for the first time. The password is an ASCII printable string of up to 16 characters used to access the PortMaster administration features. Only the administrator can change the password.

To set the password, use the following command

```
Command> set password [Password]
```

Using the **set password** command and pressing **Enter** resets the password to the default value, which is no password.

Setting the Dynamic Host Control Protocol (DHCP) Server

The **set dhcp server** command supports the Cable Modem Telephone Return Interface Specification (CMTRIS) developed by the Multimedia Cable Network System (MCNS) Partners Limited. The CMTRIS solves the problem of limited upstream bandwidth in a cable modem system by providing for the use of a standard telephone interface for upstream traffic. Downstream traffic travels on the coaxial cable.

The specification requires that a cable modem be able to use the telephone interface to request and receive the cable interface address and configuration information via a dynamic host control protocol (DHCP) request.

Use the following command to configure a PortMaster product to forward a DHCP request from a cable modem to the DHCP server:

Command> **set dhcp server address**



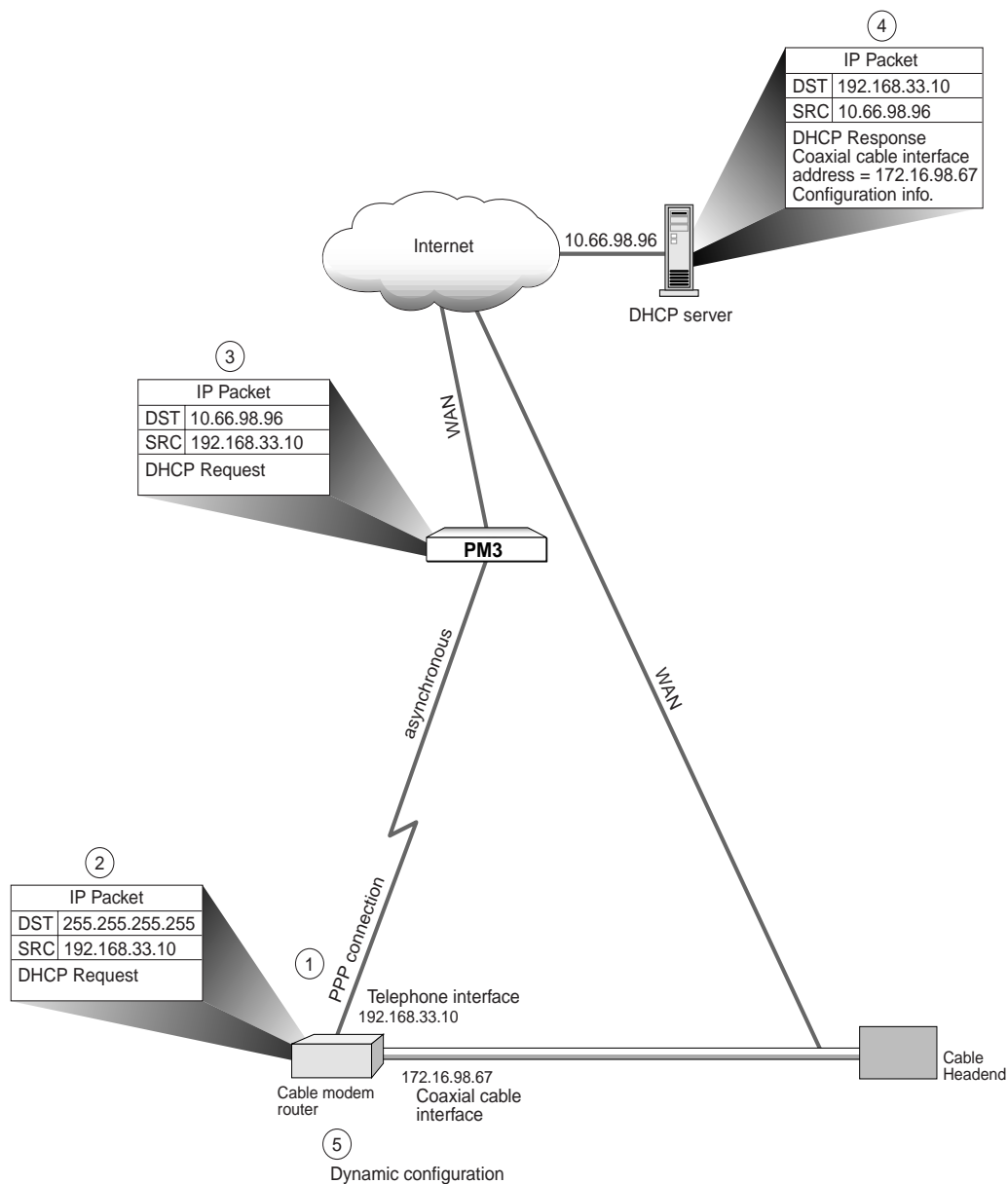
Note – The ComOS does not support DHCP requests over Ethernet (nor requests from PortMaster OR-U dial-up routers).

How the Cable Modem Telephone Return System Works

After you set the IP address of the DHCP server on the PortMaster product, the cable modem dynamically configures itself so that all subsequent data travels upstream via the telephone interface, and downstream on the coaxial cable.

Figure 3-1, using sample IP addresses, illustrates the series of events that begin upon startup and culminate in the dynamic configuration of the cable modem.

Figure 3-1 Cable Modem Telephone Return Interface Startup



11820024

1. Using the telephone interface, the cable modem dials the PortMaster and establishes a PPP connection. The PortMaster assigns IP address 192.168.33.10 to the telephone interface of the cable modem.
2. Using the telephone interface, the cable modem broadcasts a DHCP request. The destination of the request is 255.255.255.255 and the source is 192.168.33.10.
3. The PortMaster forwards the request to the DHCP server by substituting the IP address of the DHCP server (10.66.98.96) for the broadcast destination address.
4. The DHCP server responds with configuration information for the cable modem and an IP address (172.16.98.67) for the coaxial cable interface on the cable modem.
5. Using the configuration information received from the DHCP server, the cable modem dynamically assigns 172.16.98.67 to the cable interface, and configures the cable modem so that upstream IP packets leave the cable modem via the *telephone* interface with the IP address of the cable interface (172.16.98.67) as the source address. Because packets now carry the source address of the cable interface, response to these packets travels via the coaxial cable.

The ComOS does not add routes to its table when forwarding or returning DHCP requests. It transparently forwards and returns DHCP requests from dial-in clients to the specified server.

To view DHCP relaying information, use the **set console** command followed by the **set debug 0x81** command. See the *PortMaster Troubleshooting Guide* for debugging information.

To disable DHCP reply information, enter the following command:

```
Command> set dhcp server 0.0.0.0.
```

The PortMaster does not forward packets to the address 255.255.255.255.

Setting the Default Route Gateway

The default route gateway is the address of a router of last resort to which packets are sent when the PortMaster has no routing information for a packet. The default route gateway is also the destination address the PortMaster selects when it cannot locate the destination of a packet on the local Ethernet segment. You identify the default gateway by its IP address entered in dotted decimal notation. A PortMaster can never be its own default gateway.

You can set a metric between 1 and 15 for the IP and IPX gateways to indicate the hop count associated with the gateway route. The PortMaster uses the hop count value for comparisons if the PortMaster is set to listen for default routes from other routers.

Refer to Appendix A, “Networking Concepts,” for more information about address formats. Refer to the *PortMaster Routing Guide* for more information about routing.

To set the default gateway, use the following command:

```
Command> set gateway Ipaddress [Metric]
```

If you do not specify a value for *Metric*, the PortMaster assumes a default value of 1.

Configuring Default Routing

As described in the *PortMaster Routing Guide*, PortMaster products can automatically send and accept route information as part of RIP messages if routing is turned on. If default routing is on, default routes are sent and accepted as part of the messages.

To configure default routing, use the following command:

```
Command> set default on|off|broadcast|listen
```

Table 3-1 describes the results of using each keyword.

Table 3-1 Default Routing Keywords

Keyword	Description
on	The PortMaster broadcasts and listens for default route information.
off	The PortMaster neither broadcasts nor listens for default route information. This is the default.
broadcast	The PortMaster broadcasts default route information, if it has a default route.
listen	The PortMaster listens for default route information.

Configuring Name Resolution

You can use either a network name service or the host table on the PortMaster to map hostnames to IP addresses.

Using the Host Table

Each host attached to an IP network is assigned a unique IP address. Every PortMaster supports a local host table to map hostnames to IP addresses. If your network lacks a computer that can perform hostname resolution, the PortMaster allows entries in a local host table. Hostnames are used by the PortMaster only for your convenience when using the command line interface, or if you require users to enter hostnames at the host prompt.

To avoid confusion and reduce administrative overhead, Lucent recommends using the Domain Name System (DNS) or Network Information Service (NIS) for hostname resolution rather than the local host table. The PortMaster always checks the local host table before using DNS or NIS. For information on setting the NIS or DNS name service, refer to “Setting the Name Service” on page 3-7.

Setting the Name Service

The PortMaster can work with network name services such as the Network Information Service (NIS) or the Domain Name System (DNS). Appendix A, “Networking Concepts,” describes these name services. You must explicitly identify any name service used on your network.

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

To set the name service, use the following command:

```
Command> set namesvc dns|nis
```

Once the name service is set, you must set the address of your NIS or DNS name server and enter the domain name of your network. See “Setting the Name Server” on page 3-8 for instructions.

Setting the Name Server

The PortMaster supports RFC 1877, which allows remote hosts also supporting RFC 1877 to learn a name server through PPP negotiation. You must provide the IP address of the name server if you use a name service.

You must set a name service before you set a name server. See “Setting the Name Service” on page 3-7. If you are not using a name service, you do not need a name server.

To set the name server, use the following command:

```
Command> set nameserver Ipaddress
```

You can set an alternate name server with the following command:

```
Command> set nameserver 2 Ipaddress
```

You must set a domain name for your network after you set a name server. See “Setting the Domain Name” on page 3-8.

You can disable the use of a name service by setting the name server’s IP address to 0.0.0.0.

Setting the Domain Name

The domain name is used for hostname resolution. If you are using DNS or NIS, you must set a domain name for your network.

To set the domain name of your network, use the following command:

```
Command> set domain String
```

Setting the Telnet Port

The Telnet access port can be set to any number between 0 and 65535. The Telnet port enables you to access and maintain the PortMaster using a Telnet connection to this TCP port. If 0 (zero) is used, Telnet administration is disabled. The default value is 23. Ports numbered 10000 through 10100 are reserved and should not be used for this function. Up to four administrative Telnet sessions at a time can be used.

To set the Telnet access port to port number *Tport*, use the following command:

```
Command> set telnet Tport
```

Using the Telnet Port as a Console Port

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



Note – Only one Telnet session can receive console messages at a time.

To set the current Telnet access port as a console port, enter the following command:

```
Command> set console
```

Setting the Number of Management Application Connections

PMVision, ChoiceNet, and the ComOS utilities **pmdial**, **pmcommand**, **pminstall**, **pmreadconf**, **pmreadpass**, and **pmreset** all use port 1643. In order for more than one of these applications to connect at the same time, you must set the maximum number of connections to two or higher. The maximum is 10 connections.

To set the maximum number of concurrent connections for management applications into the PortMaster, use the following command:

```
Command> set maximum pmconsole Number
```

Setting System Logging

PortMaster products enable you to log authentication information to a system log file for network accounting purposes.

Setting the Loghost

To set the IP address of the loghost—the host to which the PortMaster sends syslog messages—use the following command:

```
Command> set loghost Ipaddress
```



Note – Do not set a loghost at a location configured for on-demand connections, because doing so keeps the connection up or brings up the connection each time a syslog message is queued for the syslog host.

Setting the loghost's IP address to 0.0.0.0 disables syslog from the PortMaster. This change requires a reboot to become effective.

RADIUS accounting provides a more complete method for logging usage information. Refer to the *RADIUS Administrator's Guide* for more information on accounting.

Disabling and Redirecting Syslog Messages

By default, the PortMaster logs five types of events at the informational (info) priority level using the authorization (auth) facility on the log host. You can disable logging of one or more types of events and change the facility and/or priority of log messages.

To disable logging of a type of event, use the following command:

```
Command> set syslog Logtype disabled
```

Use the *Logtype* keyword described in Table 3-2 to identify the type of event you want to disable—or enable again:

Table 3-2 Logtype Keywords

Logtype Keyword	Description
admin-logins	!root and administrative logins.
user-logins	Nonadministrative logins; you might want to disable this logtype if you are using RADIUS accounting.
packet-filters	Packets that match rules with the log keyword.
commands	Every command entered at the command line interface.
termination	More detailed information on how user sessions terminate.

You can change the facility, the priority, or both, of log messages.

To change the facility or priority of log messages, use the following command. Be sure to separate the *Facility* and *Priority* keywords with a period (.).

```
Command> set syslog Logtype Facility.Priority
```

The facility and priority can be set for each of the five types of logged events listed in Table 3-2.

Table 3-3 and Table 3-4 show the keywords used to identify facilities and priorities. Lucent recommends that you use the **auth** facility or the **local0** through **local7** facilities to receive syslog messages from PortMaster products, but all the facilities are provided. See your operating system documentation for information on configuring syslog on your host.

Table 3-3 Syslog Facility Keywords

Facility	Facility Number	Facility	Facility Number
kern	0	cron	15
user	1	local0	16
mail	2	local1	17
daemon	3	local2	18
auth	4	local3	19
syslog	5	local4	20
lpr	6	local5	21
news	7	local6	22
uucp	8	local7	23

Table 3-4 Syslog Priority Keywords

Priority	Number	Typically Used for
emerg	0	System is unusable
alert	1	Action must be taken immediately
crit	2	Critical messages
err	3	Error messages

Table 3-4 Syslog Priority Keywords (Continued)

Priority	Number	Typically Used for
warning	4	Warning messages
notice	5	Normal but significant messages
info	6	Informational messages
debug	7	Debug-level messages

To determine current syslog settings, enter the following command:

Command> **show syslog**

Setting Administrative Logins to Serial Ports

When you log in using **!root**, administrative logins to the serial ports are enabled by default. You can disable or enable them by using the following command:

Command> **set serial-admin on|off**

If administrative login is disabled, you can still use port S0 (or C0) by setting the console DIP switch (first from the left, also known as DIP 1) to the up position.

Configuring an IP Address Pool

You can dynamically assign IP addresses to PPP or SLIP dial-in users. By assigning addresses as needed from a pool, the PortMaster requires fewer addresses than if each user is assigned a specific address. When a dial-in connection is closed, the address goes back into the pool and can be reused.

When creating an address pool, you explicitly identify the first address in the sequence of addresses available for temporary assignment. The PortMaster allocates one address in the pool of addresses for each port configured for network dial-in.

To set the value of the first IP address to assign for dial-in ports, use the following command:

Command> **set assigned_address** *Ipaddress*

The default number of addresses available for the address pool is equal to the number of ports configured for network dial-in. The address pool size is determined during the boot process. You can instead set the number of IP addresses assigned to the pool with the **set pool** command.

To limit the size of the IP address pool, use the following command:

```
Command> set pool Number
```



Note – If you decrease the number of addresses in the pool, you must reboot the PortMaster for the change to take effect.

Setting the Reported IP Address

Some sites require a number of different PortMaster devices to appear as a single IP address to other networks. You can set a reported address different from the Ether0 address. For PPP connections, this address is reported to the outside and placed in the PPP startup message during PPP negotiation. For SLIP connections, this address is reported and placed in the SLIP startup message during SLIP startup.

To set a reported IP address, use the following command:

```
Command> set reported_ip Ipaddress
```

Configuring SNMP

The simple network management protocol (SNMP) is an application-layer protocol that allows devices to communicate management information. You can configure the PortMaster to provide network and device information via SNMP to a network management system (NMS). You must have NMS software to use SNMP.

SNMP consists of the following parts:

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

SNMP specifies the message format for exchanging information between the SNMP manager and an SNMP agent.

The SNMP agent returns values for management information base (MIB) variables that can be changed or queried by the SNMP manager. The agent gathers information from the MIB, which resides on the target device. MIB information can include device parameters and network status. The agent is capable of responding to requests to get or set data from the manager.

PortMaster products support MIB II variables as specified in RFC 1213, along with a MIB specific to PortMaster products. SNMP management can be enabled for any PortMaster. Lucent Remote Access ships configuration files compatible with various network management packages along with the PMconsole software.

About the livingston.mib Definition File

livingston.mib is the MIB definitions file that SNMP tools can read and use to query SNMP agents for information about PortMaster products. The PortMaster extensions to the MIB are located in the latter part of this file under *Livingston Extensions*.

The **livingston.mib** file can be found in the SNMP directory of the ComOS software, or on the World Wide Web at: <http://www.livingston.com/Forms/one-click-download.cgi>. To view the file with a browser, scroll down to the Miscellaneous drop-down menu, select **SNMP—Livingston MIB**, and then click the **Download** button. When the **Download** page appears, click the **livingston.mib** link.

Examining the MIB Structure

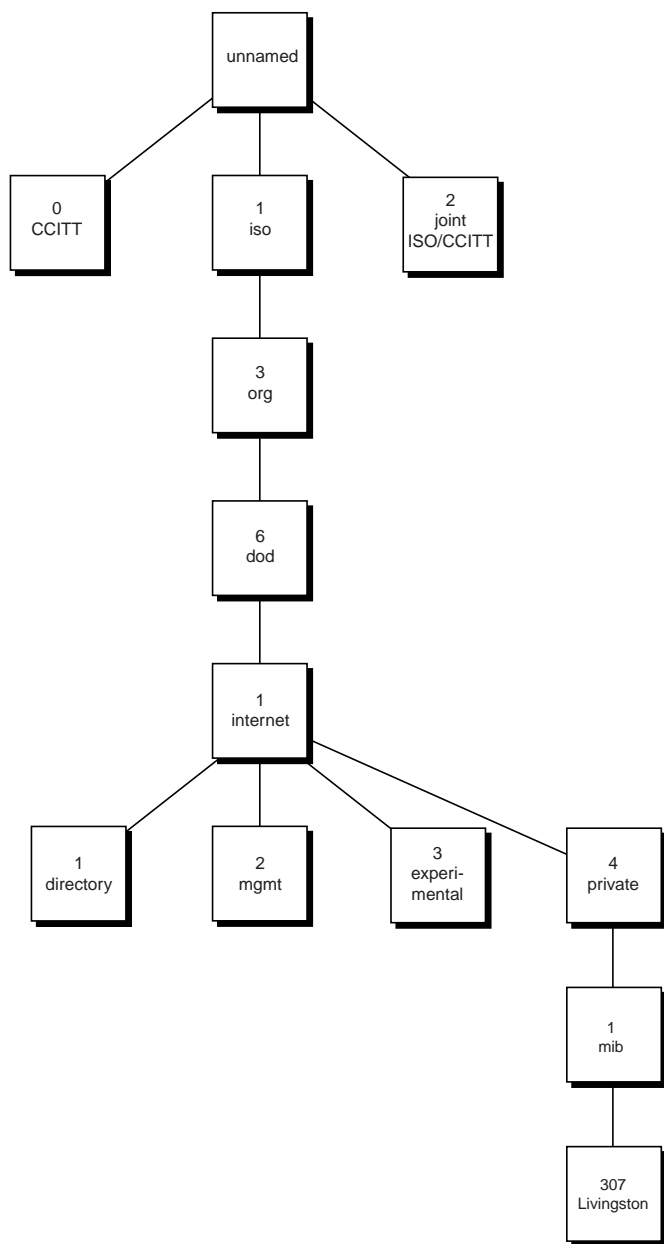
The entire management information base (MIB) hierarchy can be represented by a tree structure. In this representation, the unnamed “root” of the tree divides into the following main branches:

- Consultative Committee for International Telegraph and Telephone (CCITT)
- International Organization for Standardization (ISO)
- ISO/CCITT

Each branch and sub-branch in the tree structure is known as an **object**, and each object is represented by an **object name** and an **object identifier** (OID). Figure 3-2 traces the “path” from the ISO branch of the MIB to the *Livingston* MIB.

OIDs provide compact representations of object names. An OID shows the position of an object in the MIB hierarchy. As shown in Figure 3-2, the OID for the Livingston MIB is 1.3.6.1.4.1.307.

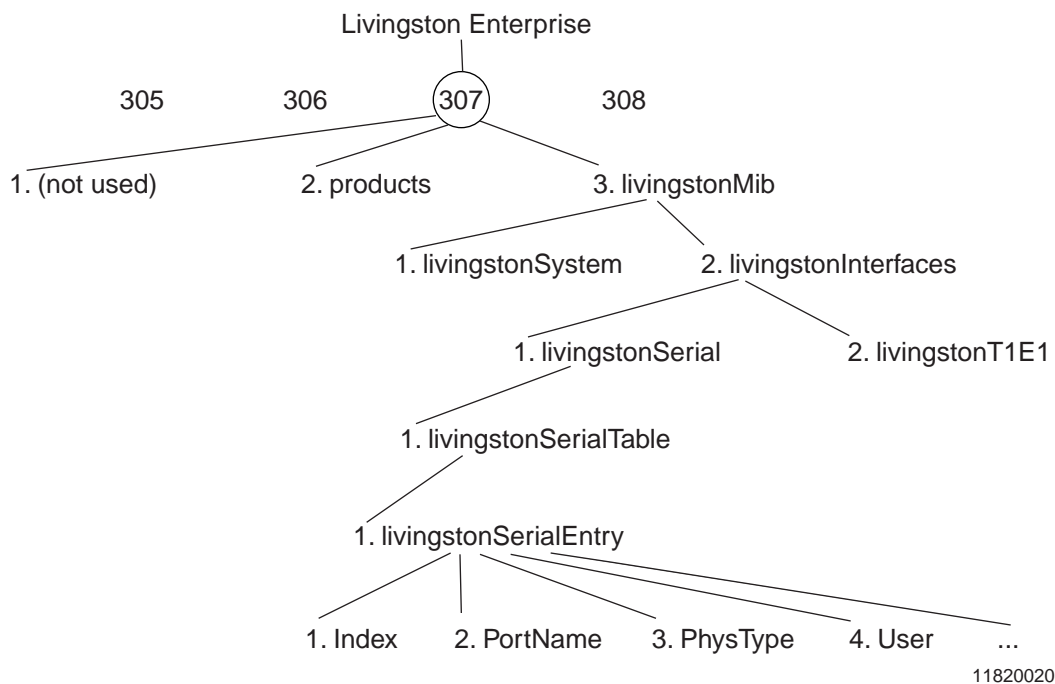
Figure 3-2 Management Information Base (MIB) Hierarchy



11820021

Figure 3-3 shows the tree structure of the private Livingston portion of the MIB.

Figure 3-3 Part of MIB Structure showing PortMaster Port S0.



Reading from the top down, the object identifier (OID) in Figure 3-3 (307.3.2.1.1.1.2) breaks out as follows:

- 307 refers to the Livingston namespace
- 3 refers to the MIB
- 2 refers to interfaces
- 1 refers to serial interfaces
- 1 refers to the serial interfaces table
- 1 refers to an entry in the serial interfaces table
- 2 refers to the PortName variable

The SNMP manager queries the agents by means of OIDs. Each OID uniquely identifies a single MIB variable. For example, the OID 307.3.2.1.1.1.2.0, returns the portname for port S0, and the OID 307.3.2.1.1.1.2.1 returns the port name for port S1 (see Table 3-5).

Table 3-5 Partial View of the Livingston Serial Table.

OID	S0 (0)	S1 (1)	S2 (2)	S3 (3)	S4 (4)
...307.3.2.1.1.1.1	Index	Index	Index	Index	Index
...307.3.2.1.1.1.2	PortName	PortName	PortName	PortName	PortName
...307.3.2.1.1.1.3	PhysType	PhysType	PhysType	PhysType	PhysType
...307.3.2.1.1.1.4	User	User	User	User	User
...307.3.2.1.1.1.5	SessionId	SessionId	SessionId	SessionId	SessionId
...307.3.2.1.1.1.6	Type	Type	Type	Type	Type
...307.3.2.1.1.1.7	Direction	Direction	Direction	Direction	Direction

PortMaster Serial Interfaces

Table 3-6 lists the objects in the serial interface table from the Livingston Extensions section of the MIB. Modem-specific objects apply to the PortMaster 3 only.

Table 3-6 Serial Interfaces Table

Object	Definition
Index	Unique value for each serial interface.
PortName	Text string containing the name of the serial interface (for example, S0, W1, and so on).
PhysType	Type of physical serial interface, distinguished according to the physical or link protocol(s) currently being used on the interface.
User	Name of the active user. Blank if not active.
SessionId	Unique session identifier that matches the RADIUS session ID.
Type	Active type of service being provided by the serial interface.

Table 3-6 Serial Interfaces Table (Continued)

Object	Definition
Direction	Direction in which the active session was initiated.
PortStatus	Status of the serial interface.
Started	Amount of time this session has been active.
Idle	Amount of time this session has been idle.
InSpeed	Estimate of the current inbound bandwidth in bits per second of the serial interface.
OutSpeed	Estimate of the current outbound bandwidth in bits per second of the serial interface.
ModemName (PortMaster 3 only)	Text string containing the name of the digital modem in use by the serial interface.
IpAddress	IP address associated with the serial interface. When characterizing a network port, this value is the IP address of the remote user. When characterizing a device or login port, this value is the IP address of the host to which the user is connected.
ifDescr	Text string containing information about the network interface bound to the serial interface.
InOctets	Total number of octets received on the serial interface.
OutOctets	Total number of octets transmitted on the serial interface.
QOctets	Total number of octets queued on the serial interface.
ModemStatus	Status of the modem used by the serial interface.
ModemCompression (PM-3 only)	Compression being used in the modem or by the serial interface.
ModemProtocol (PortMaster 3 only)	Error correcting protocol being used in the modem or by the serial interface.
ModemRetrains (PortMaster 3 only)	Number of retrains attempted by the modem attached to the serial interface.
ModemRenegotiates (PortMaster 3 only)	Number of renegotiates attempted by the modem attached to the serial interface.

PortMaster T1/E1 Interfaces

Table 3-7 lists the objects in the T1/E1 interfaces from the Livingston Extensions section of the MIB. T1/E1 interfaces are supported on the PortMaster 3 only.

Table 3-7 T1/E1 Interfaces Table

Object	Definition
Index	Unique value for each T1/E1 interface
PhysType	Type of interface (T1 or E1)
Function	Configured function of the interface
Status	Current operational state of the interface. Operational states include the following: <ul style="list-style-type: none">• up (1)• down (2)• loopback (3)
Framing	Configured line framing. Line framing types include the following: <ul style="list-style-type: none">• esf (1)• d4 (2)• crc4 (3)• fas (4)
Encoding	Configured line signal encoding
PCM	Configured voice modulation
ChangeTime	Amount of time this interface has been up or down
RecvLevel	Estimate of the current receive signal level, in decibels, of the interface
BlueAlarms	Total number of blue alarms on the interface
YellowAlarms	Total number of yellow alarms on the interface

Table 3-7 T1/E1 Interfaces Table (Continued)

Object	Definition
CarrierLoss	Total number of times the interface has lost the carrier signal
SyncLoss	Total number of times the interface has lost frame synchronizations
BipolarErrors	Total number of frame-level CRC errors detected on the interface
CRCErrors	Total number of frame-level CRC errors detected on the interface
SyncErrors	Total number of frame synchronization errors detected on the interface

PortMaster Modem Table

Table 3-8, lists the objects in the modem table from the Livingston Extensions section of the MIB. Modem objects are supported only on the PortMaster 3 Integrated Access Server.

Table 3-8 Modem Table

Object Type	Definition
livingstonModemIndex	Unique value for each modem interface
livingstonModemPortName	Textual string containing the name of the serial interface (for example, S0, S1, and so on)
livingstonModemStatus	Current state of the modem
livingstonModemProtocol	Error-correcting protocol being used in the modem
livingstonModemCompression	Compression being used in the modem interface
livingstonModemInSpeed	Estimate of the modem interface's current inbound bandwidth in bits per second
livingstonModemOutSpeed	Estimate of the modem interface's current outbound bandwidth in bits per second

Table 3-8 Modem Table (Continued)

Object Type	Definition
livingstonModemInByteCount	Total number of bytes received by the modem
livingstonModemOutByteCount	Total number of bytes transmitted by the modem
livingstonModemRetrains	Number of retrains attempted by the modem
livingstonModemRenegotiates	Number of renegotiates attempted by the modem
livingstonModemCalls	Number of times a call received by the modem
livingstonModemDetects	Number of analog calls received by the modem
livingstonModemConnects	Number of successful calls received by the modem

Setting SNMP Monitoring

Simple network management protocol (SNMP) monitoring is used to set and collect information on SNMP-capable devices. This feature is most often used to monitor network statistics such as usage and error rate.

If SNMP monitoring is on, the PortMaster accepts SNMP queries. If SNMP monitoring is off, all SNMP queries are ignored.

To turn SNMP monitoring on or off, use the following commands:

```

Command> set snmp on|off
Command> save all
Command> reboot

```

Setting SNMP Read and Write Community Strings

Community strings allow you to control access to the MIB information on selected SNMP devices. The read and write community strings act like passwords to permit access to the SNMP agent information. The read community string must be known by any device allowed to access or read the MIB information. The default read community string is **public**. The write community string must be known by any device before

information can be set on the SNMP agent. The default write community string is **private**. Community strings must be set on SNMP agents so that configuration information is not changed by unauthorized users.

To use this feature, you must set both a read community string and a write community string for your network.

To set SNMP read and write community strings, use the following command:

```
Command> set snmp readcommunity|writecommunity String
```



Note – Use of the default write community string—**private**—is strongly discouraged. Because it is the default, it is known to all users and therefore provides no security. Use another value for the write community string.

Adding SNMP Read and Write Hosts

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

You can also specify a list of hosts allowed to read or write SNMP information. You can permit all hosts or you can deny all hosts.



Note – Permitting all hosts to read and write SNMP information can compromise security and is not recommended.

To add SNMP read and write hosts, use the following command:

```
Command> add snmphost reader|writer any|none|Ipaddress
```

To delete read and write hosts, use the following command:

```
Command> delete snmphost reader|writer Ipaddress
```

Viewing SNMP Settings

Settings for SNMP monitoring, read and write community strings, and read and write hosts are stored in the SNMP table.

To display the SNMP table, enter the following command:

```
Command> show table snmp
```

Monitoring SNMP Alarms

When an interface or modem fails, the SNMP agent traps the error message generated by the failure and sends it to the SNMP Manager.

To view the status of failed modems or interfaces from the command line interface, enter the following command:

```
Command> show alarm
```

The output of this command lists alarm messages and associated alarm identification numbers. For details about a specific alarm, enter the following command:

```
Command> show alarm [alarm-id]
```

To clear alarms from the SNMP alarm table, enter the following command:

```
Command> clear alarm alarm-id|all
```

Refer to the *PortMaster Command Line Reference* for more information.

Displaying the Routing Table

Use the following command to display the IP routing table entries:

```
Command> show routes [String|Prefix/NM]
```

You can replace *String* with **ospf** or **bgp** to display only OSPF or BGP routes. Replacing *Prefix/NM* with an IP address prefix and netmask displays only routes to that destination. Enter the IP address prefix in dotted decimal format and the netmask as a number from 1 to 32, preceded by a slash—for example, /24. The netmask indicates the number of high-order bits in the IP prefix.

To display the IPX routing table entries, enter the following command:

Command> **show ipxroutes**

The routes appear in the following order:

1. Default route
2. Host routes
3. Network routes
4. Expired routes that are no longer being advertised

Setting Static Routes

Static routes provide routing information unavailable from the Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, or Border Gateway Protocol (BGP). RIP, OSPF, or BGP might not be running for one of the following two reasons.

- Network administrators choose not to run RIP, OSPF, or BGP.
- Hosts connected to the PortMaster do not support RIP, OSPF, or BGP.

Separate static routes tables are maintained for IP and for IPX, which you display with the **show routes** and **show ipxroutes** commands.

You construct a static route table manually on a PortMaster by adding and deleting static routes as described in the following sections. Refer to the *PortMaster Routing Guide* for information about routing and static routes.

Adding and Deleting a Static Route for IP

A static route for IP contains the following items:

- **Destination**—The IP address prefix of the host or the number of the IPX network to which the PortMaster will be routing.
- **Netmask** —The static netmask in use at the destination. See “Modifying the Static Netmask Table” on page 3-26 for more information about netmasks.

- **Gateway**—The address of a locally attached router where packets are sent for forwarding to the destination.
- **Metric**—The number of routers (or hops) a packet must cross to reach its destination. The metric represents the cost of sending the packet through the gateway to the specified destination.



Note – Never set the gateway for the PortMaster to an address on the same PortMaster; the gateway must be on another router.

Use the following commands to add a static route for IP:

```
Command> add route Ipaddress[/NM] Ipaddress(gw) Metric
Command> save all
```

Use the following commands to delete a static route for IP:

```
Command> delete route Ipaddress[/NM] Ipaddress(gw)
Command> save all
```

You can delete only static routes.

Adding and Deleting a Static Route for IPX

A static route for IPX contains the following items:

- **Destination**—The number of the IPX network to which the PortMaster will be routing.
- **Gateway**—The address of a locally attached router where packets are sent for forwarding to the destination.

For IPX networks, the gateway address consists of 8 hexadecimal digits for the network address, a colon (:) and the node address of the gateway router expressed as 12 hexadecimal digits—for example, 00000002:A0B1C2D3E4F5.

The IPX node address is usually the media access control (MAC) address on a PortMaster.

- **Metric**—The number of routers (or hops) a packet must cross to reach its destination. The metric represents the cost of sending the packet through the gateway to the specified destination.

- **Ticks**—The time required to send the packet to its destination. Ticks are measured in 50ms increments. The ticks metric is used in addition to the hops metric only on IPX networks.



Note – Never set the gateway for the PortMaster to an address on the same PortMaster; the gateway must be on another router.

Use the following commands to add a static route for IPX:

```
Command> add route Ipxnetwork Ipxaddress Metric Ticks  
Command> save all
```

Use the following commands to delete a static route for IPX:

```
Command> delete route Ipxnetwork Ipxaddress  
Command> save all
```

Use the following command to set a static default route for all IPX packets not routed by a more specific route:

```
Command> set ipxgateway Network|Node Metric
```



Note – You can delete only static routes.

Modifying the Static Netmask Table

The netmask table is provided to allow routes advertised by RIP to remain uncollapsed on network boundaries in cases where you want to break a network into noncontiguous subnets. The PortMaster normally collapses routes on network boundaries as described in RFC 1058. However, in certain circumstances where you do not want to collapse routes, the netmask table is available.



Note – Do not use the static netmask table unless you thoroughly understand and need its function. In most circumstances its use is *not* necessary. Very large routing updates can result from too much use of the netmask table, adversely affecting performance. In most cases it is easier to use OSPF instead of using the netmask table and RIP. Lucent strongly recommends you use OSPF if you require noncontiguous subnets or variable-length subnet masks (VLSMs).

For example, suppose the address of Ether0 is 172.16.1.1 with a 255.255.255.0 subnet mask (a class B address subnetted on 24 bits) and the destination of ptp1 is 192.168.9.65 with a 255.255.255.240 subnet mask (a class C address subnetted on 28 bits). If routing broadcast is on, the PortMaster routing broadcast on Ether0 claims a route to the entire 192.168.9.0 network. Additionally, the broadcast on ptp1 claims a route to 172.16.0.0.

Sometimes, however, you want the PortMaster to collapse routes to some bit boundary, other than the network boundary. In this case, you can use the static netmask table. However, RIP supports only host and network routes, because it has no provision to include a netmask. Therefore, if you set a static netmask in the netmask table, the PortMaster collapses the route to that boundary instead, and broadcasts a host route with that value. Other PortMaster routers with the same static netmask table entry convert the host route back into a subnet route when they receive the RIP packet.

This work-around works only if all the products involved are from PortMaster products, with the following two exceptions:

- If you use a netmask table entry of 255.255.255.255. In this case, the routes broadcast as host routes really are host routes, so non-PortMaster routers can use them. Keep in mind that not all routers accept host routes.
- If the non-PortMaster router can convert host routes into subnet routes through some mechanism of its own.

Uses for Static Netmasks

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

The next most common use for the static netmask table is to allow dial-in users to use specified IP addresses across multiple PortMasters in situations where assigned IP addresses are not sufficient. This use can result in very large routing tables and is not recommended except where no other alternative is possible.

The netmask table can be accessed only through the command line interface. To add a static netmask, use the **add netmask** command. To delete a static netmask, use the **delete netmask** command. The **show table netmask** command shows both dynamic netmasks and static netmasks, marking them accordingly.



Note – Static routes use the netmask table entries that are in effect when the routes are added. If the netmask table is changed, the static route must be deleted from the route table and added again.

Example of Applying Static Netmasks

Note – Lucent recommends that you use OSPF in this circumstance instead of static routes.

This static netmask example assumes the following:

- You have anywhere between 8 and 250 PortMaster routers.
- You assign all the user addresses from the dynamic address assignment pools on the PortMaster routers.
- You are using 27-bit subnets of these three class C networks 192.168.207.0, 192.168.208.0, and 192.168.209.0.
- You are using the 192.168.206.0 network for your Ethernet.
- All PortMaster routers involved are running ComOS 3.1.2 or later.
- You do not use proxy ARP. Instead, you use your 192.168.206.0 network for the Ethernet, and divide your other networks up among the PortMaster routers.
- Each network provides 30 addresses for the assigned pool of each PortMaster.

To create the subnets defined in this example, enter the following commands on all the PortMaster routers:

```
Command> set Ether0 address 192.168.206.X (for some value of X)
Command> set gateway 192.168.206.Y (where Y points at your gateway)
Command> add netmask 192.168.207.0 255.255.255.224
Command> add netmask 192.168.207.0 255.255.255.224
Command> add netmask 192.168.207.0 255.255.255.224
Command> set Ether0 rip on
Command> save all
```

The netmask table collapses routes on the boundaries specified. As a result, if one PortMaster has an assigned pool starting at 192.168.207.33, it broadcasts a host route to 192.168.207.32 instead of broadcasting a route to the 192.168.207.0 network. The other PortMaster routers consult their own netmask tables and convert that route back into a subnet route to 192.168.207.33 through 192.168.207.32.

If your gateway on the Ethernet is not a PortMaster product, the netmask table is not supported. However, you can set a static route on the gateway for each of the three destination networks for your assigned pools (192.168.207.0, 192.168.208.0, and 192.168.209.0), pointing at one of the PortMaster routers. The identified PortMaster then forwards packets to the proper PortMaster.

If you are using an IRX running ComOS 3.2R or later as your gateway, you can configure the netmask table on the router also. This allows your PortMaster to listen to RIP messages from the other PortMaster routers and route directly to each of them.

Enabling NetBIOS Broadcast Packet Propagation

NetBIOS is a programmable entry into the network that enables systems to communicate over multiple media. NetBIOS over IPX uses type 20 broadcast packets propagated to all networks to get and forward information about the named nodes on the network.

NetBIOS uses a broadcast mechanism to get this information because it does not implement a network layer protocol. Before forwarding the packets, the PortMaster performs loop detection as described by the IPX Router Specification available from Novell.

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

To turn NetBIOS on or off, use the following command:

```
Command> set netbios on|off
```

Setting Authentication for Dial-In Users

You can configure the PortMaster for three authentication methods, PAP, CHAP, and username/password login.

By default, PAP and CHAP are set to **on**. Dial-in users are asked to authenticate with PAP when PPP is detected. If users refuse, they are asked to authenticate with CHAP.

If you set PAP to **off**, and CHAP to **on**, dial-in users are asked to authenticate with CHAP. PAP authentication is neither requested nor accepted. If you set both PAP and CHAP to **off**, dial-in users must authenticate with a username/password login.

To set PAP authentication, use the following command:

```
Command> set pap on|off
```

To set CHAP authentication, use the following command:

```
Command> set chap on|off
```

Setting Call-Check Authentication

You can enable services without authenticating the user at the point of entry on PortMaster products that support PRI or in-band signaling. To enable the call-check feature in the ComOS, you must first configure call-check user entries on the RADIUS server.

To enable call checking on the PortMaster, use the following command:

```
Command> set call-check on|off
```



Note – The call-check feature is **off** by default.

For more information about enabling RADIUS call checking, refer to the ComOS 3.8 Release Notes.

Setting the ISDN Switch

You can configure the switch provisioning for ISDN PRI and BRI connections to PortMaster ISDN ports. See Chapter 11, “Configuring the PortMaster 3,” for details on PRI connections. See Chapter 12, “Using ISDN BRI,” for details on BRI connections.

This chapter describes how to configure PortMaster Ethernet interfaces and subinterfaces, and includes the following topics:

- “Setting General Ethernet Parameters” on page 4-1
- “Setting IP Parameters” on page 4-3
- “Setting Ethernet IPX Parameters” on page 4-5
- “Configuring Ethernet Subinterfaces” on page 4-7
- “Setting OSPF on the Ethernet Interface” on page 4-8

Before configuring the Ethernet interface, you must make the appropriate Ethernet connection for your needs. Refer to the relevant installation guide for your PortMaster product for information on making the Ethernet connection.

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Setting General Ethernet Parameters

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

This subsection describes the general Ethernet settings that apply to your network regardless of the protocol you use.

Configuring RIP Routing

As described in the *PortMaster Routing Guide*, PortMaster products automatically send and accept route information as RIP messages.

To configure RIP routing, use the following command:

```
Command> set Ether0 rip on|broadcast|listen|off
```



Note – ComOS releases prior to 3.5 use the keyword **routing** instead of the **rip** keyword.

Table 4-1 describes the results of using each keyword.

Table 4-1 Keywords for Configuring RIP Routing

Keyword	Description
on	The PortMaster broadcasts and listens for RIP information from other routers on the local Ethernet. This is the default.
off	The PortMaster neither broadcasts nor listens for RIP information from the local Ethernet.
broadcast	The PortMaster broadcasts RIP information to the local Ethernet.
listen	The PortMaster listens for RIP information from the local Ethernet.

See the *PortMaster Routing Guide* for OSPF and BGP routing configuration instructions.

Applying Filters

Filters enable you to control network traffic. After you have created filters in the filter table, you can apply them to the Ethernet interface as either input or output filters. For more information about filters, see Chapter 9, “Configuring Filters.”

Filters applied to the Ethernet interface take effect immediately. If you change the filter, the change will not take effect until you set the filter on the interface again or you reboot the PortMaster.

Input Filters

When an input filter is used, all traffic coming into the PortMaster on the Ethernet interface is compared to the input filter rules. Only packets permitted by the filter rules are accepted by the PortMaster.

To apply an input filter to the Ethernet interface, use the following command:

```
Command> set Ether0 ifilter Filtername
```

To remove the input filter, omit the filter name when entering the command.

Output Filters

When an output filter is used, all traffic going out of the PortMaster on the Ethernet interface is compared to the output filter rules. Only packets permitted by the filter rules are sent by the PortMaster.



Note – ICMP and UDP packets generated by the PortMaster are never blocked by the output filter.

To apply an output filter to the Ethernet interface, use the following command:

```
Command> set Ether0 ofilter Filtername
```

To remove the output filter, omit the filter name when entering the command.

Setting IP Parameters

PortMaster products support both the IP and IPX protocols. When you select a protocol for the Ethernet interface, you must enter certain values appropriate for the selected protocol.

This section describes the IP commands, keywords, and values that must be entered if you select IP protocol support.

Setting the IP Address

During the PortMaster installation process, you set the IP address for the Ethernet interface.

To change the IP address of the Ethernet interface, use the following command:

```
Command> set Ether0 address Ipaddress
```



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

Setting the Subnet Mask

The default subnet mask is 255.255.255.0. If you have divided your network into subnets, enter the subnet mask that identifies how your network addresses are divided between the network portion and the host portion.

To set the subnet mask, use the following command:

```
Command> set Ether0 netmask Ipmask
```

See Appendix A, “Networking Concepts,” for more information about using subnet masks.

Setting the Broadcast Address

You can define the IP address used as the local broadcast address. The RIP routing protocol uses this address to send information to other hosts on the local Ethernet network. The actual broadcast address is constructed from the IP address of the Ethernet interface and the netmask. The two valid values are **high**, where the host part of the address is all 1s (such as 192.168.1.255) or **low**, where the host part of the address is all 0s (such as 192.168.1.0). The PortMaster default is **low**. The standard for hosts is to broadcast high, but some hosts still use the low broadcast address, including hosts running SunOS 4.x (Solaris 1.x) and earlier.

The broadcast address you set for the Ethernet interface on the PortMaster must match the broadcast address set for other hosts on your local Ethernet segment.

To set the broadcast address, use the following command:

```
Command> set Ether0 broadcast high|low
```

Enabling or Disabling IP Traffic

IP traffic is sent and received through the PortMaster Ethernet interface. IP is enabled by default on PortMaster Ethernet ports. If the setting has been changed, you must enable IP on the Ethernet interface of all PortMaster products attached directly to a local Ethernet. Disable IP traffic on this port only if the PortMaster is not attached to a local Ethernet network.

To enable or disable IP traffic, use the following command:

Command> **set ether0 ip enable|disable**



Note – This command is currently available only on the Ether0 port.

Setting Ethernet IPX Parameters

You must set the following values to send IPX traffic on the Ethernet interface. IPX routing is enabled when routing is enabled.

- Network address
- Protocol
- Frame type

Setting the IPX Network Address

You must identify the IPX network of your local Ethernet segment. An IPX network address is a number entered in hexadecimal format, described in Appendix A, “Networking Concepts.”

To set the IPX network address, use the following command:

Command> **set Ether0 ipxnet Ipxnetwork**



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

Enabling or Disabling IPX Traffic

Ethernet IPX traffic is sent and received through the PortMaster Ethernet interface. You may enable IPX on the Ethernet interface on any PortMaster products attached directly to a local Ethernet. Disable IPX traffic on this port only if the PortMaster is not attached to a local Ethernet network.

To enable or disable IPX traffic, use the following command:

```
Command> set ether0 ipx enable|disable
```



Note – This command is available only on the Ether0 port.

Setting the IPX Frame Type

The IPX frame type must be identified and set to the value used on the local IPX network. The frame type identifies the encapsulation method used on your IPX ports. The IPX protocol can be implemented with one of the four commonly used IPX encapsulation and frame types shown in Table 4-2.

Table 4-2 Novell IPX Encapsulation and Frame Types

IPX Frame Type	Encapsulation
Ethernet_802.2	Consists of a standard 802.3 media access control (MAC) header followed by an 802.2 Logical Link Control (LLC) header. This is the default encapsulation used by Novell NetWare 4.0.
Ethernet_802.2_II	Not commonly used.
Ethernet_802.3	Consists of a standard 802.3 MAC header followed directly by the IPX header with a checksum of FFFF. This is the default encapsulation used by Novell NetWare 3.11.
Ethernet_II	Uses Novell's Ethernet_II and is sometimes used for networks that handle both TCP/IP and IPX traffic.

The encapsulation method and frame type were selected when your IPX network servers were installed. The IPX frame type you set on the PortMaster must match the frame type set for your network. Contact your IPX network administrator for information about the frame type used on your network.

To set the IPX frame type, use the following command—entered on one line:

```
Command> set Ether0 ipxframe  
ethernet_802.2|ethernet_802.2_ii|ethernet_802.3|ethernet_ii
```

Configuring Ethernet Subinterfaces

With the subinterface feature of the ComOS, you can create up to 512 subinterfaces (the total number of interfaces available on a PortMaster) on a single primary Ethernet interface. Because you have the bandwidth of only a single Ethernet interface, however, efficiency begins to degrade significantly when you add more than 8 subinterfaces.

Subinterfacing is essentially the segmenting of a single wire, or port, into multiple IP networks. Instead of subnetting and routing, you can create a subinterface and then set it up as you would a standard Ethernet interface. To avoid routing loops, however, you must be sure not to create two subinterfaces in the same TCP/IP network on the same port. Each Ethernet subinterface must have a unique network.

A drawback to subinterfacing is that it supports static routing only; IPX, RIP, OSPF, packet filtering, and route propagation are not supported on subinterfaces.

You must configure the primary Ethernet interface before adding subinterfaces (see “Setting General Ethernet Parameters” on page 4-1 for details). After you configure the primary Ethernet interface, follow this procedure to add a subinterface.

1. Create a subinterface.

```
Command> add subinterface name
```

This command adds an entry to the subinterface table, which you can then view with the **show subi** command. Remove a subinterface from the subinterface table with the **del subi** command.

2. Associate the subinterface with a physical port.

```
Command> set subinterface name port-name portlabel
```

3. Assign an IP address or and IP address and net mask to the subinterface.

```
Command> set subinterface name Iaddress [/NM] |[Iaddress/NM]
```

You can specify the netmask in the */NM* or dotted decimal format. You can also configure the IP address and netmask separately (see the *PortMaster Command Line Reference* for details).

4. Set the broadcast for the interface.

```
Command> set subinterface name broadcast high|low
```

You can view or modify a subinterface with the **ifconfig** command (see the *PortMaster Command Line Reference*). If you modify the interface with the **ifconfig** command, you must reboot the PortMaster for the changes to take effect.

Setting OSPF on the Ethernet Interface

You can enable or disable Open Shortest Path First (OSPF) routing protocol on an Ethernet interface.

To set OSPF on the interface, use the following command—entered all on one line:

```
Command> set Ether0 ospf on|off [cost Number] [hello-interval Seconds]
[dead-time Seconds]
```

The **on** keyword enables OSPF on the specified Ethernet interface; **off** disables OSPF on that interface.

You can specify the cost of sending a packet on the interface with a link state metric by using the **cost Number** keyword and value. The *Number* metric is a 16-bit number between 1 and 65535; the default is 1.

Routers in OSPF networks continually exchange hello packets with their neighbor routers. You can set the interval that elapses between the transmission of hello packets on the interface by using the **hello-interval Seconds** keyword and value. *Seconds* can range from 10 to 120 seconds; the default is 10 seconds.

If the PortMaster stops receiving hello packets from a neighbor, it treats that router as inactive, or down. You can specify how long the PortMaster waits for hello packets from neighbors by using the **dead-time Seconds** keyword and value. *Seconds* can range from 40 to 1200 seconds; the default is 40 seconds.



Note – You must set the same **cost** value, the same **hello-interval** value, and the same **dead-time** value on all routers attached to a common network.

To enable acceptance of RIP packets on the OSPF network, use the following command:

```
Command> set Ether0 ospf accept-rip on|off
```

See the *PortMaster Routing Guide* for more information about OSPF.

Each asynchronous port can be configured for several different functions, giving the PortMaster configuration more flexibility. However, each port can carry out only one function at a time. For example, if a port receives a dial-in user login request, this port cannot be used for anything else until the current session is terminated. The port is then available for dial-out use or any other purpose specified when the port was configured.

This chapter discusses the following topics:

- “Asynchronous Port Uses” on page 5-1
- “General Asynchronous Port Settings” on page 5-3
- “Configuring a PortMaster for Login Users” on page 5-8
- “Configuring a Port for Access to Shared Devices” on page 5-11
- “Configuring a Port for Network Access” on page 5-15
- “Configuring a Port for a Dedicated Connection” on page 5-20
- “Connecting without TCP/IP Support” on page 5-25

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Asynchronous Port Uses

The following examples describe various uses for asynchronous ports.

Connections between Offices. Office-to-office connections can be achieved with either dial-up asynchronous connections or dial-up synchronous connections, depending on your application. Chapter 15, “Using Office-to-Office Connections,” gives an example of a dial-up asynchronous office-to-office connection. Chapter 12, “Using ISDN BRI,” gives an example of a dial-up synchronous office-to-office connection.

Once a PortMaster is installed in each office and connected to the local Ethernet with an AUI, 10Base2, or 10BaseT connector, one or more asynchronous serial ports can be configured to dial another office or a set of offices when network traffic for the specified location exists. The two most common configurations are a **star** where multiple branch

offices dial into a central hub that routes among them, and a **mesh** where every office can speak to any other office on demand. Intermediate configurations between star and mesh are also possible.

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

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

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

Chapter 16, “Using Internet Connections,” gives an example of an asynchronous continuous dial-out connection to the Internet.

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

Chapter 17, “Providing User Dial-In Access,” gives an example of an asynchronous remote log-in connection.

Dial-In Network Connectivity. A PortMaster asynchronous port can provide PPP or SLIP service to a dial-in user, allowing the user to route TCP/IP traffic across a modem to access the local network or the entire Internet. If the port is running PPP, the user can also route IPX traffic in this way. This configuration is very heavily used by ISPs and by corporations with remote users running client/server applications that require to access central hosts from home, field offices, or on the road.

Chapter 17, “Providing User Dial-In Access,” gives an example of an asynchronous dial-in connection.

Sharing Devices across the Network. PortMaster asynchronous ports can be configured to allow network hosts access to shared devices connected directly to the PortMaster. If the network host is running the PortMaster **in.pmd** daemon, a

connection can be established to a specified port on the PortMaster. Once the connection is established, the connected device such as a printer or modem can be accessed as if it were connected directly to the host.

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

Chapter 18, “Accessing Shared Devices,” gives an example of sharing devices across a network.

General Asynchronous Port Settings

Certain settings must be configured for every asynchronous port, regardless of the port type and configuration you select.

Overriding Certain Port Settings

If you configure a port as a host device, you can specify that the host device can override certain port settings. This feature allows the host running **in.pmd** to alter the active parameters through software control, by using operating system I/O calls (**ioctl** calls in UNIX). The settings that the host can override are speed, parity, databits, and flow control. These settings can be changed by the host using an **ioctl()** system call. All overrides are turned off by default. If you want to allow a host to override a port setting, turn override for the parameter on.

You can override the settings for all asynchronous commands by using the **set all override** command.

To turn override on for a particular parameter, use the following command:

```
Command> set S0|all override xon|rts|speed|parity|databits on|off
```

Setting the Port Speed

Modern modems should be set to run at a fixed rate. To define a fixed rate, lock the data terminal equipment (DTE) rate by setting all three speeds to the same value.

You can set the speed for all the asynchronous ports simultaneously by using the **set all speed** command.

To set the port speed, use the following command—entered on one line:

```
Command> set S0|all speed [1|2|3] Speed
```

You can set *speed* to any of the following standard modem speed settings:

300	1200	4800	19200	57600	115200
600	2400	9600	38400	76800	

Parity Checking

Parity checking is off by default.

Setting Databits

You can set the number of databits per byte for a single asynchronous port or all asynchronous ports. The default (8) is the most common.

You can set the databits for all the asynchronous ports simultaneously by using the **set all databits** command.

To set databits, use the following command:

```
Command> set S0|all databits 5|6|7|8
```

Setting Flow Control

The PortMaster can use either software or hardware flow control to communicate with the attached device to start and stop the flow of data. Because hardware flow control is more reliable, Lucent recommends that you set software flow control to off and hardware flow control to on.

To set software flow control to off, use the following command:

```
Command> set S0|all xon/xoff off
```

To set hardware flow control to on, use the following command:

```
Command> set S0|all rts/cts on
```


Setting the Dial Group

You can create modem pools for dial-out connections by associating ports and dial-out locations with dial groups. Dial groups can be used to reserve ports for dial-out to specific locations, or to differentiate among different types of modems that are compatible with the remote location. Dial groups are numbered 0 to 99. The default dial group is 0.

To assign a port to a dial group, use the following command:

```
Command> set S0 group Group
```

Displaying Extended Port Information

The PortMaster can display port information in brief or extended modes. The default setting is **off**.

To enable or disable extended information for a port, use the following command:

```
Command> set S0 extended on|off
```



Note – This command only affects the display of port information. It does not affect port behavior.

Setting the Login Prompt

You can set a custom login prompt for each port using any valid ASCII characters. The default login prompt is **\$hostname login:.** For example, on a host named **marketing**, the login prompt is **marketing login:.** Double quotation marks and control characters must not be used inside the login prompt.

To set a login prompt for a port, use the following command:

```
Command> set S0 prompt String
```

For example:

```
Command> set s1 prompt marketing
```

Setting the Login Message

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

To set a login message for a port, use the following command:

```
Command> set S0 message String
```

For example:

```
Command> set s1 prompt Welcome to the FTP Server
```

Setting an Optional Access Filter

An access filter can provide additional login security. To enable access security, you must define an access filter as described in Chapter 9, “Configuring Filters.”

Setting Port Security

Port security requires that each username be found in the user table or in the RADIUS database. If port security is on, all users who log in must have their usernames verified before they are allowed to connect to the specified host.

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

To turn security for a port on or off, use the following command:

```
Command> set S0 security on|off
```

Allowing Users to Connect Directly to a Host

With the automatic login feature, you can set up users so that they connect directly to a specified host without receiving a login prompt. When you set *String* to a username with the **set autolog** command, the PortMaster product automatically substitutes that username for the login prompt and starts the host session.

To enable automatic login for a particular user on a particular port, use the following command:

```
Command> set S0 username|autolog String
```

Setting a Port as the Console

You can set any asynchronous port to be the console for administrative functions such as configuring the PortMaster. The **set console** command takes effect immediately. If you use the **save console** command, the port remains the console even after the current session is ended.

To set a port as the console port, use the following command:

```
Command> set console S0
```

Setting the Port Idle Timer

The idle timer is used to control how long the PortMaster waits after activity stops on a port before disconnecting a dial-in connection, and how long the PortMaster should wait for a response to a login, password, or host prompt.

You can set the idle time in seconds or minutes, to any value from 0 to 240. The default setting is 0 minutes.

If set to the special value of 1 second, a dial-in user has 5 minutes to respond to a login, password, or host prompt. If the user does not respond, the port resets, making it available to another user. Setting the idle time to 1 second turns off the idle timer after the user logs in.



Note – The idle time special value of 1 second applies only to asynchronous ports that have modem control turned on with the **set S0 cd on** command. Ports that are in the command state—with an administrator logged on—are not timed out with the special value of 1 second. In ComOS releases earlier than 3.5, the idle time special value is 1 minute.

You can set the idle time of all the ports simultaneously by using the **set all idletime** command.

To enable the idle timer and set a timeout value, use the following command:

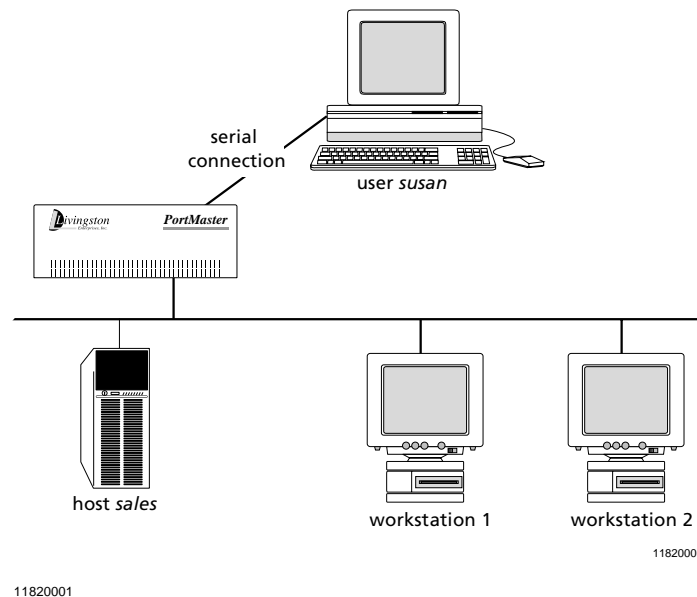
```
Command> set S0 |all idletime Number [minutes|seconds]
```

To disable the idle timer, set it to 0.

Configuring a PortMaster for Login Users

A PortMaster can be configured to allow dial-in users to log in to a specified host. This configuration is called **user login**. In user login mode, the user is prompted for his or her login name after the attached modem answers and completes rate negotiation. Once the user is identified as a valid user through the user table or RADIUS security, a login session is established on the host specified for the asynchronous port.

Figure 5-1 User Login Configuration



In Figure 5-1 the user named *susan* is verified as an authorized user and is connected to the host named *sales*, which has been specified as the host for this port.

To configure a PortMaster for user login, use the following steps. These steps are described in more detail in later sections.

1. Set the port type to login.

```
Command> set S0 login
```

2. Set the login service.

```
Command> set S0 service_login portmaster|rlogin|telnet|netdata [Tport]
```

3. Set the login host.

```
Command> set S0 host 1|2|3|4 default|prompt|Ipaddress
```

4. Specify the terminal type.

```
Command> set S0|all termtype String
```

5. Reset the port and save the settings.

```
Command> reset S0
```

```
Command> save all
```

Setting the Port Type

If you use the **set S0 login** command, the port is set for user login. After being verified or authenticated, a login session is established to the host computer.

You can set the port type to **login** for all asynchronous ports simultaneously by using the **set all** command as shown in the following example:

```
Command> set all login
```

Setting the Login Service

The **login service** specifies how login sessions are established. Table 5-1 describes the four types of login services available.

Table 5-1 Types of Login Service

Login Service	Function
portmaster	PortMaster is the default login service and can be used to access any host that has the PortMaster in.pmd daemon installed. This type of login service is preferred because it makes the PortMaster port operate like a serial port attached to the host. This service is the most cost effective in terms of host resources.
rlogin	The remote login service rlogin uses the rlogin protocol to establish a login session to the specified host. Generally, rlogin is used on mixed UNIX networks where the PortMaster login service is impractical to use.
telnet	Telnet is supported on most TCP/IP hosts. This login service should be selected when the PortMaster and rlogin protocols are not available. The default port number is 23.
netdata	The netdata login service creates a virtual connection between the PortMaster port and another serial port on another PortMaster, or between the PortMaster port and a host. This login service creates a clear channel TCP connection. To connect to another PortMaster port using netdata, you must configure that port as /dev/network with the netdata device service and the same TCP port number. The default netdata port is 6000; however, you can specify any TCP port number between 1 and 65535. This range allows TCP/IP to be used with a hardwired connection using an RS-232 cable. However, some serial communications protocols, such as FAX, might have latency problems with netdata.

Setting the Login Host

You can specify how the login host is determined for the selected port. The three ways to determine the login host are described in Table 5-2.

Table 5-2 Login Host Options

Host Option	Description
default	The host used for this port is the default or alternate host specified in the global settings.
prompt	The user is given the opportunity to enter a hostname or IP address instead of the standard login prompt.
<i>Ipaddress</i>	You set a primary host and up to three alternate hosts for this port. This option allows you to assign specific ports to specific hosts.

Setting the Terminal Type

You can set the terminal type for a port if it has been configured as a user login or twoway port and you have set the login service to PortMaster, rlogin, or Telnet. The terminal type is passed as an environment variable when a connection is established with a host. The terminal type should be compatible with the host you are logging in to.

You can set the terminal type for all asynchronous ports simultaneously using the **set all termttype** command.

Configuring a Port for Access to Shared Devices

One of the functions of a communications server is to provide network users access to shared devices such as printers and modems. The port connected to the printer or modem can provide shared access if it is configured as a host device port. This configuration is also useful when using the UNIX **tip** command and UNIX-to-UNIX Copy Protocol (UUCP) services.

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

You can provide access to host device ports by establishing a pseudo-tty connection to the port from a UNIX host with the PortMaster daemon software installed. In this case, the port operates as a host-controlled device. Figure 5-2 shows a host device configuration using the PortMaster device service and a pseudo-tty connection. This configuration is most commonly used to provide access to shared devices such as printers.

Figure 5-2 Host Device Configuration

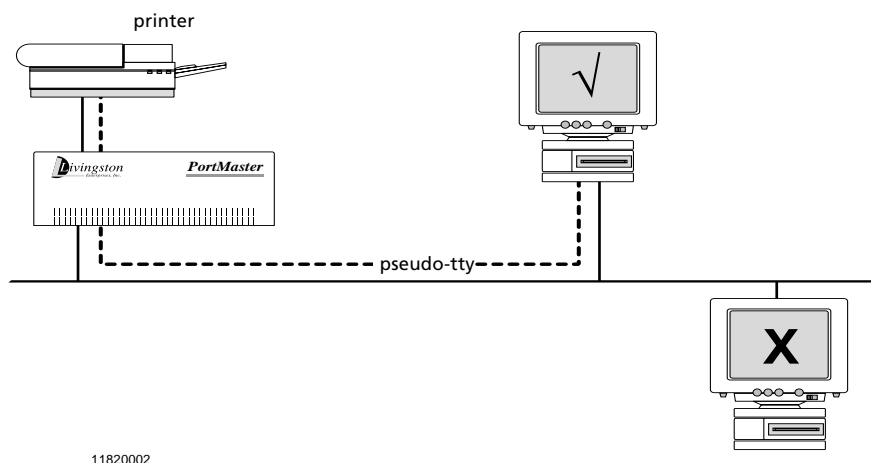
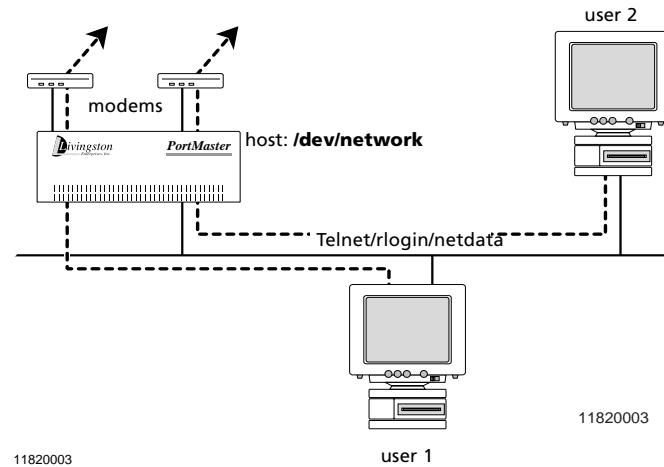


Figure 5-3 shows a host device configuration where the device service is set as rlogin, Telnet, or netdata. In this configuration, the host device name is set as **/dev/network**. This configuration is used in cases where users want to log in remotely via Telnet or rlogin to the shared device before transferring data, such as with a modem.

Figure 5-3 Network Device Configuration



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

To configure a port for access to shared devices, follow these steps:

1. **Set the port type to device.**

```
Command> set S0 device Device
```

2. **Set the device service.**

```
Command> set S0 service_device portmaster|telnet|netdata [Tport]
```

3. **Save the configuration.**

```
Command> save all
```

Setting the Device Service

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

- PortMaster
- Telnet
- Netdata

Selecting the host device port type with the PortMaster device service is sometimes referred to as the host device configuration because the shared device you are connecting to through the PortMaster is known to the host as **/dev/tty****, where the double asterisk (**) is the specific host device identifier.

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

PortMaster Device Service

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

When using the PortMaster device service, you must use a host device name listed in the **/dev** directory of each UNIX host with access to the shared device. The standard device entries have ranges like the following:

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

These tty devices can be dynamically selected for use by a variety of host programs. Most programs start their selection from the beginning of the device list. You should select devices at the end of the list to maximize the possibility of finding a device available.

Telnet Device Service

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

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

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



Note – If you use Telnet to administer the PortMaster, select a TCP port number for your shared device port that is different from your administrative Telnet port.

Netdata Device Service

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

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

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

Configuring a Port for Network Access

You can configure PortMaster asynchronous ports for network dial-in-only access, dial-out-only access, or both dial-in-and-out access (also known as two-way access). You can combine dial-in and dial-out access with the login and device services discussed in the previous sections.

When you configure a port for network dial-in, dial-out, or two-way access, the port becomes available for connections to and from remote sites using modems and the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP).

To configure a port for network access, follow these steps:

1. Set the port to network and choose the access type.

Command> **set SO network dialin|dialout|twoway**

2. Save the configuration.

Command> **save all**

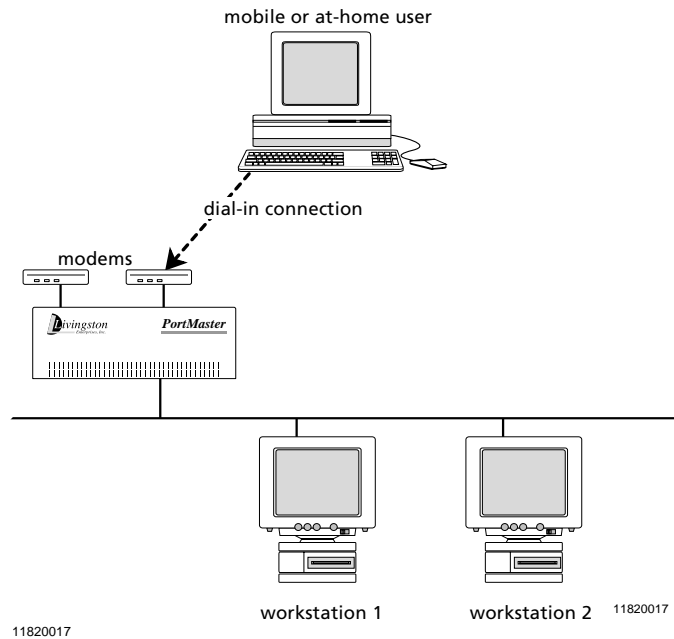


Note – In any of these dial modes (dial-in, dial-out, and two-way) you can also configure the port for other concurrent port types.

Network Dial-In-Only Access

Network dial-in-only access can be set on ports dedicated to answering requests from mobile or home users. In this configuration, the selected port allows an authorized user to connect to the network for mail, file, and other services through SLIP or PPP encapsulation. Figure 5-4 shows how the PortMaster provides network connectivity for remote users.

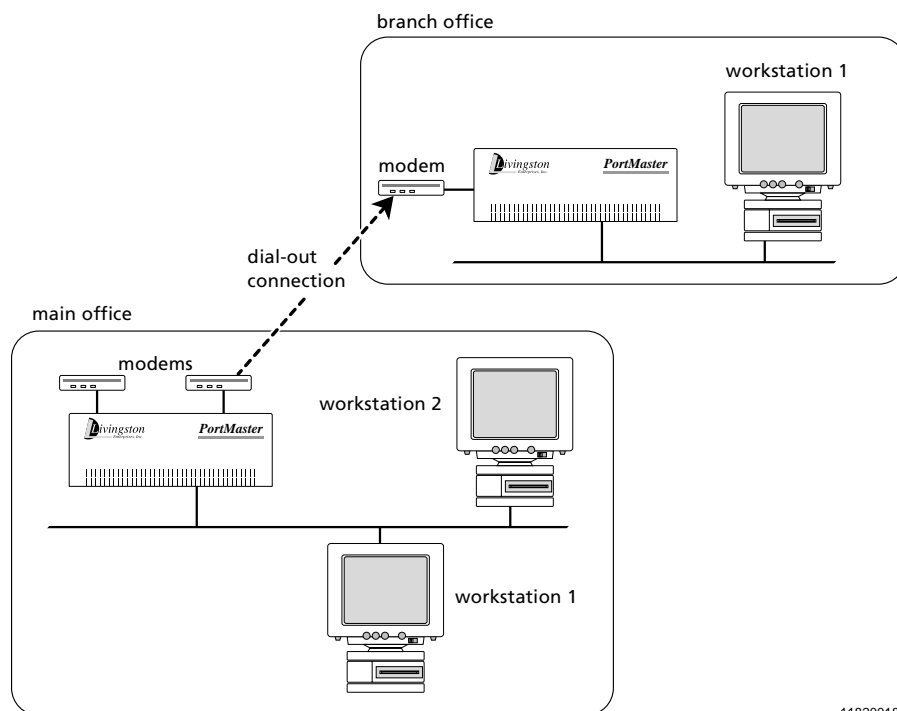
Figure 5-4 Dial-In-Only Port Access



Network Dial-Out-Only Access

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

Figure 5-5 Dial-Out-Only Access



11820018

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

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

To configure two-way access, set the port type for network use and then set the network dial access for two-way use. The specified port operates in user login mode if DCD is detected on pin 8 of the RS-232 connector. Otherwise, it can be accessed as a host device on the computer through **in.pmd** or a Telnet session.

As mentioned in “Network Dial-In-Only Access” on page 5-16, SLIP or PPP is used to define the method for sending IP packets over standard asynchronous lines with a minimum line speed of 1200bps. These encapsulation methods allow you to establish connections on an as-needed basis to reduce telephone costs.

To set a port for network two-way access, use the following commands

```
Command> set S0 network twoway
```

```
Command> save all
```

PPP and SLIP Connections

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

PPP is a method of encapsulating network layer IP protocol information on asynchronous point-to-point links. PPP is described in RFC 1331 and RFC 1332. Lucent's implementation of PPP provides PPP autodetection support for the Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) on serial ports running PPP. ComOS 3.3 and later releases support Multilink PPP as described in RFC 1717 on ISDN BRI ports, and all ports on the PortMaster 3.



Note – Be sure to use the **set S0 rts/cts** command to enable hardware flow control (RTS/CTS) for all SLIP and PPP connections.

PAP and CHAP Authentication

PAP and CHAP authentication occur in the following sequence:

1. A user dials in to a port and starts sending PPP packets.
2. The PortMaster negotiates the authentication protocol with the remote host.
3. If the host refuses PAP authentication, the PortMaster prompts the host to authenticate using CHAP. If the host refuses CHAP authentication, the PortMaster hangs up.

Both the local communications server and the remote device must support CHAP to use this protocol.

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

To disallow PAP authentication and accept only CHAP, enter the following command:

```
Command> set pap off
```

Configuring a Port for a Dedicated Connection

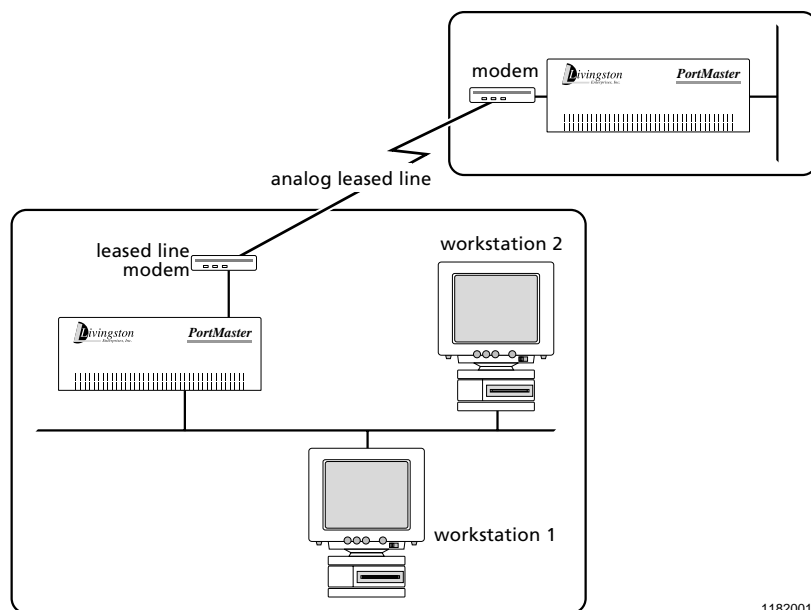
You can configure an asynchronous port for a permanent network connection (also known as a hardwired connection). Hardwired connections require no modem dialing or authentication protocol and are designed for connections to modems configured for leased line service, asynchronous-to-synchronous converters, or Frame Relay asynchronous devices (FRADs). Hardwired connections can use SLIP or PPP with IP and IPX.



Note – This type of configuration creates a continuous uninterrupted connection on this port. If the port is configured for a hardwired connection, it cannot be used for any other purpose.

Figure 5-6 illustrates an example of a hardwired connection.

Figure 5-6 Hardwired Port Configuration



11820019

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

To configure a port for a hardwired connection, follow this procedure:

1. Set the port for network hardwired.

```
Command> set S0 network hardwired
```

2. Set the protocol.

```
Command> set S0 protocol slip|ppp
```

3. Set the maximum transmission unit (MTU) size.

```
Command> set S0 MTU MTU
```

4. Set the destination IP address.

```
Command> set S0 destination Ippaddress [Ipmask]
```

5. Set the IPX network number if you are using IPX.

```
Command> set S0 ipxnet Ipxnetwork
```

6. Enable RIP routing.

```
Command> set S0 rip on|off|broadcast|listen
```

7. Set compression.

```
Command> set S0 compression on|off|stac|vj
```

8. Set the PPP asynchronous map (if required).

```
Command> set S0 map Hex
```

9. Set input and output filters (if using).

```
Command> set S0 ifilter [Filtername]
```

```
Command> set S0 ofilter [Filtername]
```

Omitting the *Filtername* removes any filter previously set on the port.

10. Save the configuration.

```
Command> save all
```

11. Reset the port.

```
Command> reset S0
```

Setting the Protocol

The network protocol for the hardwired port can be set for PPP packet encapsulation or SLIP encapsulation as described in “PPP and SLIP Connections” on page 5-19. If you want to use PPP you have your choice of the following options:

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

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

Setting the MTU Size

The maximum transmission unit (MTU) defines the largest frame or packet that can be sent through this port. If a packet exceeds the specified MTU size, it is automatically fragmented if IP or discarded if IPX. PPP connections can have an MTU set from 100 to 1500 bytes. SLIP connections can have an MTU set from 100 to 1006 bytes. The remote host can negotiate smaller MTUs if necessary.

The MTU is typically set to the maximum allowed for the protocol being used, either 1500 or 1006 bytes. Setting smaller MTU values is useful for interactive (typing) users who send small packets, while larger values are better for multi-line load balance.

Setting the Destination IP Address and Netmask

The IP address or hostname of the machine on the other end of the hardwired connection must be entered to identify the port destination. For PPP, the IP destination can be set to **negotiated** (255.255.255.255). You can optionally specify the netmask of the system on the other end of the hardwired connection.

Setting the IPX Network Number

IPX traffic can be passed through a port if you assign an IPX network number to the hardwired network connection.



Note – The IPX network number must be different from the IPX networks used on the Ethernets on either end of the connection.

Configuring RIP Routing

As described in the *PortMaster Routing Guide*, PortMaster products automatically send and accept route information as part of RIP messages if RIP routing is turned on.

To configure RIP routing for a network hardwired asynchronous port, use the following command:

```
Command> set S0 rip on|broadcast|listen|off
```



Note – ComOS releases prior to 3.5 use **routing** instead of the **rip** keyword.

Table 5-3 describes the results of using each keyword.

Table 5-3 Keywords for Configuring RIP Routing

Keyword	Description
on	The PortMaster broadcasts and listens for RIP information from other routers on this interface. This is the default.
off	The PortMaster neither broadcasts nor listens for RIP information on this interface.
broadcast	The PortMaster broadcasts RIP information on this interface.
listen	The PortMaster listens for RIP information on this interface.

Refer to the *PortMaster Routing Guide* for OSPF and BGP configuration instructions.

Configuring Compression

Compression can increase the performance of interactive TCP sessions over network hardwired asynchronous lines. Lucent implements Van Jacobson TCP/IP header compression and Stac LZS data compression. Compression is on by default.

Compression should not be used with multiline load-balancing, but can be used with Multilink PPP.

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

The PortMaster supports Stac LZS data compression only for PPP connections with bidirectional compression. Stac LZS data compression cannot be used for SLIP connections.

To configure compression, use the following command:

```
Command> set S0|W1 compression on|stac|vj|off
```

Table 5-4 describes the results of using each keyword.

Table 5-4 Keywords for Configuring Compression

Keyword	Description
on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and on leased lines on Office Router products, or Van Jacobson compression only on other PortMaster products. This is the default.
off	Disables compression.
stac	Enables Stac LZS data compression only. Stac LZS compression is supported only on PortMaster 3 and leased lines on Office Router products.
vj	Enables Van Jacobson TCP/IP header compression only.



Note – This command is used only on network hardwired asynchronous ports. Dial-in users must use the user table or RADIUS instead. Dial-out locations must use the location table instead.

To display compression information about a connection, enter the following command:

```
Command> show S0
```

Setting the PPP Asynchronous Map

The PPP protocol supports the replacement of nonprinting ASCII characters found in the datastream. These characters are not sent through the connection but are instead replaced by a special set of characters that the remote system interprets as the original

characters. The PPP asynchronous map is a bitmap of characters that should be replaced. The default PPP asynchronous map is 00000000. If the remote host requires a PPP asynchronous map, the PortMaster accepts the request for the map.

Setting Input and Output Filters

Input and output packet filters can be attached to a network hardwired port. Filters allow you to monitor and restrict network traffic. If an input filter is attached, all incoming packets on that port are evaluated against the rule set for the attached filter. Only packets permitted by the filter are passed through the PortMaster.

If an output filter is attached, packets going to the interface are evaluated against the rule set in the filter and only packets permitted by the filter are sent to the interface.

For more information about filters, see Chapter 9, “Configuring Filters.”

Connecting without TCP/IP Support

You can configure the PortMaster to connect to bulletin board service (BBS) systems or other hosts that have serial ports and allow bidirectional communications, but do not support TCP/IP. This connection requires that you connect the PortMaster to the host with a null modem cable. For more information about null modem cables, refer to your hardware installation guide.

The default setting is on, which sets the DTR drop time to 500 milliseconds (ms). Setting the Data Terminal Ready (DTR) signal to off changes the behavior of the port to better accommodate the connection.

To turn DTR on or off, use the following command:

```
Command> set S0 dtr_idle on|off
```

The following example shows how to configure this feature on port S1:

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



Note – The PortMaster ignores the Data Set Ready (DSR) signal. Some PCs might require DSR high, but they do not tie DSR to DTR.

This chapter describes the steps required to configure a PortMaster synchronous Wide Area Network (WAN) port.

This chapter discusses the following topics:

- “Synchronous Port Uses” on page 6-1
- “Configuring WAN Port Settings” on page 6-4

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Synchronous Port Uses

Synchronous WAN ports are used for high-speed dedicated connections between two remote local area networks (LANs). Once a connection is established between two remote sites, a wide area network (WAN) is achieved. Synchronous WAN connections can be achieved through the use of dedicated leased lines, Frame Relay connections, switched 56Kbps lines, or ISDN lines. Connection rates can range from 9600bps to 2.048Mbps (E1). PortMaster products support any of these connection types using one or more synchronous ports.

All WAN port connections are similar and are represented in Figure 6-1 on page 6-3. For most applications, a dedicated line connects two PortMaster routers, each located on a separate remote network

The following examples describe various uses for synchronous ports.

Routing over Leased Lines. A synchronous port can be used to connect to synchronous leased lines from 9600bps to T1 (1.544Mbps) or E1 (2.048Mbps) for continuous operation. A digital service unit/channel service unit (DSU/CSU) must be attached to the WAN port on the PortMaster. For more information, see Chapter 19, “Using Synchronous Leased Lines.”

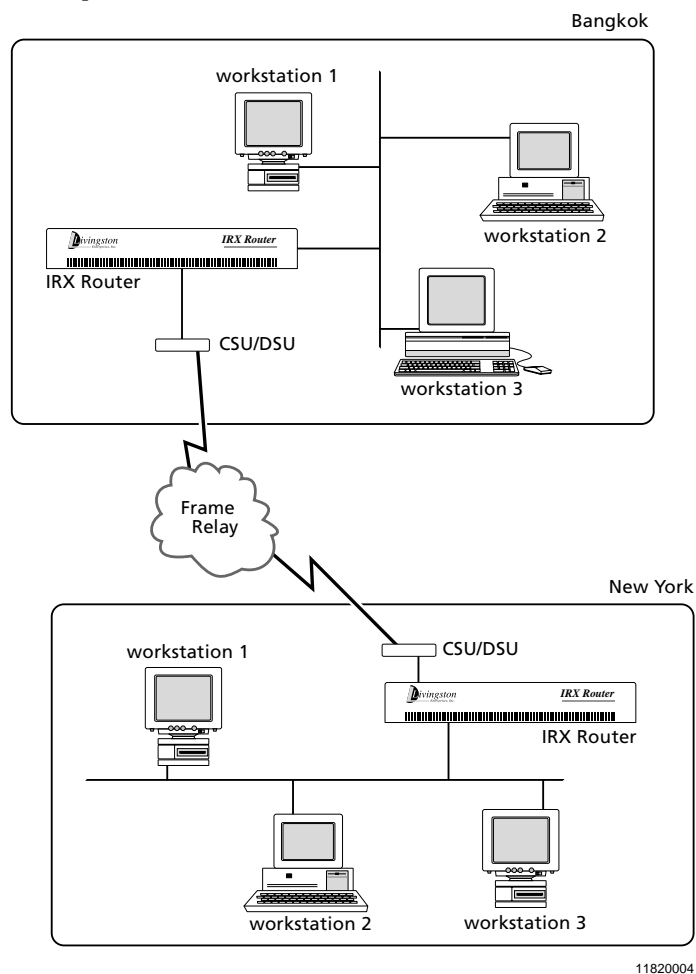
Routing over Frame Relay. Frame Relay provides connectivity using a packet-switched network. Its two advantages over a leased line network are lower cost and the ability to have multiple permanent virtual circuits (PVCs) come into a single physical port. It is especially popular for hub-and-spoke network arrangements. For example, a

dozen field offices with 56Kbps or fractional T1 Frame Relay connections can connect to a central office using a fractional T1 or T1 Frame Relay connection. The central office requires only one CSU/DSU and synchronous port on the router, instead of 12. For more information, see Chapter 13, "Using Frame Relay."

Routing over Switched 56Kbps. Switched 56Kbps can be less expensive than Frame Relay in applications where short bursts of connectivity are required but dial-up modems do not provide enough bandwidth. V.25bis dialing is used to establish a link over a switched network, and the link is brought down after a specified period with no traffic. For more information, see Chapter 14, "Using Synchronous V.25bis Connections."

Routing over ISDN. Integrated Services Digital Network (ISDN) provides fast dial-up connectivity for applications where the expense of a dedicated Frame Relay or leased line connection is not called for by the amount and nature of the traffic. For more information, see Chapter 12, "Using ISDN BRI."

Figure 6-1 Synchronous WAN Connection



Once you have determined the type of synchronous connection to use between your remote locations, the synchronous port on each end of the connection must be configured.

Configuring WAN Port Settings

The WAN port settings described in this section enable you to configure your synchronous port for you needs. “General Synchronous Settings” on page 6-4 includes settings that are available for all connection types. The settings in “Settings for Hardwired Connections” on page 6-7 are available only for network hardwired connections.

General Synchronous Settings

The following settings can be used on synchronous ports configured for all connection types.

Displaying Extended Port Information

The PortMaster can display synchronous port information in brief or extended modes. The default setting is **off**.

To enable or disable extended information for a port, use the following command:

```
Command> set W1 extended on|off
```



Note – This command affects only the display of port information. It does not affect port behavior.

Setting the Port Type and Connection Type

The port type for synchronous ports is always **network**, but you must explicitly set it. You also must specify the kind of connection to use on the synchronous port.

To set the port type and the connection type, use the following command:

```
Command> set W1 network dialin|dialout|twoway|hardwired
```



Note – Some PortMaster products use S1 through S4 for the synchronous ports. Others use W1, or W0 through W59. Refer to your hardware installation guide for information on port numbering

Table 6-1 describes the four connection types available on synchronous ports.

Table 6-1 Port and Network Types

Type	Description
hardwired	Allows you to establish a dedicated network connection between two sites without modem dialing or authentication. In this mode, the port immediately begins running the specified protocol. If the port is set for a hardwired connection, it cannot be used for any other purpose. A hardwired connection must be used for a leased line or Frame Relay connection.
dialin	<p>Allows the port to accept dial-in network connections, for use with switched 56Kbps or ISDN connections. The dial-in user is required to enter a username and password before the connection is established. Authorized users are managed through the user table described in Chapter 7, “Configuring Dial-In Users,” or through RADIUS.</p> <p>PPP users wishing to authenticate with PAP or CHAP can start sending PPP packets. When the packets are received, the PortMaster automatically detects PPP and requests PAP or CHAP authentication.</p>
dialout	Allows dial-out to establish connections with remote locations. Dial-out network destinations are managed through the location table described in Chapter 8, “Configuring Dial-Out Connections.” This network type can be used for ISDN and switched 56Kbps connections.
twoway	Allows the port to accept dial-in users and use dial-out locations. This network type can be used for ISDN and switched 56Kbps connections.

Setting the Port Speed Reference

The port or line speed is set either by the external clock signal on the device to which the PortMaster is connected, or by the carrier. You can record this value as a reference associated with a synchronous port, but it has no effect on PortMaster behavior.

To record the port speed, use the following command:

```
Command> set W1 speed Speed
```

You can substitute any of the following for *Speed*:

9600	19200	56000	64000	115200	1536k	t1	e1
14400	38400	57600	76800	1344k	2048k	t1e	

Setting Modem Control

When modem control is on, the PortMaster uses the condition of the carrier detect (DCD) signal from an attached modem to determine whether the line is in use.

Modem control is off for synchronous connections by default. With modem control set off, the PortMaster assumes the carrier detect line is always asserted. Table 6-2 describes the effects of DCD condition on port behavior.

Table 6-2 Effects of Carrier Detect Condition on Port Behavior

Connection Type	Carrier Detect Asserted	Carrier Detect De-asserted
Hardwired	Port attempts to establish a network connection.	Port is unavailable.
Dialin	PortMaster initiates authentication and displays a login prompt.	Port is unavailable.
Dialout	No effect.	Transition from asserted to de-asserted resets the port.
Twoway	Port attempts to establish a network connection.	Port is available.

Set modem control on only if you want to use the DCD signal from the attached device. In general, set modem control on for network dial-in or dial-out configurations. Modem control is usually off for leased line or Frame Relay connections, but you can use it if the CSU/DSU is configured accordingly.

To set modem control, use the following command:

```
Command> set w1 cd on|off
```

Assigning a Port to a Dial Group

You can create modem pools for dial-out connections by associating ports and dial-out locations with dial groups. Dial groups can be used to reserve ports for dial-out to specific locations, or to differentiate among different types of modems that are compatible with the remote location. Dial groups are numbered 0 to 99. The default dial group is 0.

To assign a port to a dial group, use the following command:

```
Command> set W1 group Group
```

Setting Hangup Control

You can control whether the data terminal ready (DTR) signal on the synchronous port is dropped after a user session terminates. Hangup is set to **on** by default. In this state, DTR is dropped for 500 milliseconds, causing a hangup on the line.

To set the hangup control, use the following command:

```
Command> set W1 hangup on|off
```

The **reset** command always drops the DTR signal.

Setting the Port Idle Timer

The idle timer indicates how long the PortMaster waits after activity stops on a synchronous port before disconnecting a dial-in or dial-out connection.

You can set the idle time in seconds or minutes, to any value from 0 to 240. The default setting is 0 minutes. If the value is set to 2 seconds or a longer interval, the port is reset after having no traffic for the designated time. The idle timer is not reset by RIP, keepalive, or SAP packets. To disable the idle timer, set the value to 0.

To set the idle timer, use the following command:

```
Command> set W1 idle Number [minutes|seconds]
```

Settings for Hardwired Connections

The following settings can be used only when the synchronous port is configured for network hardwired connections.

Setting the Transport Protocol

The transport protocol for synchronous connections must be set for a network hardwired synchronous port. Choose PPP for leased line, switched 56Kbps, and ISDN connections, or Frame Relay for a Frame Relay connection. Additional Frame Relay settings must be configured for Frame Relay connections, described in Chapter 13, “Using Frame Relay.”

To set the transport protocol, use the following command:

```
Command> set W1 protocol ppp|frame
```

Setting the Port IP Address

You can set the local IP address of the network hardwired synchronous port to create a numbered interface.

You can use any IP address. If you set the local address of the WAN port to 0.0.0.0 for PPP, the PortMaster uses the Ether0 address for the end of the serial link. If you set the WAN port address to 0.0.0.0 for a Frame Relay connection, the port is disabled.

To set the IP address, use the following command:

```
Command> set W1 address Ipaddress
```

Setting the Destination IP Address

The destination IP address or hostname of the machine on the other end of the connection is used for leased line connections only. The destination IP address can also be set to 255.255.255.255 for PPP users. This setting allows the PortMaster to learn the IP address of the system on the other end of the connection using PPP IPCP address negotiation.

Do not set a destination IP address for Frame Relay connections. Instead, use the data link connection identifier (DLCI) list to link IP addresses to DLCIs, or use LMI or Annex-D and Inverse ARP to discover Frame Relay addresses dynamically. See Chapter 13, “Using Frame Relay,” for more information.

For network dial-in or dial-out connections, do not set a destination IP address for the port. Instead, you set the destination address in the user table or RADIUS for dial-in, or in the location table for dial-out. See Chapter 7, “Configuring Dial-In Users,” and Chapter 8, “Configuring Dial-Out Connections,” for more information.

To set the destination IP address for a leased-line connection only, use the following command:

```
Command> set W1 destination Ipaddress [Ipmask]
```

Setting the Subnet Mask

The default subnet mask is 255.255.255.0. If you have divided your network into subnets, enter the subnet mask that identifies how your network addresses are divided between the network portion and the host portion. The value of *Ipmask* is dependent upon the size of the IP subnet of which the IP address is a member. This setting is used on network hardwired ports only.

To set the subnet mask, use the following command:

```
Command> set W1 netmask Ipmask
```

See Appendix A, “Networking Concepts,” for more information about using subnet masks.

Setting the IPX Network Address

When using IPX, you must identify an IPX network number of the serial link that is unique from every other IPX number on the network. An IPX network address is entered in hexadecimal format, as described in Appendix A, “Networking Concepts.”



Note – The serial link itself must have an IPX network number that is different from those at either end of the connection.

To set the IPX network address, use the following command:

```
Command> set W1 ipxnet Ipxnetwork
```

Configuring RIP Routing

As described in the *PortMaster Routing Guide*, PortMaster products automatically send and accept route information as RIP messages.

Turn on RIP routing for the port for network hardwired connections only such as leased lines or Frame Relay. Routing is set in the user table for dial-in connections and in the location table for dial-out connections.

To configure RIP routing, use the following command:

```
Command> set W1 rip on|broadcast|listen|off
```



Note – ComOS releases prior to 3.5 used the keyword **routing** instead of the **rip** keyword.

Table 6-3 describes the results of using each keyword.

Table 6-3 Keywords for Configuring RIP Routing

Keyword	Description
on	The PortMaster broadcasts and accepts RIP packets from the system at the other end of the WAN connection. This is the default.
off	The PortMaster neither broadcasts nor listens for RIP information on the interface.
broadcast	The PortMaster broadcasts RIP packets to the system at the other end of the WAN connection.
listen	The PortMaster accepts RIP packets from the device connected to the WAN port.

Refer to the *PortMaster Routing Guide* for OSPF and BGP configuration instructions.

Setting Input and Output Filters

Input and output packet filters can be attached to a synchronous port for network hardwired ports. Filters allow you to monitor and restrict network traffic. If an input filter is attached, all packets received from the interface are evaluated against the rule set for the attached filter. Only packets permitted by the filter are passed through the PortMaster. If an output filter is attached, packets going to the interface are evaluated against the rule set in the filter and only packets permitted by the filter are sent out of the interface.



Note – You must define a filter in the filter table before you can apply it. For more information about filters, see Chapter 9, “Configuring Filters.”

To apply an input filter to a synchronous port, use the following command:

```
Command> set W1 ifilter [Filtername]
```

To apply an output filter to a synchronous port, use the following command:

```
Command> set W1 ofilter [Filtername]
```

You can remove filters from the port by entering the command without a filter name. If a filter is changed, you must reset the port for the change to take effect.

For example, to remove the output filter from a synchronous port, use the following commands:

```
Command> set W1 ofilter
```

```
Command> reset W1
```

```
Command> save all
```



Note – You must reset the port and re-establish the connection for the new settings to take effect.

Setting Compression

You can set Van Jacobson TCP/IP header compression and/or Stac LZS data compression on the port. To set compression, use the following command:

```
Command> set compression on|off|stac|vj
```

Van Jacobson TCP/IP header compression and Stac LZS data compression improve performance on asynchronous lines but can degrade performance on high-speed synchronous lines.

This chapter describes how to configure the PortMaster user table to support dial-in connections. The user table settings define how each dial-in user is authenticated and how dial-in connections are made.

To configure network dial-in connections from other routers, you must define each remote router as a user on the PortMaster.

If you are using RADIUS, you must configure user attributes in individual user files in the RADIUS user database rather than in the PortMaster user table. Refer to the *RADIUS Administrator's Guide* for more information.

This chapter discusses the following topics:

- “Configuring the User Table” on page 7-1
- “User Types” on page 7-3
- “Configuring Settings for Network and Login Users” on page 7-4
- “Configuring Network Users” on page 7-4
- “Configuring Login Users” on page 7-10



Note – Only 100 to 200 users can be configured in the user table and stored in the nonvolatile memory of the PortMaster. Therefore, use RADIUS for user authentication when you must configure multiple PortMaster Communication Servers to handle more than a few dozen users.

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Configuring the User Table

This section describes how to display user information and how to add users to or delete them from the user table.

Displaying User Information

You can display the current users in the user table or the complete configuration information for a specified user.

To display the current users in the user table, for example, enter the following command:

```
Command> show table user
```

Name	Type	Address/Host	Netmask/Service	RIP
jozef	Netuser	negotiated	0000000000	
adele	Login User	default	Telnet	
elena	Netuser	assigned	255.255.255.255	No
taffy	Login User	defaults	PortMaster	
john	Netuser	192.168.7.8	0000000000	No

To display configuration information for a particular user, for example, use the following command:

```
Command> show user elena
```

Username:	elena	Type:	Dial-in Network User
Address:	Assigned	Netmask:	255.255.255.255
Protocol:	PPP	Options:	Quiet, compressed
MTU:	1500	Async Map:	00000000

Adding Users to the User Table

You must add users to the user table before configuring any settings for them. The username is a string of from 1 to 8 printable, nonspace ASCII characters. The optional user password is a string of from 0 to 16 printable ASCII characters. You cannot add users with blank usernames.

To add a login user to the user table, use the following command:

```
Command> add user Username [password Password]
```

To add a network user to the user table, use the following command:

```
Command> add netuser Username [password Password]
```



Note – To add a network user, you must use the **netuser** keyword. Thereafter, you can use either the **netuser** or the **user** keyword to configure settings for the network user. You must always use the **user** keyword when configuring login users.

Deleting Users from the User Table

To delete a user from the user table, use the following command:

```
Command> delete user Username
```

User Types

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

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

PortMaster products allow you to configure two types of users, network users and login users.

Network Users

Network users dial in to an asynchronous serial, synchronous serial, or ISDN port on the PortMaster. A connection is established as soon as the user logs in. A PPP or SLIP (on asynchronous ports) session is started. This type of connection can be used for dial-in users or for other routers that need to access and transfer data from the network. Define this type of user when network packets must be sent through the connection.

Login Users

Login users are allowed to establish PortMaster (**in.pmd**), rlogin, Telnet, or netdata (TCP clear) connections through an asynchronous serial or ISDN port. A connection is established to the specified host as soon as the user logs in. This type of connection is useful for users who need to access an account on a host running TCP/IP.

Configuring Settings for Network and Login Users

The following settings can be configured for either network or login users.

Setting a Password

To set a password for either a login or network user, use the following command:

```
Command> set user Username password Password
```

The password can contain between 0 and 16 printable ASCII characters.

Setting the Idle Timer

The idle timer defines the number of minutes or seconds the line can be idle—in both directions—before the PortMaster disconnects the user. You can set the idle time in seconds or minutes, with any value between 2 and 240. The default setting is 0 minutes. The idle timer is not reset by RIP, keepalive, or SAP packets.

To set the idle timer, use the following command:

```
Command> set user Username idle Number [minutes|seconds]
```

To disable the idle timer, set the time to 0 minutes.

Setting the Session Limit

You can define the maximum length of a session permitted before the PortMaster disconnects the user. The session length can be set to between 0 and 240 minutes.

To set the session limit, use the following command:

```
Command> set user Username session-limit Minutes
```

To disable the session limit, set the time to 0.

Configuring Network Users

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

Setting the Protocol

You can set the network protocol for the network user to PPP or SLIP as described in Chapter 5, “Configuring an Asynchronous Port.” Select a protocol that is compatible with the rest of your network configuration and the user’s capabilities.

To set the network protocol for a network user, use the following command:

```
Command> set user Username protocol slip|ppp
```

If you set a nonzero IP address for a network user using PPP, IP is automatically routed. If you set a nonzero IPX network number for the user, IPX is automatically routed.



Do not set an IPX number of all 0s (zeros) or all Fs for the IPX network address.

Setting the User IP Address

You must define the IP address or hostname of the remote host or router. Table 7-1 describes three different ways that the user IP address can be determined.

Table 7-1 User IP Address Options

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

To set the user IP address for a normal network user, use the following command:

```
Command> set user Username destination assigned|negotiated|Ipaddress
```

Setting the Subnet Mask

Do not set a subnet mask for a network user unless the user is routed to another network from your network. In that case, set the subnet mask to 255.255.255.255.

To set the subnet mask, use the following command:

```
Command> set user Username netmask Ipmask
```

Setting the IPX Network Number

If you are using the IPX protocol for this user, you must assign a unique IPX number to the network connection between the remote user device and the PortMaster. Each user's connection requires a different IPX network number. If you use **fffffffe** as the IPX network number, the PortMaster assigns the user an IPX network number based on an IP address from the IP address pool.



Note – Do not set a value of all 0s (zeros) or all Fs for the IPX network number.

To set the IPX network number, use the following command:

```
Command> set user Username ipxnet Ipxnetwork
```

Configuring RIP Routing

As described in the *PortMaster Routing Guide*, PortMaster products automatically send and accept route information as RIP messages.

To configure RIP routing for a network user, use the following command:

```
Command> set user Username rip on|off|broadcast|listen
```



Note – ComOS releases prior to 3.5 used the keyword **routing** instead of the **rip** keyword.

Table 7-2 describes the results of using each keyword.

Table 7-2 Keywords for Configuring RIP Routing

Keyword	Description
on	The PortMaster broadcasts and listens for RIP information.
off	The PortMaster neither broadcasts nor listens for RIP information from the local Ethernet. This is the default.
broadcast	The PortMaster broadcasts RIP information to the host at the other end of the connection.
listen	The PortMaster listens for RIP information from the host or other router.

Setting the Asynchronous Character Map

The PPP protocol supports the replacement of nonprinting ASCII data in the PPP stream. These characters are not sent through the line, but instead are replaced by a special set of characters that the remote site interprets as the original characters. The PPP asynchronous map is a bit map of characters that should be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. In most environments, the asynchronous map should be set to zero to achieve maximum throughput.

To set the PPP asynchronous character map, use the following command:

```
Command> set user Username map Hex
```

Setting the MTU Size

The maximum transmission unit (MTU) defines the largest frame or packet that can be sent without fragmentation. A packet that exceeds this value is fragmented, if IP, or discarded if IPX. PPP connections can have a maximum MTU of 1520 bytes. SLIP connections can have a maximum MTU of 1006 bytes. PPP can negotiate smaller MTUs when requested by the calling party.

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

To set the MTU for a network user, use the following command:

```
Command> set user Username mtu MTU
```

Setting the Maximum Number of Dial-In Ports

You can define the number of dial-in ports that a user can use on the PortMaster for Multilink V.120, Multilink PPP (only on ISDN), and multiline load-balancing.

If the maximum number of ports is unconfigured, port limits are not imposed and PortMaster's multiline load-balancing, Multilink V.120, and Multilink PPP sessions are allowed. You can also set the dial-in port limit using the RADIUS Port-Limit attribute.

To set the maximum number of dial-in ports, use the following command:

```
Command> set user Username maxports Number
```

The *Number* variable can be set to between 0 and the number of available ports—up to 60.

Setting Compression

Compression of TCP/IP headers can increase the performance of interactive TCP sessions over network hardwired asynchronous lines. Lucent implements Van Jacobson TCP/IP header compression and Stac LZS data compression. Compression is on by default.

Compression cannot be used with multiline load-balancing, but can be used with Multilink PPP.

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

The PortMaster supports Stac LZS data compression only for PPP connections with bidirectional compression. Stac LZS data compression cannot be used for SLIP connections.

To set header compression for a network user, use the following command:

```
Command> set user Username compression on|off
```

Table 7-3 describes the results of using each keyword.

Table 7-3 Keywords for Configuring Compression

on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and on leased lines on Office Router products, or Van Jacobson compression only on other PortMaster products. This is the default.
off	Disables compression.

To find out what type of compression was negotiated for the user, enter the following command:

```
Command> show S0
```

Setting Filters

Input and output packet filters can be applied to each network user. If an input filter is applied to a user, when the user dials in and establishes a connection, all packets received from the user are evaluated against the rule set for the applied filter. Only packets allowed by the filter can pass through the PortMaster. If an output filter is applied to a user, packets going to the user are evaluated against the rule set for the applied filter. Only packets allowed by the filter are sent out of the PortMaster to the user. If either filter is changed while a user is logged on, the change will not take effect until the user disconnects and logs in again.



Note – You must define a filter in the filter table before you can apply it. For more information about filters, see Chapter 9, “Configuring Filters.”

To apply an input filter for a network user, use the following command:

```
Command> set user Username ifilter [Filtername]
```

To apply an output filter for a network user, use the following command:

```
Command> set user Username ofilter [Filtername]
```

Omitting the *Filtername* removes any filter previously set on the port.



Note – Filters will be applied to the user the next time the user dials in.

Specifying a Callback Location

You can configure the user for callback connections to enhance network security or to simplify telephone charges. When a network user logs in, the PortMaster disconnects the user and then calls back to the location specified for that user. The location is stored in the location table. The PortMaster always calls back using the same port on which the user called in. Network users have PPP or SLIP sessions started for them, as defined in the user table.

To specify the callback location for a network user, use the following command:

```
Command> set user Username dialback Locname | none
```

To disable callback connections for the user, use the **none** keyword.

For more information about configuring locations, refer to Chapter 8, “Configuring Dial-Out Locations.”

Configuring Login Users

Login users establish connections with hosts using one of the login services—dial-in, dial-out, or two-way—described in Chapter 5, “Configuring an Asynchronous Port.”

Setting the Login Host

You must define the host to which the user is connected. The login host can be defined in one of three ways. Table 7-4 shows the login host options.

To set the login host for a login user, use the following command:

```
Command> set user Username host default|prompt|Ipaddress
```

Table 7-4 Login Host Options

Host Option	Description
default	This option allows the user to log in to the default or alternate host specified for this PortMaster. You can specify the default host with the set host command shown on page 17-5.
prompt	This option allows the user to log in to a host by IP address or name at the time the login session is established.
Ipaddress	<p>This option allows the user to connect only to the host specifically named. A valid hostname or IP address must be entered.</p> <p>This configuration is used when you want to allow a user to access a specific host. For example, this configuration can be used to allow the user <i>carmela</i> to always be connected with the host <i>sales</i>.</p>

Applying an Optional Access Filter

An access filter is an input filter that restricts which hosts users can log in to. Access filters work as follows:

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

To apply an access filter to a login user, use the following command:

```
Command> set user Username ifilter [Filtername]
```



Note – You must define a filter in the filter table before you can apply it. For more information about filters, see Chapter 9, “Configuring Filters.”

Setting the Login Service Type

All login users must have an associated login service that determines the nature of their connection with the host.

The **login service** specifies how login sessions are established. Four types of login service are available as described in Table 7-5.

Table 7-5 Types of Login Service

Login Service	Function
portmaster	PortMaster is the default login service and can be used to access any host that has the PortMaster in.pmd daemon installed. This type of login service is preferred because it makes the PortMaster port operate like a serial port attached to the host. This service is the most cost-effective in terms of host resources.
rlogin	The remote login service rlogin uses the rlogin protocol to establish a login session to the specified host. Generally, rlogin is used on mixed UNIX networks where the PortMaster login service is impractical to use.
telnet	Telnet is supported on most TCP/IP hosts. This login service should be selected when the PortMaster and rlogin protocols are not available. The default port number is 23, but you can enter another number.

Table 7-5 Types of Login Service (Continued)

Login Service	Function
netdata	<p>The netdata login service creates a virtual connection between the PortMaster port and another serial port on another PortMaster, or between the PortMaster port and a host. This login service creates a clear-channel TCP connection. To connect to another PortMaster port using netdata, you must configure that port as /dev/network with the netdata device service and the same TCP port number.</p> <p>The default netdata port is 6000; however, you can specify any TCP port number between 1 and 65535. This range allows TCP/IP to be used with a hardwired connection using an RS232 cable. However, some serial communications protocols, such as FAX, might have potential latency problems.</p>

To set the login service type for a login user, use the following command:

```
Command> set user Username service portmaster|rlogin|telnet|netdata [Tport]
```

Specifying a Callback Telephone Number

You can configure the login user for callback connections to enhance network security or to simplify telephone charges. When a user logs in, the PortMaster disconnects the user and then dials out to the telephone number specified for that user. The user is reconnected to the host specified in the user table, via the same port on which the user dialed in.

To enter the callback telephone number for a login user, use the following command:

```
Command> set user Username dialback String|none
```

To disable callback connections for the user, use the **none** keyword.

This chapter discusses how to create locations—settings for dial-out destinations—for dial-out connections.

This chapter discusses the following topics:

- “Configuring the Location Table” on page 8-1
- “Setting Multiline Load Balancing” on page 8-11
- “Setting Filters” on page 8-13
- “Testing Your Location Configuration” on page 8-14

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Configuring the Location Table

A location defines a dial-out destination and the characteristics of the dial-out connection. Locations control dial-out network connections in much the same way the user table controls dial-in network connections.

Locations are stored in the location table. All dial-out locations have the following minimum settings:

- Location name
- Name and password that the local PortMaster uses to authenticate itself to the remote host
- Telephone number of the remote host
- IP address and netmask of the remote host
- Protocol used for the connection
- Dial group that associates the location with a particular dial-out port
- Maximum number of ports

Locations can also optionally have the following settings:

- Connection type (dial-on-demand, continuous, or manual)
- Routing protocol
- IPX network number
- MTU size
- Compression
- Idle timer
- Data-over-voice for ISDN connections
- CHAP authentication
- Asynchronous character map
- Multiline load balancing



Note – The location table is not used for dialing out with the **tip** command or UUCP. For information on these applications, refer to Chapter 18, “Accessing Shared Devices.”

To display the location table, enter the following command:

Command> **show table location**

A location table display looks like the following. The location table entries shown here are examples only. PortMasters have empty locations tables by default.

Location	Destination	Netmask	Group	Maxcon	Type
-----	-----	-----	-----	-----	-----
hq	172.16.1.1	255.255.255.0	1	4	On Demand
sf	192.168.1.21	255.255.255.0	99	1	Manual
sub1	192.168.3.1	255.255.255.0	2	0	Manual
bsp	172.16.1.21	255.255.255.0	99	1	Manual

Creating a Location

You must create a unique dial-out location for each remote host or router you want to access. Location table entries are identified by this unique location name, which can contain up to 12 characters.

To create a location, use the following command:

```
Command> add location Locname
```

Setting the Connection Type

Because the default method of initiating a connection is **manual**, you need to use the **dial** command to cause the PortMaster to manually dial out to a location. You can change the connection type as shown in Table 8-1. If you are changing an existing location's connection type, verify that the connection is not active.

Table 8-1 Dial-Out Connection Types

Connection Type	Description
on_demand	This type of connection is automatically started when packets for the remote location are queued by the PortMaster.
continuous	This type of connection is always active. If the telephone connection is dropped, the PortMaster initiates a new connection with the location after a 30-second waiting period.
manual	This type of connection is started when you request a connection. You can use this configuration to test a connection or for network callback users. This is the default

To configure the connection type, use the following command:

```
Command> set location Locname on_demand|continuous>manual
```

On-Demand

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



Note – When configuring a dial-on-demand location, be careful not to have the on-demand location be the route to the loghost, RADIUS server, RADIUS accounting server, or any host for a port using the PortMaster login or device service, unless you understand the effect of these services upon dial-on-demand.

If routing for a dial-on-demand location is set to **on**, **listen**, or **broadcast**, the PortMaster dials out to that location when it boots, to update routing information. The PortMaster hangs up when the idle timer expires because RIP traffic does not reset the idle timer.

To configure a location to support a dial-on-demand connection, use the following command:

```
Command> set location Locname on_demand
```

Continuous

To establish a continuous dial-out connection, you must set the location type to **continuous**. In this configuration, the PortMaster dials out after it boots and establishes a network connection to the specified location. If the connection is dropped for any reason, the PortMaster dials out again and establishes the connection again after a 30-second wait.

To configure a location to support a continuous connection, use the following command:

```
Command> set location Locname continuous
```

Manual Dial-Out

Use manual dial-out to test the connection or if you want the connection to be established only when you or a network callback user requests. You should test any connection before configuring it as a continuous or on-demand location.

To configure a location to support a manual connection, use the following command:

```
Command> set location Locname manual
```



Note – Disconnect dial-out connections by resetting the port before switching a connection type from **manual** to **on demand**.

Setting the Telephone Number

The telephone number setting is used to dial out to the remote location.

To set the telephone number of the remote location, use the following command:

```
Command> set location Locname telephone String
```

Setting the Username and Password

The username and password are what the PortMaster uses to authenticate itself to the remote host. Note that the username and password you enter here must also be resident on the remote host (in the user table, RADIUS, or other authentication mechanism).

To set the username and password, use the following commands:

```
Command> set location Locname username Username  
Command> set location Locname password Password
```

Setting the Protocol

The network protocol for a dial-out location can be set for PPP packet encapsulation, SLIP encapsulation, or a Frame Relay subinterface. PPP can be used with either or both IP and IPX packet routing. You should select a protocol that is compatible with the remote location.



Note – New location table entries default to PPP.

To set the protocol for a location, use the following command:

```
Command> set location Locname protocol slip|ppp|frame|x75-sync
```

For more information about setting the location protocol to a Frame Relay subinterface, see “Frame Relay Subinterfaces” on page 13-12.

Setting the Destination IP Address

The destination IP address is the IP address expected on the system at the remote end of the dial-out connection.

For PPP connections, you can either specify an IP address or have it negotiated. If you enter 255.255.255.255 (negotiated) for the destination IP address, the PortMaster learns the IP address of the remote system during PPP IPCP negotiation.

For SLIP connections and locations set for on-demand dialing, enter the IP address or a valid hostname of the system at the remote end of the connection.



Note – Assigned addresses are not supported for dial-out locations.

To set the destination IP address for a location, use the following command:

```
Command> set location Locname destination Ipaddress
```

Setting the Destination Netmask

If the host or network on the remote end of the connection requires a netmask, you must define it in the location table.

To set the destination netmask for a location, use the following command:

```
Command> set location Locname netmask Ipmask
```

Setting the IPX Network Number

If you are using the IPX protocol, you must assign a unique IPX network number to the network connection between the remote host and the PortMaster. Enter the IPX network number in the hexadecimal format described in Appendix A, “Networking Concepts.” The number can consist of up to eight characters. The number is used only for the serial link, and must be different from the IPX network numbers used for Ethernets at either end.

To set the IPX network number for a location, use the following command:

```
Command> set location Locname ipxnet Ipxnetwork
```



Note – Do not set a value of all 0s (zeros) or all Fs for the IPX network numbers.

Setting RIP Routing

You can associate RIP routing with locations—for example, a dial on-demand connection where the remote router is defined as a location on the local PortMaster.

As described in the *PortMaster Routing Guide*, PortMaster products automatically send and accept route information as RIP messages.

Refer to the *PortMaster Routing Guide* for OSPF and BGP configuration instructions.

To set RIP routing for a location, use the following command:

```
Command> set location Locname rip on|off|broadcast|listen
```

Table 8-2 describes the results of using each keyword.

Table 8-2 Keywords for Configuring RIP Routing

Keyword	Description
on	The PortMaster broadcasts and listens for RIP packets from this network interface when it is established.
off	The PortMaster neither broadcasts nor listens for RIP packets from this network interface when it is established. This is the default.
broadcast	The PortMaster broadcasts RIP packets to this network interface when it is established.
listen	The PortMaster listens for RIP packets from this network interface when it is established.



Note – ComOS releases prior to 3.5 use **routing** instead of the **rip** keyword.

Setting the Dial Group

Dial groups associate locations with specific dial-out ports. By default, all ports and locations belong to dial group 0 (zero). You can configure locations and ports into dial groups numbered from 0 to 99. Dial group numbers can be used to reserve ports for dial-out to specific locations, or to differentiate among different types of modems that are compatible with the remote location.

The dial group associated with a location works with the dial group specified for each port. For example, you create a dial-out location called *home* and specify that the dial group for *home* is 2. When you configure each port, you can assign the port to a dial group. Only ports assigned to group 2 will be used to dial the location *home*, while other ports will not.

To associate a location with a dial group number, use the following command:

```
Command> set location Locname group Group
```

Setting the MTU Size

The maximum transmission unit (MTU) defines the largest frame or packet that can be sent through this port, without fragmentation. If an IP packet exceeds the specified MTU, it is automatically fragmented. An IPX packet that exceeds the specified MTU is automatically dropped. PPP connections can have a maximum MTU of 1500 bytes. SLIP connections can have a maximum MTU of 1006 bytes. With PPP, the PortMaster can negotiate smaller MTUs when requested during PPP negotiation.

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

To set the MTU for a location, use the following command:

```
Command> set location Locname mtu MTU
```

Configuring Compression

Compression of TCP/IP headers can increase the performance of interactive TCP sessions over network hardwired asynchronous lines. Lucent implements Van Jacobson TCP/IP header compression and Stac LZS data compression. Compression is on by default.

Compression cannot be used with multiline load-balancing, but can be used with Multilink PPP.

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

The PortMaster supports Stac LZS data compression only for PPP connections with bidirectional compression. Stac LZS data compression cannot be used for SLIP connections.

To configure compression for a location, use the following command:

```
Command> set location Locname compression on|off|stac|vj
```

Table 8-3 describes the results of using each keyword.

Table 8-3 Keywords for Configuring Compression

Keyword	Description
on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and on leased lines on Office Router products, or Van Jacobson compression only on other PortMaster products. This is the default.
off	Disables compression.
stac	Enables Stac LZS data compression only. Stac LZS compression is supported only on the PortMaster 3 and on leased lines on Office Router products.
vj	Enables Van Jacobson TCP/IP header compression only.

To display compression information about a location, enter the following command:

```
Command> show S0
```

Setting the Idle Timer

You can set the idle timer for a location with manual or on-demand connections. This timer defines the length of time the line can be idle, with no network traffic in either direction, before the PortMaster disconnects the connection. You can set the idle time in seconds or minutes, to any value from 0 to 240. The default setting is 0 minutes. If the value is set to 2 seconds or a longer interval, the port is reset after having no traffic for the designated time. The idle timer is not reset by RIP, keepalive, or SAP packets. To disable the idle timer, set the value to 0.



Note – Idle timers for dial-in connections are set on each port or for specific users. Idle timers for dial-out connections are set in the location table.

To set the idle time for a location with a manual or on-demand connection, use the following command:

```
Command> set location Locname idletime Number [minutes|seconds]
```

Setting Data over Voice

The PortMaster supports data-over-voice for inbound and outbound ISDN connections. The PortMaster automatically accepts inbound voice calls and treats them as data calls. You can force a data-over-voice call on an outbound ISDN connection by setting the capability to **on**.

To turn on the data-over-voice capability for ISDN connections to a location, use the following command:

```
Command> set location Locname voice on|off
```

For more information on ISDN connections, see Chapter 11, “Configuring the PortMaster 3,” and Chapter 12, “Using ISDN BRI.”

Setting CHAP

When you enter a username and password into the location table, they are used as the system identifier and MD5 secret for CHAP authentication. You can turn on outbound CHAP authentication and eliminate the need to use the **sysname** identifier and user table configurations for CHAP, unless the device being dialed also dials in to the PortMaster. The default setting is **off**.

To set CHAP authentication for a location, use the following command:

```
Command> set location Locname chap on|off
```

Setting the Asynchronous Character Map

The PPP protocol supports the replacement of nonprinting ASCII data in the PPP stream. These characters are not sent through the line, but instead are replaced by a special set of characters that the remote site interprets as the original characters. The PPP asynchronous map is a bit map of characters that should be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments should set the asynchronous map to 0 (zero) to achieve maximum throughput.

To set the PPP asynchronous map for a location, use the following command:

```
Command> set location Locname map Hex
```

Setting Multiline Load Balancing

You can set several ports to connect to a single location to distribute heavy traffic loads. This capability is called multiline load balancing. You can define a threshold known as a high-water mark for a location. The high-water mark triggers the PortMaster to bring up an additional connection to the location when the amount of data specified by the high-water mark is queued. The PortMaster examines the queue several times a minute to determine if the high-water mark has been reached.

Load balancing is useful for on-demand routing because additional ports for the location are added as the load exceeds what can be handled by one port. When the ports are idle for the time specified by the **set location idletime** command (see “Setting the Idle Timer” on page 8-10), all ports used for that connection are timed out simultaneously.

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

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

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

Setting the Maximum Number of Dial-Out Ports

To configure load balancing, you must define the number of dial-out ports that can be used to dial and establish a connection with this location. This setting creates a pool of ports that can be used at the same time to establish a connection with this location.

If the maximum number of ports is set to 0, no connection with this location is established. If the maximum number of ports is set to any number greater than one, the high-water mark is used to determine when additional connections are established with this location.

When more than one line is open to a given location, the PortMaster balances the load across each line. When the ports are idle for the time specified by the **set location idletime** command (see “Setting the Idle Timer” on page 8-10), all ports used for that connection are timed out simultaneously.

To set the maximum number of dial-out ports for a location, use the following command:

```
Command> set location Locname maxports Number
```

Setting Bandwidth-on-Demand

Bandwidth-on-demand determines when an additional line to this location should be established. The PortMaster uses the high-water mark setting to configure bandwidth-on-demand

The high-water mark specifies the number of bytes of network traffic that must be queued before the PortMaster opens an additional connection. The PortMaster examines the queue several times a minute to determine if the high-water mark has been reached.

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

This value is used only when the maximum number of ports is greater than one. The default high-water mark is zero.

To set the high-water mark in bytes for a location, use the following command:

```
Command> set location Locname high_water Number
```

Setting Filters

You can attach input and output filters to each location. Filters must be defined in the filter table before they can be added to the location table. For more information about filters, see Chapter 9, “Configuring Filters.” When a filter is changed, all ports in use by the location must be reset to have the changes take effect.



Note – If a matching filter name is not found in the filter table, this command is not effective and all traffic is permitted.

Input Filters

Input filters cause all packets received from the interface to be evaluated against the filter rule set. Only packets allowed by the filter are accepted.

To set an input filter for a location, use the following command:

```
Command> set location Locname ifilter Filtername
```

Output Filters

Output filters cause all packets going out to the interface to be evaluated against the filter rule set. Only packets allowed by the filter are passed out to the interface.

To set an output filter for a location, use the following command:

```
Command> set location Locname ofilter Filtername
```

Testing Your Location Configuration

When you are configuring a location, you can set a manual connection for the location so that you can test the configuration before resetting the connection to on-demand or continuous. To test the configuration, you must initiate a connection with the remote location by using the **dial** command from the command line.

To display the chat script (if you are using one) during dialing, use the optional **-x** keyword. You can watch the connection process to ensure that location-specific settings are configured correctly. This keyword also resets some debugging values previously set with **set debug**.

When your location is configured correctly, change the connection type from manual to continuous or on-demand.

To test your configuration, use the following command:

```
Command> dial Locname [-x]
```

This chapter describes how to configure input and output packet filters. IP, IPX, and Service Advertising Protocol (SAP) rules are reviewed, and filter examples are given. You can also use the ChoiceNet application to filter IP packets by lists of sites rather than by individual IP addresses. For more information on ChoiceNet, see the *ChoiceNet Administrator's Guide*.

This chapter discusses the following topics:

- “Overview of PortMaster Filtering” on page 9-1
- “Creating Filters” on page 9-5
- “Displaying Filters” on page 9-8
- “Deleting Filters” on page 9-8
- “Example Filters” on page 9-9
- “Restricting User Access” on page 9-15

Each topic in this chapter includes examples of filters used to accomplish the goal described.

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of PortMaster Filtering

Packet filters can increase security and decrease traffic on your network. Filters can be used to limit certain kinds of internetwork communications by permitting or denying the passage of packets through network interfaces. By creating appropriate filters, you can control access to specific hosts, networks, and network services.

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

You use Ethernet filters to constrain the types of packets allowed to pass through the local Ethernet port, and you can set filters on asynchronous ports configured for hardwired operation when security with another network is an issue.

The packet filtering process analyzes the header information contained in each packet sent or received through a network interface. The header information is evaluated against a set of rules that either allow the packet to pass through the interface or cause the packet to be discarded.

A maximum of 256 filter rules per filter is allowed for the PortMaster 3 and IRX. For other PortMaster products, the maximum number of filter rules allowed is 100. The PortMaster generates an error message when the number of filter rules exceeds the limit.

If a packet is discarded by a filter, an appropriate “ICMP unreachable” message is returned to the source address. This message provides immediate feedback to the user attempting the unauthorized access. Packets permitted or denied can optionally be logged to a host.

Filters can also be used for packet selection—for example, you can use a packet trace filter to do troubleshooting. The packets permitted by the **ptrace** filter are displayed, while packets not permitted by the filter are not displayed. For more information about the **ptrace** facility, see the *PortMaster Troubleshooting Guide*.

Filter Options

Table 9-1 shows different filter options.

Table 9-1 Filter Options

Option	Description
Restricting packet traffic	Each user, location entry, and network hardwired port can be assigned both an input packet filter and an output packet filter. Having both input and output filters can decrease the number of rules needed and can provide better tuning of your security policy.

Table 9-1 Filter Options (Continued)

Option	Description
Restricting access based on source and destination address	You can create filters that evaluate both the source and destination addresses of a packet against a rule list. The number of significant bits used in IP address comparisons can be set, allowing filtering by host, subnet, network number, or group of hosts whose addresses are within a given bit-aligned boundary.
Restricting access to particular protocols	Packets of certain protocols can be permitted or denied by a filter, including IPX, SAP, TCP, UDP, and ICMP packets.
Restricting access to network services	You can create filters that use the source and destination port numbers to control access to certain network services. The evaluation can be based upon whether the port number is less than, equal to, or greater than a specified value.
Restricting access based on TCP status	You can create filters that use the status of TCP connections as part of the rule set. This feature can allow network users to open connections to external networks without allowing external users access to the local network.

Filter Organization

Filters are stored in a filter table in the PortMaster nonvolatile configuration memory. Filters can be created or modified at any time, and the changes are not applied to an active use of the filter. Filter names must be between 1 and 15 characters.

Each packet filter can contain three sets of rules: IP, IPX, and SAP. Within each set, the rules are numbered starting at one. Newly created packet filters contain zero rules, or an empty set of rules.

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

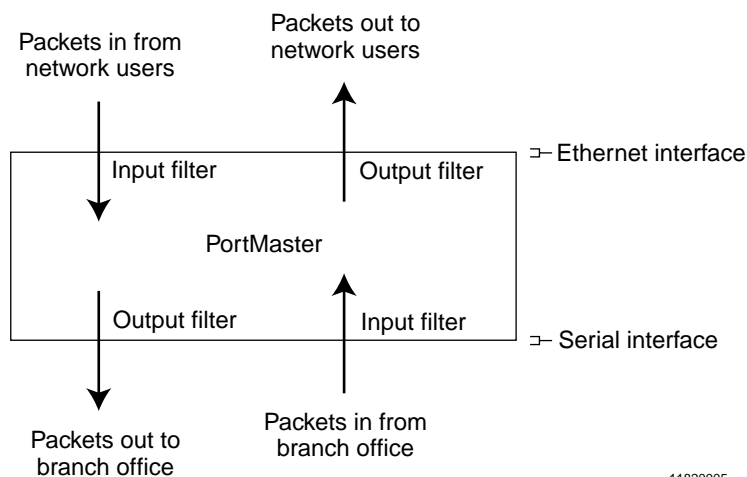
A maximum of 256 filter rules per filter is allowed for the PortMaster 3 and IRX. For other PortMaster products, the maximum number of filter rules allowed is 100. The PortMaster generates an error message when the number of filter rules exceeds the limit.

How Filters Work

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

Input and output are defined relative to the PortMaster interface. As shown in Figure 9-1, an input filter is used on packets entering the PortMaster and an output filter is used on packets exiting the PortMaster.

Figure 9-1 Input and Output Filters



11820005

All packets entering a PortMaster through an interface with an input filter are evaluated against the rules in the filter. As soon as a packet matches a rule, the action specified by that rule is taken. If no rules match the specific packet, the packet is denied and is discarded. Whenever an IP packet is discarded, the PortMaster generates an "ICMP Host Unreachable" message back to the originator.

For interfaces with output filters attached, all packets exiting the interface are evaluated against the filter rules and only those packets permitted by the filter are allowed to exit the interface.

Creating Filters

You construct a filter by creating the filter and then adding rules that permit or deny certain types of packets. A maximum of 256 filter rules per filter is allowed for the PortMaster 3 and IRX. For other PortMaster products, the maximum number of filter rules allowed is 100. The PortMaster generates an error message when the number of filter rules exceeds the limit.

Packets are evaluated in the same order as the rules are listed. Therefore, the rules representing the highest security concern should be specified early in the list of rules, followed by a rule limiting the volume of traffic.

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

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

You can attach filters for incoming packets, or for outgoing packets or for both. It is usually more effective to filter incoming packets so that you can protect the PortMaster itself.

For more detailed instructions on using the filter commands, see the *PortMaster Command Line Reference*.

To create a filter, use the following command:

```
Command> add filter Filtername
```

You must then use the appropriate **set** command to add rules that permit or deny packets. A maximum of 256 filter rules per filter is allowed. The PortMaster generates an error message when the number of filter rules exceeds the limit.

See the following sections for instructions:

- “Creating IP Filters” on page 9-6
- “Filtering TCP and UDP Packets” on page 9-7
- “Creating IPX Filters” on page 9-7

Creating IP Filters

You can create a rule that filters IP packets according to their source and destination IP addresses. For more information on the command syntax for creating filters, see the *PortMaster Command Line Reference*.

To create an IP filter rule that filters by address, use the following command—entered on one line:

```
Command> set filter Filtername RuleNumber permit|deny [Ipaddress/NM  
Ipaddress(dest)/NM] [protocol Number] [log] [notify]
```

You can replace **protocol** *Number* with one of the following keywords:

- **esp**—matches packets using Encapsulation Security Payload (ESP) protocol. See RFC 1827 for more information on this protocol.
- **ah**—matches packets using Authentication Header (AH) protocol. See RFC 1826 for more information on this protocol.
- **ipip**—matches packets using the IP Encapsulation within IP (IPIP). See RFC 2003 for more information on this protocol.

If you are using ChoiceNet, you can also replace either the source or destination IP address with the value *=ListName* which specifies a list of sites in the **/etc/choicenet/lists** directory in the ChoiceNet server. The equal sign (=) must immediately precede the value.

Filtering ICMP Packets

Internet Control Message Protocol (ICMP) packets—commonly known as ping packets—report errors and provide other information about IP packet processing. You can filter ICMP packets by source and destination IP address, or by ICMP packet type. Packet types are identified in RFC 1700.

To create an ICMP filter rule, use the following command—entered on one line:

```
Command> set filter Filtername RuleNumber permit|deny [Ipaddress/NM  
Ipaddress(dest)/NM] icmp [type Itype] [log]
```

Filtering TCP and UDP Packets

TCP Packets

You can filter TCP packets by source and destination IP address, or by TCP port number. Appendix B, “TCP and UDP Ports and Services,” lists port numbers commonly used for UDP and TCP port services. For a more complete list, see RFC 1700.

To create a TCP filter rule, use the following command—entered on one line:

```
Command> set filter Filtername RuleNumber permit|deny [Ipaddress/NM  
Ipaddress(dest)/NM] tcp [src eq|lt|gt Tport] [dst eq|lt|gt Tport]  
[established] [log]
```

UDP Packets

You can filter UDP packets by source and destination IP address, or by UDP port number. Appendix B, “TCP and UDP Ports and Services,” lists port numbers commonly used for UDP and TCP port services. For a more complete list, see RFC 1700.

To create a UDP filter rule, use the following command—entered on one line:

```
Command> set filter Filtername RuleNumber permit|deny [Ipaddress/NM  
Ipaddress(dest)/NM] udp [src eq|lt|gt Tport] [dst eq|lt|gt Tport]  
[established] [log]
```

Creating IPX Filters

You can filter IPX packets in the following ways:

- Source and/or destination IPX network number
- Source and/or destination IPX node address
- Source and/or destination IPX socket number

To create an IPX filter rule, use the following command—entered on one line:

```
Command> set ipxfilter Filtername RuleNumber permit|deny [srcnet Ipxnetwork]  
[srchost Ipxnode] [srcsocket eq|gt|lt Ipxsock] [dstnet Ipxnetwork]  
[dsthost Ipxnode] [dstsocket eq|gt|lt Ipxsock]
```

Creating SAP Filters

The Service Advertising Protocol (SAP) is an IPX protocol used over routers and servers that informs network clients of available network services and resources. SAP packets can be filtered only on output. You can filter SAP packets according to the following information about the server that is advertising the service via SAP:

- Name
- IPX network number
- IPX node address
- IPX socket number

To create a SAP filter rule, use the following command—entered on one line:

```
Command> set sapfilter Filtername RuleNumber permit|deny  
[server String][network Ipxnetwork] [host Ipxnode] [socket eg|gt|lt Ipxsock]
```

Displaying Filters

To display the filter table, use the following command:

```
Command> show table filter
```

To display a particular filter, use the following command:

```
Command> show filter Filtername
```

Deleting Filters

To delete a filter, use the following command:

```
Command> delete filter Filtername
```

Example Filters

Because filters are very flexible, you must carefully evaluate the types of traffic that a specific filter permits or denies through an interface before attaching the filter. If possible, a filter should be tested from both sides of the filtering interface to verify that the filter is operating as you intended. Using the **log** keyword to log packets that match a rule to the loghost is useful when you are testing and refining IP filters.

Some of the following examples use the 192.168.1.0 network as the public network. You should substitute the number of your network or subnetwork if you use these examples.



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

Simple Filter

A simple filter can consist of the following rules:

```
Command> set filter simple 1 permit udp dst eq 53
Command> set filter simple 2 permit tcp dst eq 25
Command> set filter simple 3 permit icmp
Command> set filter simple 4 permit 0.0.0.0/0 192.168.1.3/32 tcp dst eq 21
Command> set filter simple 5 permit tcp src eq 20 dst gt 1023
```

Table 9-2 describes, line by line, each rule in the filter.

Table 9-2 Description of Simple Filter

Rule	Description
1.	Permits Domain Name Service (DNS) UDP packets from any host to any host.
2.	Permits SMTP (mail) packets.
3.	Permits ICMP packets.
4.	Permits FTP from any host, but only to the host 192.168.1.3.
5.	Permits FTP data to return to the requesting host. This rule is required to provide a reverse channel for the data portion of FTP.

Input Filter for an Internet Connection

The filter in this example is designed as an input filter for a network hardwired port that connects to the Internet. You can use this filter for a dial-on-demand connection by attaching it to the location entry.

The rules for the filter are set as follows:

```
Command> set filter internet.in 1 deny 192.168.1.0/24 0.0.0.0/0 log
Command> set filter internet.in 2 permit tcp estab
Command> set filter internet.in 3 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 25
Command> set filter internet.in 4 permit 0.0.0.0/0 172.16.0.4/32 tcp dst eq 21
Command> set filter internet.in 5 permit tcp 0.0.0.0/0 192.168.0.5/32 dst eq 80
Command> set filter internet.in 6 permit tcp src eq 20 dst gt 1023
Command> set filter internet.in 7 permit udp dst eq 53
Command> set filter internet.in 8 permit tcp dst eq 53
Command> set filter internet.in 9 permit icmp
```

Table 9-3 describes, line by line, each rule in the filter.

Table 9-3 Description of Internet Filter

Rule	Description
1.	Denies any incoming packets from the Internet claiming to be from—or spoofing —your own network (192.168.1.0). This rule blocks IP spoofing attacks. This rule also logs the header information in the spoofing packets to syslog.
2.	Permits already established TCP connections that originated from your network—packets with the ACK bit set.
3.	Permits SMTP connections to 10.0.0.3 (the mail server).
4.	Permits FTP connections to host 172.16.0.4.
5.	Permits Hypertext Transfer Protocol (HTTP) access to host 192.168.0.5.
6.	Permits an FTP data channel.
7.	Permits DNS.
8.	Permits DNS zone transfers. (You can write this rule to allow only connections to your name servers.)

Table 9-3 Description of Internet Filter (Continued)

Rule	Description
9.	Permits ICMP packets.

Input and Output Filters for FTP Packets

Filters can be used to either permit or deny File Transfer Protocol (FTP) packets. You must understand how this protocol works before you develop FTP filters.

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

Consult *Firewalls and Internet Security: Repelling the Wily Hacker* by Cheswick and Bellovin and *Building Internet Firewalls* by Chapman and Zwicky for information on FTP proxies and passive FTP.

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

In the following examples, 172.16.0.2 is the address of your FTP server and 192.168.0.1 is the address of the host from which you allow outgoing FTP.



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

The rules for the input filter are as follows:

```
Command> set filter internet.in 1 permit 0.0.0.0/0 192.168.0.1/32 tcp src eq
20 dst gt 1023
Command> set filter internet.in 2 permit 0.0.0.0/0 192.168.0.1/32 tcp src eq
21 estab
Command> set filter internet.in 3 permit 0.0.0.0/0 172.16.0.2/32 tcp dst eq 21
Command> set filter internet.in 4 permit 0.0.0.0/0 172.16.0.2/32 tcp src gt
1023 dst eq 20 estab
```

The rules for the output filter are as follows:

```
Command> set filter internet.out 1 permit 192.168.0.1/32 0.0.0.0/0 tcp dst eq
21
Command> set filter internet.out 2 permit 192.168.0.1/32 0.0.0.0/0 tcp src gt
1023 dst eq 20 estab
Command> set filter internet.out 3 permit 172.16.0.2/32 0.0.0.0/0 tcp src eq
20 dst gt 1023
Command> set filter internet.out 4 permit 172.16.0.2/32 0.0.0.0/0 tcp src eq
21 dst gt 1023 estab
```

If you allow any internal host to send out packets with FTP, replace 192.168.0.1/32 with 0.0.0.0/0 or your *network_number*/24. Take appropriate precautions to reduce the risk this configuration creates.

Rule to Permit DNS into Your Local Network

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

```
Command> set filter filtername RuleNumber permit udp src eq 53
```

This rule permits DNS replies into your local network.

Rule to Listen to RIP Information

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

```
Command> set filter filtername RuleNumber permit 172.16.0.0/32 192.168.0.0/32
udp dst eq 520
```

In the above example, 172.16.0.0/32 is the other end of the Internet connection and 192.168.0.0/32 is the local address of the connection.

Rule to Allow Authentication Queries

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

```
Command> set filter filtername RuleNumber permit tcp dst eq 113
```

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

Rule to Allow Networks Full Access

To allow some other network to have complete access to your network, add the following rule. In the example below, 172.16.12.0 is granted full access to 192.168.1.0/24:

```
Command> set filter filtername RuleNumber permit 172.16.12.0/24 192.168.1.0/24
```



Caution – Beware of associative trust. If you allow a network complete access to your network, you might unknowingly allow other networks complete access, as well. Any network that can access a network having complete access privileges to your network, also has access to your network. For example, if Network 1 trusts Network 2 and Network 2 trusts Network 3, then Network 1 trusts Network 3.

Restrictive Internet Filter

This example filter allows any kind of outgoing connection from the server, but blocks all incoming traffic to any host but your designated Internet server. This filter also limits incoming traffic on your Internet server to: SMTP, Network News Transfer Protocol (NNTP), DNS, FTP, and ICMP services.



Note – Even if you have the latest versions of the daemons **ftpd**, **httpd**, and **sendmail** you may be vulnerable to attacks through these services. Check the latest CERT Coordination Center advisories, available on **ftp.cert.org**, for the vulnerabilities of these services.

If you use the following example, replace the name **server** with the IP address or hostname of your Internet server:

```
Command> set filter restrict.in 1 deny 192.168.1.0/24 0.0.0.0/0 log
Command> set filter restrict.in 2 permit 0.0.0.0/0 10.0.0.3/32 tcp estab
Command> set filter restrict.in 3 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 21
Command> set filter restrict.in 4 permit 0.0.0.0/0 10.0.0.3/32 tcp src eq 20
dst gt 1023
Command> set filter restrict.in 5 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 119
Command> set filter restrict.in 6 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 25
Command> set filter restrict.in 7 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 80
Command> set filter restrict.in 8 permit 0.0.0.0/0 10.0.0.3/32 udp dst eq 53
Command> set filter restrict.in 9 permit 0.0.0.0/0 10.0.0.3/32 tcp dst eq 53
Command> set filter restrict.in 10 permit 0.0.0.0/0 10.0.0.3/32 icmp
```

Table 9-4 describes, line by line, each rule in the filter.

Table 9-4 Description of Restrictive Internet Filter

Rule	Description
1.	Denies any incoming packets from your own network (192.168.1.0) and makes a log.
2.	Permits packets from any established TCP connection to 10.0.0.3 (the Internet server).
3.	Permits FTP from any IP address to 10.0.0.3 (the server).
4.	Permits the FTP data back channel.
5.	Permits incoming NNTP (news) to 10.0.0.3 (the Internet server).
6.	Permits incoming SMTP (mail) to 10.0.0.3 (the Internet server).
7.	Permits HTTP requests to 10.0.0.3 (the Internet server).
8.	Permits DNS queries to 10.0.0.3 (the Internet server).
9.	Permits DNS zone transfers from 10.0.0.3 (the Internet server).
10.	Permits ICMP to 10.0.0.3 (the Internet server). You can further limit ICMP packet types to types 0, 3, 8, and 11 using four rules instead of one.

To log all packets that are denied, add the following rule to the end of your filter:

```
Command> set filter filtername RuleNumber deny log
```

Restricting User Access

Access filters enable you to restrict Telnet or rlogin connections to a specific host or network, or a list of hosts or networks. You can create an access filter that restricts user access to particular hosts.

Access filters work as follows:

1. The user specifies a host.
2. The host address is compared against the access filter.
3. If the address is permitted by the filter, the connection is established.
4. If the address is not permitted, the connection is denied unless access override is enabled.

If you want a user to be able to override a port's access filter, enable access override on that port. In this case, the process is as follows:

1. Access is denied by the access filter.
2. The user is prompted for a user name and password.
3. The user is verified by the user table or RADIUS.
4. The access filter defined for this user is used to determine if the user has permission to access the specified host.

To enable a user to override a port's access filter with his or her own filter, use the following command:

```
Command> set S0 access on
```


This chapter explains how to configure external modems to work with PortMaster products. For information on using the internal digital modems with the PortMaster 3, see Chapter 11, “Configuring the PortMaster 3.”

This chapter discusses the following topics:

- “Null Modem Cable and Signals” on page 10-1
- “Modem Functions” on page 10-2
- “Using Automatic Modem Configuration” on page 10-2
- “Configuring Ports for Modem Use” on page 10-7

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Because the PortMaster is a DTE device, a straight-through RS-232 cable is used to connect modems to it. Straight-through cables for modems use pins 2, 3, 4, 5, 6, 7, 8, and 20.

Null Modem Cable and Signals

Ports S0 through S29 are asynchronous DTE ports with female RS-232 connectors. To connect these ports to a terminal or other DTE, use a null modem cable, typically male-to-female. Directions (input/output) are with respect to the PortMaster. The PortMaster does not use the Data Set Ready (DSR) signal.



Note – When the console port is connected to a terminal, it uses software flow control and therefore requires pins 2, 3, and 7 only.

Null modem cables can be obtained from most suppliers of computer equipment.

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

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

Modem Functions

Configure modems to do the following for use with the PortMaster:

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

Using Automatic Modem Configuration

PortMaster products use a modem table to automate the modem configuration process. The modem table is user-configurable and includes long and short modem names, preferred DTE rate, and the modem initialization string. For convenience, the table is preconfigured by Lucent for many common modems.

When you specify the name of the modem and the attached port, the PortMaster automatically configures the modem for you, provided the modem is in the factory default state when it is initialized.

After a modem type has been specified, the PortMaster automatically sets the port for hardware flow control, the correct speed, and modem control when the port is reset.

Displaying Modem Settings and Status

To display the modems currently configured in your modem table, use the following command:

```
Command> show table modem
```


A modem table display looks like the following:

Short Name	Long Name	Type
-----	-----	-----
cardinal	Cardinal MVP288XF	System
mega	Massive MegaFast	User
supra-288	Supra V.34	System

The modem **type** is either system or user. *System* indicates that the configuration settings are the factory default settings. *User* indicates that the user has configured the modem table settings for that modem.

To display the settings for a particular modem, use the following command:

Command> **show modem** *ModemName(short)*

The display for a modem looks like this:

```

Short Name: supra-fax-288
Long Name: SupraFax 28.8
Optimal Speed: 115200
Type: User Defined
Init Script: Send Command
-----
AT&F2&C1&D3S0=1S2=129s10=20&W
-----
Wait for Reply
-----
OK

```

Adding a Modem to the Modem Table

To add a modem to the modem table, use the following command:

Command> **add modem** *ModemName(short)* "*ModemName(long)*" *Speed* "*String*"

For example, to add a Paradyne 3811+ modem to the modem table, enter:

Command> **add modem para3811** "Paradyne 3811+" 115200 "AT&FS0=1&W\r^OK"



Note – Use a **\r** for a carriage return, and a caret (^) to separate the send and expect characters in the string. In the example above, the PortMaster expects **OK**. Never use **on** or **off** for a modem short name.

Table 10-1 shows the current factory default settings for commonly used modems.

Table 10-1 Factory Default Modem Table Entries

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
at&t-v32	AT&T Keep In Touch	57600	AT&F&D3&T5&R0\\D1S0=1&W^OK
cardinal	Cardinal MVP288XF	11520 0	AT&F1&C1&D2&K3S0=1S2=129S10=20&W0&W1
card-v34-p	Cardinal MVP288CC PCMCIA	11520 0	AT&F&C1&D3S0=1s2=129S10=20&W
eiger-v32-p	Eiger 14.4 PCMCIA	57600	AT&F&C1&D3S0=1S10=20&W
eiger-v34-p	Eiger 28.8 PCMCIA	11520 0	AT&F&C1&D3S0=1S10=20&W
gvc-14.4	GVC/Maxtech V.32	57600	AT&F&C1&D3S0=1S10=20&W0
gvc-28.8	GVC/Maxtech V.34	11520 0	AT&F&C1&D3S0=1S10=20&W0
hay-cent2	Hayes Century 2 Rack V.32bis	11520 0	AT&F&C1&D2&K3S0=1S10=20&W0
intel-v32-p	Intel V.32bis PCMCIA	11520 0	AT&F&C1&D3S0=1&W&W1^rOK
megahz-v32-p	Megahertz XJ2288 V.34bis PCMCIA	11520 0	AT&F&C1&D3S0=1&W
megahz-v32-p	Megahertz XJ2288 V.34bis PCMCIA	11520 0	AT&F&C1&D3S0=1&W
micro-desk	Microcom 28.8	11520 0	AT&F&C1&D2\$B115200\\Q3%U1&T5S0=1S10=20*W0&Y0
mot-uds	Motorola UDS V.34	11520 0	AT&F&C1&D2\\Q3S0=1S10=20S80=18&W
mot-bit	Motorola Bitsurfr	11520 0	AT&F&C1&D2%A4=1%A2=95&m0@P2=115200@P1=a&W

Table 10-1 Factory Default Modem Table Entries (Continued)

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
mot-pwr-p	Motorola Power 14.4 PCMCIA	57600	AT&F&C1&T5&C1&D2&W
mot-life-p	Motorola Lifestyle 14.4 PCMCIA	57600	AT&FS0=1&C1&D2\\Q3&T5&W^OK
multizdx	MultiTech Z/DX fax/data v.32	11520 0	AT&F^ATM0&E1&C1&D3\$SB115200S0=1S10= 20%E0&W0
multi-v34	MultiTech MT2834 28.8k	11520 0	AT&F^AT&C1&D3S0=1&W0
multi-v34	MultiTech MT2834 28.8k	11520 0	AT&F^AT&C1&D3S0=1&W0
pp-v32	Practical Peripherals PP9600SA	57600	AT&F&C1&D3S0=1S2=129&W
pp-v34	Practical Peripherals PM288T II	11520 0	AT&F0M0S0=1V1&C1&D3&K3&W0&W1
para3811	Paradyne 3811+	11520 0	AT&FS0=1&W
ppi-v34-p	PPI ProClass V.34 PCMCIA	11520 0	AT&F&C1&D3&K3S0=1&W&W1
premax-v32-p	Premax V.32bis PCMCIA	11520 0	AT&F&C1&D3S0=1&W&W1
scout-v32-p	DSI Scout V.32bis PCMCIA	11520 0	AT&F&C1&D3S0=1&W
supra-288	Supra V.34	11520 0	AT&F2S0=1&W
supra-fax-288	SupraFax 28.8	11520 0	AT&F2&C1&D3S0=1S2=129s10=20&W
tdk-288-p	TDK DF2814 V.Fast PCMCIA	11520 0	AT&F&C1&D3S0=1&W

Table 10-1 Factory Default Modem Table Entries (Continued)

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
usr-v32-p	USR Courier/Sportster V.32bis PCMCIA	57600	AT&F1&W
usr-v34-p	USR Courier/Sportster V.34 PCMCIA	11520 0	AT&F1S0=1&W
usr-v32	USR Courier/Sportster V.32bis	57600	AT&F1S0=1&W
usr-v34	USR Courier/Sportster V.34	11520 0	AT&F1S0=1&W
usr-spt-v32	USR Sportster V.32bis	57600	AT&F1S0=1S10=20S13.0=1&W0
usr-spt-336	USR Sportster 33.6	11520 0	AT&F1S0=1S10=20S13.0=1&W0
zyxel	Zyxel U1496E	57600	AT&FM0&D2S0=1S2=1

Associating a Modem with a Port

To automatically configure a modem and associate it in the modem table with the port it is attached to, use the following commands:

```
Command> set S0|all modem ModemName(short)
Command> reset S0|all
```

For example; to associate a U. S. Robotics V.34 modem with port S1 and configure the modem, enter:

```
Command> set s1 modem usr-v34
Command> reset s1
```

To configure all ports for the same modem type, use **all** instead of the port number in the previous example. After the modem is attached to the port, configure the other modem settings described in “Configuring Ports for Modem Use” on page 10-7.

To configure the modem **not** to answer when users dial in, set **S0=0** in the initialization string.

Configuring Ports for Modem Use

The modem settings described in this section are configured for each port and should match the configuration on the attached modem.

Setting the Port Speed

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

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

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

To set the port speed, use the following command—entered on one line:

```
Command> set S0|all speed [1|2|3] Speed
```

You can substitute any of the following for *Speed*:

300	1200	4800	19200	57600	115200
600	2400	9600	38400	76800	

You can set the speed for all the asynchronous ports simultaneously by using the **set all speed** command.

Setting Modem Control

Set modem control on if you want to use the DCD signal for modem connections. When modem control is on, the PortMaster uses the condition of the carrier detect line to determine whether the line is in use. Modem control must be on for PortMaster outbound traffic. If modem control is off, the PortMaster assumes the carrier detect line is always asserted. As a result, the PortMaster cannot attach to the modem for outbound traffic because it regards the line as busy.

To set modem control, use the following command:

```
Command> set S0 cd on|off
```

Setting Parity

The parity setting must be configured to match the parity setting on the attached modem. The parity default value is **none** and must be used for ports configured for network dial-in or dial-out operation. Table 10-2 describes the parity options.

Table 10-2 Parity Options

Option	Description
none	Assumes 8 databits, 1 stop bit, and no parity bit.
even	Assumes 7 databits, 1 stop bit, and even parity.
odd	Assumes 7 databits, 1 stop bit, and odd parity.
strip	Assumes 8 databits and 1 stop bit. The parity bit is stripped from the datastream when it is received by the PortMaster.

To set the parity for a modem and its port, use the following command:

```
Command> set S0 parity even|none|odd|strip
```

Setting the Flow Control

The PortMaster supports both software flow control and hardware flow control. Software flow control uses the ASCII control characters DC1 and DC3 to communicate with the attached device and to start and stop the flow of data.

To set software flow control for a modem, use the following command:

```
Command> set S0 xon/xoff on|off
```

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

To set hardware flow control for a modem, use the following command:

```
Command> set S0 rts/cts on|off
```



Note – Because it is more reliable, you should always use hardware flow control if it is available. Do not use both hardware and software flow control on the same port.

Hanging Up a Line

You can specify whether the DTR signal is dropped and the modem disconnected after a session is terminated. If line hangup is enabled and the session is terminated, DTR is held low, signaling the modem to disconnect. If line hangup is disabled, the DTR signal does not drop and the modem does not hang up when the user session terminates.

To set line hangup for a modem, use the following command:

```
Command> set S0 hangup on|off
```



Note – Resetting the port administratively with the **reset** command always drops DTR.

This chapter describes how to use the command line interface to configure the ISDN Primary Rate Interface (PRI) Line0 and Line1, and the digital modems on the PortMaster 3. The PortMaster 3 can also use many of the commands common to all PortMaster models.



Note – After making any configuration changes to a line (Line0 or Line1), you must use the **save all** and **reboot** commands for the changes to take effect.

This chapter discusses the following topics:

- “Configuring General Settings” on page 11-1
- “Setting the Inband Signaling Protocol for T1” on page 11-3
- “Setting the Inband Signaling Protocol for E1” on page 11-4
- “Configuring ISDN PRI Settings” on page 11-5
- “Using True Digital Modems” on page 11-8
- “Using Channelized T1” on page 11-10
- “Using Multichassis PPP” on page 11-15
- “Troubleshooting the PortMaster 3” on page 11-16

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Configuring General Settings

Use the following general settings to configure the PortMaster 3.

Displaying Line Status

To display the status of a E1 or T1 line, use the following command:

Command> **show** *Line0*

Configuring Line Use

You can use a line as a single E1 or T1 line, as PRI B channels, as fractional E1 or T1 lines divided into channel groups, or for inband signaling for channelized T1.



Note – T1 and E1 lines require an external clock signal provided by the device to which the PortMaster is connected, or by the telephone company network.

To configure a line, use the following command. Table 11-1 explains the line use options.

Command> **set** *Line0* **isdn**|**t1**|**e1**|**fractional**|**isdn-fractional**|**inband**

You use the **fractional** keyword in this command to break up a channelized T1 line into groups. The **isdn-fractional** keyword refers to PRI only.

Setting Channel Groups

You can divide the channels of a T1 or E1 line into numbered groups after the line type has been set to fractional with the **set** *Line0* **fractional** command.

To set the channel group for a T1 or E1 line, use the following command. Table 11-1 explains the channel group options.

Command> **set** *Line0* **group** *Cgroup*|**none** **channels** *Channel-list*

Table 11-1 Channel Group Options

Option	Description
<i>Line0</i>	Line0 or Line1.
<i>Cgroup</i>	Group number from 1 to 63, or none to unassign channels.
<i>Channel-list</i>	Space separated list of one or more channel numbers, from 1 through 24 for T1, or 1 through 30 for E1. The channel numbers do not have to be contiguous.



Warning – If you configure a line for fractional T1 and reboot the PortMaster 3 before configuring the group and channels, you will no longer be able to see and configure the line. You must erase your entire configuration and reboot to see the line again.

Setting the Channel Rate

To set the channel rate to 56Kbps or 64Kbps for a channel group, use the following command. Table 11-2 explains the channel rate options.

Command> **set Line0 group Cgroup 56k|64k**

Table 11-2 Channel Rate Options

Option	Description
<i>Line0</i>	Line0 or Line1.
<i>Cgroup</i>	Defined channel group from 1 to 63.
56k	56Kbps, typically used for D4 framing.
64k	64Kbps, used for framing types other than D4. This is the default.

Setting the Inband Signaling Protocol for T1

To set the inband signaling protocol and the inband call options used with channelized T1, use the following command. Table 11-3 explains the inband signaling protocol options.

Command> **set Line0 signaling wink|immediate|fxs**

Table 11-3 T1 Inband Signaling Protocol Options

Option	Description
<i>Line0</i>	Line0 or Line1.
wink	E & M wink start protocol, an option for use with T1 lines. This is the T1 default.
immediate	E & M immediate start protocol, used with T1 lines.
fxs	Foreign exchange station (FXS) loop start protocol used with T1 lines.

Setting the Inband Signaling Protocol for E1

Although PortMasters do not require dial digits (the calling number and caller ID) when establishing a connection, most Telcos transmit this information by default. You can use the **r2gen** signalling option if you don't require dial digits, but you must first arrange for the Telco not to transmit these signals.

The PortMaster defaults to **r2gen** when you set the line to inband (see "Configuring Line Use" on page 11-2).

To accept caller ID and dial digit tones, use the **mrf2** option. Because some countries implement different variations of multi-frequency robbed-bit signalling (MFR2), you must specify a profile with the **mrf2** option.

To set the inband signaling protocol and the inband call options used with channelized E1, use the following command.

```
Command> set Line0 signaling mrf2 r2gen|Profile
```

Table 11-4 explains the inband signaling protocol options and profiles.

Table 11-4 E1 Inband Signaling Protocol Options

Option	Profile	Description
Line0		Line0 or Line1.
mrf2		Accept caller ID and dial digit tones
	0	ITU standard, Argentina and Chile. This is the default.
	1	Mexico.
	2	Brazil.
	3	Venezuela.
	4	Mexico.
r2gen		Generic R2, the default; no caller ID and dial digit tones are exchanged.

Configuring ISDN PRI Settings

Use the following settings to configure ISDN PRI on the PortMaster 3.

Setting the ISDN PRI Switch

The switch type information is available from your ISDN PRI service provider. To set the switch type for ISDN connections to the PortMaster ISDN PRI ports, use the following command—entered on one line. Table 11-5 explains the ISDN switch options.

```
Command> set isdn-switch ni-2|dms-100|4ess  
|att-5ess|net5|vn2|vn3|ltr6|ntt|kdd
```

Setting the Framing Format

Table 11-5 ISDN Switch Options

ISDN Switch	Description
ni-2	National ISDN-2 (NI-2) compliant. This is the default.
dms-100	Northern Telecom DMS-100 Custom.
4ess	AT&T 4ESS.
att-5ess	AT&T 5ESS.
net5	European ISDN PRI standard.
vn2	France—older switch.
vn3	France—older switch.
ltr6	Germany—older switch.
ntt	Japan.
kdd	Japan.

To set the framing format used for the E1 or T1 line, use the following command. Table 11-6 explains the framing format options.

Command> **set Line0 framing esf|d4|crc4|fas**

Table 11-6 T1 Inband Signaling Protocol Options

Option	Description
<i>Line0</i>	Line0 or Line1.
esf	Extended superframe. This is the default format for T1 lines.
d4	D4 framing, an alternative format for T1 lines.
crc4	Cyclic redundancy check 4. This is the default format for E1 lines.
fas	Frame Alignment Signal, an alternative format for E1 lines.

Setting the Encoding Method

This command sets the encoding method used with T1 and E1 lines. Table 11-7 explains the encoding method options.

Command> **set Line0 encoding b8zs|ami|hdb3**

Table 11-7 Encoding Method Options

Option	Description
<i>Line0</i>	Line0 or Line1.
b8zs	Bipolar 8-zero substitution. This is the default for T1 lines.
ami	Alternate mark inversion.
hdb3	High-density bipolar 3. This is the default for E1 lines.

Setting the Pulse Code Modulation

You need to set the pulse code modulation only if you are using digital modems and your PRI service provider instructs you to change the setting to something other than the default. This command sets the digital encoding method used for analog signals.

To set the pulse code modulation, use the following command. Table 11-8 explains the pulse code modulation options.

```
Command> set Line0 pcm u-law|a-law
```

Table 11-8 Pulse Code Modulation Options

Option	Description
<i>Line0</i>	Line0 or Line1.
u-law	Default method for T1 PRI lines.
a-law	Default method for E1 PRI lines.

Setting the Loopback

You can test the telephone line of your T1 or E1 ISDN connection by setting the local network loopback.

To set the loopback, use the following command. Table 11-10 explains the loopback options.

```
Command> set Line0 loopback on|off
```

Setting the Directory Number

Normally, a T1 or E1 line has a single telephone number. However, when the line is set up as ISDN B channels, you can set a telephone number for an individual port. This feature allows you to identify the circuit telephone number associated with a specific ISDN port.

To set a telephone number for an individual port when the line is configured as ISDN B channels, use the following command. Table 11-9 explains the directory number options.

```
Command> set S0 directory Number
```

Table 11-9 Directory Number Options

Options	Description
<i>S0</i>	One of the ISDN ports
<i>Number</i>	Access telephone number

Using True Digital Modems

Use the following settings to configure the built-in digital modems on the PortMaster 3.

Setting Digital Modems

The digital modems are numbered from m0 to m59, for a maximum of 60 modems. Modem slot 0 is allocated numbers m0 through m9, modem slot 1 is allocated numbers m10 through m19, and so on. Whether 8-port or 10-port modem cards are installed, the allocation of numbers to the modem slots does not change. For example, an 8-modem card installed in modem slot 0 has modems numbered m0 through m7. Modems on an 8-modem card installed in modem slot 1 are numbered m10 through m17.

To make the digital modems available or unavailable, use the following command. Table 11-10 explains the digital modem options.

Command> **set MO on|off**

Table 11-10 Digital Modem Options

Option	Description
<i>M0</i>	Any modem number from m0 to m59. Changes to the default setting must be made to individual modems.
on	Make the modem available for use. This is the default.
off	Busy the modem so it is unavailable.



Note – Digital modems do not require any configuration or initialization string.

Hot-Swapping Digital Modem Cards

With the lastcall feature, you can hot-swap a modem card without dropping calls. To force an active modem into ADMIN mode as soon as the last active call terminates, use the following command:

```
Command> set MO lastcall
```

When the lastcall feature is set, modem status displayed by the **show m0** and **show modems** commands is ACT(LC).

Setting Digital Modems to Analog Service

When analog modem service is required for dial-out network connections, you can convert the analog service to digital service.

To set the digital modems to analog modem service for the specified location, use the following command. Table 11-11 explains the analog modem options.

```
Command> set location Locname analog on|off
```

Table 11-11 Analog Modem Options

Option	Description
<i>Locname</i>	Location name that is in the location table.
on	Enables analog modem service on dial-out.
off	Disables analog modem service on dial-out.

Use the following command to display the settings for a particular modem:

```
Command> show MO
```

You can display the status for all digital modems. Modem states are as follows:

- ACTIVE—in use
- READY—available for use
- ADMIN—busy

- TEST—under test
- DOWN—unavailable

To display the status for all modems, use the following command:

Command> **show modems**

Using Channelized T1

The PortMaster 3 has an integrated channel service unit/digital service unit (CSU/DSU). However, the other end of a T1/E1 connection might require an external clock signal provided by the telephone company, or a CSU/DSU.

Why Use Channelized T1?

Channelized T1 service provides 24 channels of 56Kbps capacity each. An ISDN PRI line provides 23 channels of 64Kbps capacity each—plus one 64Kbps signaling channel. However, channelized T1 is available in many service areas that do not yet provide ISDN PRI. In areas where PRI is available, the cost of channelized T1 may be significantly less than the cost of PRI.

How to Order DS-1 Service from the Telephone Company

The telephone company will ask you the following two questions when you order digital service level 1 (DS-1) service:

- What signaling protocol do you use?

You can use either of the following signaling protocols on the PortMaster 3:

- **E & M wink start**
- **Foreign exchange station (FXS)**
- If you use E & M wink start, how many Directory Number Identification Service (DNIS) digits do you need?

ComOS 3.6-and-later releases require one DNIS digit.

Record the line parameters provided by the telephone company.

Configuring the PortMaster 3 for Channelized T1

Follow these steps to configure the PortMaster 3 to use channelized T1 service:

1. Set the line for inband signaling.

```
Command> set Line0 inband
```

2. Set the signaling protocol and the line provisioning.

```
Command> set Line0 signaling wink|fxs inonly
```

3. Set the framing format for the line.

```
Command> set Line0 framing esf|d4|crc4|fas
```

4. Set the encoding method for the line.

```
Command> set Line0 encoding b8zs|ami
```

5. Save the configuration changes and reboot.

```
Command> save all
```

```
Command> reboot
```

6. Use the following command to display the line configuration.

```
Command> show Line0
```

Example Channelized T1 Configuration

To configure the Line1 port on a PortMaster 3 for inband, channelized T1 for inbound calls using E & M wink start, extended superframe format, and bipolar 8-zero substitution, use the following commands:

```
Command> set line1 inband
```

```
Command> set line1 signaling wink inonly
```

```
Command> set line1 framing esf
```

```
Command> set line1 encoding b8zs
```

```
Command> save all
```

```
Command> reboot
```

To display the line configuration for line 1, for example, enter the following command:

```
Command> show line1
-----line1 - T1 Inband DS0 -----
Status: UP Framing: ESF Encoding: 8ZS PCM: u-law
Signaling: Trunk E&M wink start Options: inbound calls only
Receive Level: +2dB to -7.5dB
Alarms Violations
-----
Blue 0  Bipolar 0
Yellow 1  CRC Errors 0
Receive Carrier Loss 0  Multiframe Sync 0
Loss of Sync 0
```

Using the T1 Expansion Card

The T1 expansion card is identified as **line2** on the PortMaster, and has the same settings as *line0* and *line1*. Valid line types include **fractional** and **T1**. All line framing and encoding types are supported. When set to fractional, the card supports only one line group. The first line group found (numerically) is used for the configuration. The fractional line group supports any number of time slots. It also supports 56Kbps channels.

In addition to line2, a new port is added to the list of active ports. In a single-PRI PortMaster 3, the port is identified as W2; in a two-PRI PortMaster 3 it is identified as W48.

If the Stac compression card is present in the PortMaster 3, Stac compression can be enabled for the T1 line.

Although the T1 expansion card is hot-swappable, when you remove the card from the slot you must wait approximately 5 seconds before reinserting it. If you remove the card and reinsert it immediately, the PortMaster locks up and must be restarted.

Clocking

With the T1 expansion card, you can use internal clocking on the line. Use the following command to set clocking:

```
Command> set line2 clock internal|external
```

When you specify **internal**, the built-in 1.544MHz crystal sets timing on the line. This is useful for dry wire configurations, or for back-to-back connections. When you specify **external**, the built-in DSU/CSU extracts timing from the line.

Configuring the T1 Expansion Card for Fractional T1

The T1 card is identified as line2 in the PortMaster 3. Follow these steps to configure the PortMaster 3 to use fractional T1 service:

1. Set the line for fractional T1.

```
Command> set line2 fractional
```

2. Set the channel group for fractional T1.

```
Command> set line2 group Cgroup channel Channel-list
```

3. Set the channel rate.

```
Command> set line2 group Cgroup 56k|64k
```



Note – 56Kbps is typically used for D4 framing while 64Kbps, the default, is used for other framing types.

4. Save the configuration and reboot the PortMaster.

```
Command> save all
```

```
Command> reboot
```



Note – If you reboot the PortMaster before setting the group and the channel for fractional T1, you lose the line.

Configuring the PortMaster 3 for Full T1

To configure the card for full T1, enter the following commands:

```
Command> set line2 t1
```

```
Command> save all
```

Troubleshooting the T1 Expansion Card

If the T1 expansion card is not properly installed, the **show line2** command displays the following status:

```
line2 not available
```

This message indicates that the card is either not present or installed incorrectly. If the card is present, remove it, wait 5 seconds and reinstall it. Refer to your hardware installation guide for instructions.

When you remove the card, the console displays the following message:

```
Card Service: Stopping wancard in slot 0
```

When you correctly reinstall the card, the console displays the following message:

```
Card Service: Starting wancard in slot 0
```

```
WANCTL version 0.0
```

```
WANCTL: sync_init - found device
```

Use the **show alarms** command to determine whether the T1 card is not operating (for example, if the cable is pulled out). The PortMaster does not show an alarm if the card is removed.

```
Command> show alarms
```

Alarm Id	Age	Severity	Alarm Message
-----	----	-----	-----
2851352	0	0	T1 line(2) down

```
Command> show alarm 2851352
```

```
----- Alarm Details -----
Alarm Id: 2851352      Alarm Message: T1 line(2) down
Age in minutes: 0      Alarm repeated: 1 times
Severity: 0            Reported: SNMP
```

Using Multichassis PPP

Multichassis PPP allows the use of Multilink PPP across multiple PortMasters in a single telephone hunt group, and on the same Ethernet.

Setting Multichassis PPP

To enable Multichassis PPP, set the endpoint discriminator on all PortMaster products sharing a hunt group and Ethernet, with the same 12-digit hexadecimal number. For convenience, you can use the Ethernet MAC address of one PortMaster as the endpoint discriminator for all the PortMasters on that hunt group, but any 12-digit hexadecimal number will serve.

To enable Multichassis PPP, use the following commands:

```
Command> set endpoint Hex  
Command> save all  
Command> reboot
```



Note – You must use the **save all** and **reboot** commands after issuing the **set endpoint** command for the endpoint discriminator to take effect.

Displaying Multichassis PPP Addresses

To display the addresses of the neighboring PortMasters in the same Multichassis PPP group, and a list of connections to virtual and physical ports on the PortMaster, use the following command:

```
Command> show mcppp
```

Disconnecting a User from a Virtual Port

To disconnect a user attached to a virtual port, you must reset the port. Because the virtual port has a corresponding physical port on the slave unit, once the virtual port is reset on the master, its corresponding physical port is also reset on the slave.

When using Multichassis PPP, use the following command on the master unit to reset a virtual port:

```
Command> reset V0
```

Troubleshooting the PortMaster 3

The **debug** command is useful for troubleshooting the digital modems and Multichassis PPP events. Output is sent to the system console set by the **set console** command. After completing the debugging process, disable the **debug** commands by using the correct **set debug off** command, and reset the console with the **reset console** command. Debug information is displayed to the console.

To set debug flags used for troubleshooting, use the following command—entered on one line:

Command> **set debug mdp-status|mdp-events|mcppp-event on|off**

Table 11-12 explains the debug options for the PortMaster 3

Table 11-12 Debug Options for the PortMaster 3

Option	Description
mdp-status	Set on to display the status of the digital modems.
mdp-events	Set on to display the progress of the digital modems as they initialize.
mcppp-event	Set on to display all the information related to the Multichassis PPP events.

This chapter describes how to configure the PortMaster to connect two local area networks (LANs) via ISDN using V.25bis dialing on a Basic Rate Interface (BRI) with an integrated network termination device (NT1). This chapter also provides an example to demonstrate this type of configuration.

For information on the PortMaster 3 and ISDN PRI service, see Chapter 11, “Configuring the PortMaster 3.”

This chapter discusses the following topics:

- “Overview of ISDN BRI Connections” on page 12-1
- “Configuring ISDN” on page 12-4
- “ISDN Port Configuration Tips” on page 12-9
- “ISDN BRI Unnumbered IP Configuration Example” on page 12-9
- “Troubleshooting an ISDN BRI Connection” on page 12-21

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of ISDN BRI Connections

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

PortMaster products support manual dial-on-demand and automatic ISDN connections using the BRI port and the PPP protocol. BRI supports two 64Kbps B channels for data and one 16Kbps D channel for signaling. ISDN ports are available as either a U or S/T interface.

ISDN ports are easier to configure than asynchronous or synchronous ports. Because the ISDN U interface has the NT1 device integrated in the port, no modem, CSU/DSU, or external terminal adapter is required.

For the ISDN S/T interface, a PortMaster requires an external terminal adapter to connect from the PortMaster synchronous port to the ISDN link. For terminal adapters that do not have automatic dialing or for administrators who want to manually connect with the terminal adapter, the PortMaster supports automatic location table scripting. For more information, see Chapter 8, “Configuring Dial-Out Connections.” For more information about configuring the PortMaster for ISDN with an external terminal adapter and automatic location table scripting, refer to Chapter 14, “Using Synchronous V.25bis Connections.”

ISDN BRI ports can provide the same services that an asynchronous port provides, except for direct network hardwired connections. The PortMaster automatically detects whether the port is providing asynchronous or synchronous, 56Kbps or 64Kbps.

ISDN BRI connections can be initiated as needed, or they can remain active continuously. A dial-out location must be specified in the location table for dial-out connections, and a dial-in user must be specified in the user table or RADIUS for dial-in connections. Figure 12-1 shows an example of an ISDN connection.

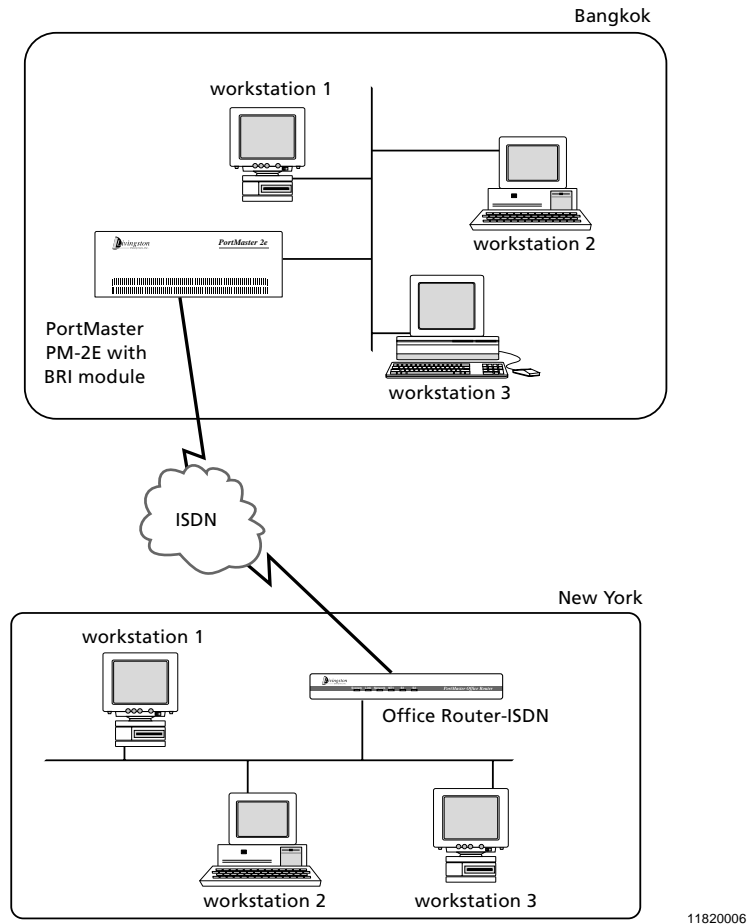
You can use PAP and CHAP for dial-in and dial-out authentication.

Contact your service provider for specific information about your ISDN switch type and service profile identifier (SPID).

The following ISDN-specific settings need to be configured for each ISDN BRI port on the PortMaster to permit ISDN service:

- ISDN switch type
- SPID—U.S. ISDN only
- Directory number (optional)

Figure 12-1 Example of an ISDN Connection



Provisioning

To help you determine the kind of provisioning you require for your ISDN setup, refer to the information in the hardware installation guide and on the Lucent Remote Access website at <http://www.livingston.com>.

Configuring ISDN

This section describes the commands that you need to configure a PortMaster for ISDN BRI service.

ISDN BRI Switch Types

The North American ISDN U interface and international S/T interface require different switch type settings on your PortMaster.

North American ISDN BRI Switch Types

The ISDN switch type for North American ISDN connections (U interface) can be set to one of four values, shown in Table 12-1.

Table 12-1 North American ISDN BRI Switch Types

ISDN Switch Type	Used for
ni-1	National ISDN-1 (NI-1) (default)
dms100	Northern Telecom DMS 100 Custom
5ess	AT&T 5ESS Custom Multipoint
5ess-ptp	AT&T 5ESS Custom Point-to-Point

International ISDN BRI Switch Types

The PortMaster ISDN S/T interface for use in Japan, Europe, and other countries using international ISDN standards uses a different set of switch type settings, shown in Table 12-2.

Table 12-2 International ISDN BRI Switch Types

ISDN Switch Type	Used for
net3	EuroISDN standard (includes Swiss standards)
vn4	France—current national switch type
1tr6	Germany—older switch type

Table 12-2 International ISDN BRI Switch Types (Continued)

ISDN Switch Type	Used for
ntt	Japan
kdd	Japan

Setting the Switch Type

To set the ISDN switch type for an ISDN BRI U interface, use the following commands:

```
Command> set isdn-switch ni-1|dms-100|5ess|5ess-ptp  
Command> reboot
```

To set the ISDN switch type for an ISDN BRI S/T interface, use the following commands:

```
Command> set isdn-switch net3|vn4|1tr6|ntt|kdd  
Command> reboot
```



Note – You must reboot the PortMaster after changing the switch type for the change to take effect.

Service Profile Identifier (SPID) for ISDN BRI

The service profile identifier (SPID) is a unique number assigned by the telephone company that identifies your ISDN equipment to the telephone company's switch. SPIDs are used with BRI ports only, and only in the United States. A SPID can have up to 20 digits. If you are connecting to a 5ESS point-to-point switch, a SPID is not required.

To set the SPID and save the configuration to nonvolatile RAM, use the following commands:

```
Command> set SO spid Number  
Command> save all
```

The **set debug isdn on** command shows any invalid SPIDs.

Terminal Identifier (TID) for ISDN BRI

The terminal identifier (TID) is a numeric value used by some telephone switches for additional identification. Some telephone companies require the SPID, while others require a TID, as well. When configuring the PortMaster, append the TID to the SPID if required by your carrier.

Directory Number

The optional directory number is a 10-digit phone number provided by the telephone company. If it is set, an incoming call must match this number to determine which port the call should be taken on.

Use either of the following commands to set the directory number.

```
Command> set SO dn Number  
Command> set SO directory Number
```

Enter the following command to save the configuration to Flash:

```
Command> save all
```

Information Elements (IEs)

“Number plan” and “number type” are values that relate to attributes associated with the called and calling party information elements (IEs) used to exchange phone numbers within a setup message in ISDN. These values can vary among countries and telephone companies.

You can configure the PortMaster to autodetect number plan and number type settings on incoming calls and, if necessary, automatically modify the PortMaster configuration. If the PortMaster detects a difference between the current settings and those of an incoming call, it sends the following console message indicating that the values are different and have been changed:

```
Call recvd numberplans do not match (n:n)
```

The first *n* refers to the new number type and the second *n* refers to the new number plan setting. Use the **save all** command to save modified settings to nonvolatile RAM.

To turn on autodetection of IEs, enter the following command:

```
Command> set isdn-numberauto on
```



Note – **numberauto** is off by default.

Setting the Number Type

To change the number type from the default manufacturer setting (so that you can, for example, begin successfully to place outbound calls), use the following command:

```
Command> set isdn-numbertype 0|1|2|4
```

The new setting becomes effective immediately; it does not need to be saved to nonvolatile RAM.

Enter this command without a number type value to display a list of all plan values available, and the current setting.

Setting the Number Plan

To change the number plan from the default manufacturer setting (so that you can, for example, begin successfully to place outbound calls), use the following command:

```
Command> set isdn-numberplan 0|1|2|7|8
```

The new setting becomes effective immediately; it does not need to be saved to nonvolatile RAM.

Enter this command without a number plan value to display a list of all plan values available, and the current setting.

Multilink PPP

Multilink PPP V.120 is supported on analog and ISDN interfaces. The PortMaster accepts and detects both multiline load balancing and Multilink PPP connections. Multiple lines can be used to increase bandwidth, either using Multilink PPP as defined in RFC 1717 or using Lucent's multiline load balancing.

To enable Multilink PPP, use the following command:

```
Command> set location Locname multilink on
```

Multiple Subscriber Network for an S/T Interface

For countries that support BRI via the S/T bus interface, you can enable the multiple subscriber network (MSN) feature. When enabled, this feature allows multiple ISDN devices attached to the same BRI line to receive calls not intended for the PortMaster. When the MSN feature is disabled, the PortMaster rejects the call if a port is not available. In this case other S/T connected devices are not given an opportunity to check or accept the call. This is the default.

To enable the MSN for an ISDN S/T interface, enter the following command:

```
Command> set isdn-msn on
```

Port Limits

You can set port limits on a per-user basis for Multilink V.120, Multilink PPP, and asynchronous multiline load balancing users. If a port limit is set, the user is limited to that number of ports on the PortMaster. If the number of dial-in ports is left unconfigured, port limits are not imposed and the PortMaster's multiline load balancing, Multilink V. 120, and Multilink PPP sessions are allowed. You can also configure this setting using the RADIUS Port-Limit attribute.

To set port limits, use the following command:

```
Command> set user Username maxports Number
```

Data over Voice

Data over voice is supported for inbound and outbound ISDN connections. The PortMaster accepts inbound voice calls and treats them as data calls.

To force a data-over-voice call for an outbound ISDN connection, use the following command:

```
Command> set location Locname voice on|off
```


ISDN Port Configuration Tips

Use the following tips to help you configure your ISDN BRI port:

- Modem control (carrier detect), flow control, and speed are not set on an ISDN port. The PortMaster automatically detects the speed and sets the port to 64000bps or 56000bps accordingly. Flow control is not set on a synchronous line because the external clock speed is provided by the telephone company and carrier detect is always used.
- Refer to your hardware installation guide for information on ISDN LED activity.
- The ISDN ports support synchronous PPP and asynchronous V.120 PPP or SLIP. The **show S0** command displays “64000/async” if the port is in use for an asynchronous V.120 connection.
- When using the ISDN port for network dial-out, use the **set location telephone**, **set location username**, and **set location password** commands as described in Chapter 8, “Configuring Dial-Out Connections.”

ISDN BRI Unnumbered IP Configuration Example

This example illustrates how to connect a PortMaster located in one office (Denver) with a PortMaster located in another office (San Francisco) using an on-demand ISDN connection.

Configuration Steps

To install your PortMaster, follow the instructions in the hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

1. **Use a cable with RJ-45 connectors to connect the BRI port to the ISDN telephone line.**

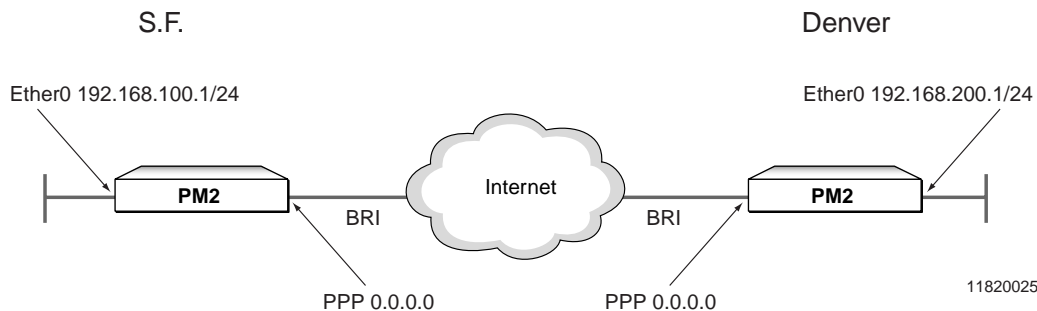


Caution – Do not plug an analog telephone line into the PortMaster BRI port. The PortMaster could be damaged.

- 2. Configure the following settings for the PortMaster in Denver:**
 - a. Configure global settings (page 12-11).
 - b. Configure Ethernet interface settings (page 12-12).
 - c. Configure ISDN port settings (page 12-12).
 - d. Configure dial-in users (page 12-13).
 - e. Configure dial-out locations (page 12-14).
- 3. Configure the following settings for the PortMaster in San Francisco:**
 - a. Configure global settings (page 12-16).
 - b. Configure Ethernet interface settings (page 12-16).
 - c. Configure ISDN port settings (page 12-17).
 - d. Configure dial-in users (page 12-18).
 - e. Configure dial-out locations (page 12-19).
- 4. Test the configuration (page 12-20).**
- 5. Troubleshoot the configuration (page 12-21).**

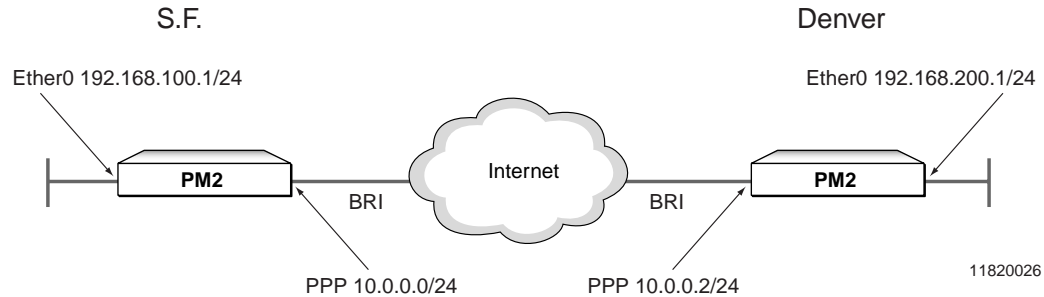
Figure 12-2 illustrates the ISDN BRI example in this section using unnumbered interfaces.

Figure 12-2 ISDN BRI Unnumbered



For comparison, Figure 12-3 shows a similar configuration using ISDN BRI with numbered interfaces.

Figure 12-3 ISDN BRI Numbered



Configuring the PortMaster in Denver

The PortMaster in Denver is being configured for an ISDN dial-up connection to the PortMaster in San Francisco.

Configuring Global Settings

Configure the global settings on the PortMaster in Denver to the values shown in Table 12-3.

Table 12-3 Global Values

Setting	Command
IP gateway	set gateway 192.168.1.1
System name	set sysname denver
ISDN switch	set isdn_switch ni-1

After you configure the global settings shown in Table 12-3, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet IP Interface Settings

Configure the following Ethernet interface settings to the values shown in Table 12-4.

Table 12-4 Ethernet Values

Setting	Command
Protocol	set ether0 ipx enable
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0
IPX network	set ether0 ipxnet F1
IPX frame type	set ether0 ipxframe ethernet_802.2
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 12-4, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring ISDN Port Settings

Configure the ISDN port with the values shown in Table 12-5 for the example in this chapter. This example assumes that the BRI used is port S1-S2 on a PortMaster ISDN Office Router (OR-U). If your application uses ports S10 through S29 on a PortMaster 2E, adjust these values accordingly

Table 12-5 ISDN Port Values

Setting	Command
Port type S1	set s1 network twoway
Port type S2	set s2 network twoway
Dial group S1	set s1 group 2
Dial group S2	set s2 group 2
Directory number S1	set s1 directory number 5551111
Directory number S2	set s2 directory number 7005551112
SPID S1	set s1 spid 700555111100
SPID S2	set s2 spid 700555111201

All the other parameters should be left at their default values.

After you configure the ISDN BRI port as shown in Table 12-5, enter the following commands to reset the ports and save the configuration:

```
Command> reset s1
Command> reset s2
Command> save all
```

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring a Dial-In User

A user account must be set up on the PortMaster router in Denver so that PortMaster in San Francisco can dial in when traffic is queued. The new user **sf** should be configured with the values shown in Table 12-6.

Table 12-6 User Table Values

Setting	Command
Username	add netuser sf
Password	set user sf password anypasswd
Protocol	set user sf protocol ppp

Table 12-6 User Table Values (Continued)

Setting	Command
User IP address	set user <i>sf</i> address 192.168.100.1
Netmask	set user <i>sf</i> netmask 255.255.255.0
IPX network	set user <i>sf</i> ipxnet F3
RIP routing	set user <i>sf</i> rip on
MTU	set user <i>sf</i> mtu 1500
Compression	set user <i>sf</i> compression on

After you configure the user table as shown in Table 12-6, enter the following command to save the configuration:

Command> **save all**

For more information about configuring user table parameters, refer to Chapter 7, “Configuring Dial-In Users.”

Configuring a Dial-Out Location

A location entry on the PortMaster in Denver must be created for the location identified as **sf**. This allows the PortMaster router in Denver to call the PortMaster in San Francisco when network traffic is queued. The new location **sf** should be configured with the values shown in Table 12-7.

Table 12-7 Location Table Values

Setting	Command
Location name	add location <i>sf</i>
Type	set location <i>sf</i> manual (Set the location for manual dialing until after the configuration has been tested. Once the configuration is verified, change the connection type to on-demand.)
Protocol	set location <i>sf</i> protocol <i>ppp</i>
IP destination	set location <i>sf</i> destination 192.168.100.1
Netmask	set location <i>sf</i> netmask 255.255.255.0

Table 12-7 Location Table Values (Continued)

Setting	Command
IPX network	set location sf ipxnet F3
RIP routing	set location sf rip on
MTU	set location sf mtu 1500
Idle timer	set location sf idle 2
Dial group	set location sf group 2
Username	set location sf username sf
Telephone number	set location sf telephone 5551212
Password	set location sf password anypasswd
High-water mark	set location sf high_water 0
Maximum ports	set location sf maxports 1



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

After you configure location table settings as shown in Table 12-7, enter the following command to save the configuration:

Command> **save all**

For more information about configuring location table parameters, refer to Chapter 8, “Configuring Dial-Out Connections.”

Configuring the PortMaster in San Francisco

The PortMaster in San Francisco is being configured for an ISDN dial-up connection to the PortMaster in Denver.

Configuring Global Settings

Configure the global settings to the values shown in Table 12-8.

Table 12-8 Global Values

Setting	Command
IP gateway	set gateway <i>192.168.1.2</i> (This is the address of the next upstream router.)
Default routing	set default <i>off</i>
System name	set sysname <i>sf</i>
ISDN switch	set isdn_switch <i>ni-1</i>

After you configure the global settings shown in Table 12-8, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet settings to the values shown in Table 12-9.

Table 12-9 Ethernet Value

Setting	Command
Protocol	set ether0 ipx enable
IP address	set ether0 address <i>192.168.100.1</i>
Netmask	set ether0 netmask <i>255.255.255.0</i>
IPX network	set ether0 ipxnet <i>F2</i>
IPX frame type	set ether0 ipxframe <i>ethernet_802.2</i>
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 12-9, enter the following command to save the configuration:

```
Command> save all
```

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring ISDN Port Settings

Configure the ISDN port with the values shown in Table 12-10 for the example in this chapter. This example assumes that the BRI used is port S1-S2 on a PortMaster ISDN Office Router (OR-U). If your application uses ports S10 through S29 on a PortMaster 2E, adjust these values accordingly.

Table 12-10 ISDN Port Values

Setting	Command
Port type S1	set s1 network twoway
Port type S2	set s2 network twoway
Dial group S1	set s1 group 2
Dial group S2	set s2 group 2
set directory number S1	set s1 directory number 5552222
set directory number S2	set s2 directory number 5552223
SPID S1	set s1 spid 700555222200
SPID S2	set s2 spid 7005552222301

All the other settings should be left at their default values.

After you configure the synchronous WAN port as shown in Table 12-10, enter the following commands to reset the ports and save the configuration:

```
Command> reset s1  
Command> reset s2  
Command> save all
```

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring a Dial-In User

A user account must be set up on the PortMaster router in San Francisco so that PortMaster in Denver can dial in when traffic is queued. The new user **denver** should be configured with the values shown in Table 12-11.

Table 12-11 User Table Values

Setting	Command
Username	add netuser <i>denver</i>
Password	set user <i>denver</i> password <i>anypasswd</i>
Protocol	set user <i>denver</i> protocol <i>ppp</i>
User IP address	set user <i>denver</i> address <i>192.168.200.1</i>
Netmask	set user <i>denver</i> netmask <i>255.255.255.0</i>
IPX network	set user <i>denver</i> ipxnet <i>F3</i>
RIP routing	set user <i>denver</i> rip on
MTU	set user <i>denver</i> mtu <i>1500</i>
Compression	set user <i>denver</i> compression on

After you configure the user table as shown in Table 12-11, enter the following command to save the configuration:

Command> **save all**

For more information about configuring user table parameters, refer to Chapter 7, “Configuring Dial-In Users.”

Configuring a Dial-Out Location

A location entry on the PortMaster in San Francisco must be created for the location identified as **denver**. This allows the PortMaster router in San Francisco to call the PortMaster in Denver when network traffic is queued. The new location **denver** should be configured with the values shown in Table 12-12.

Table 12-12 Location Table Values

Setting	Command
Location name	add location <i>denver</i>
Type	set location <i>denver manual</i> (Set the location for manual dialing until after the configuration has been tested. Once the configuration is verified, change the connection type to on-demand.)
Protocol	set location <i>denver ppp</i>
IP destination	set location <i>denver destination</i> 192.168.200.1
Netmask	set location <i>denver netmask</i> 255.255.255.0
IPX network	set location <i>denver ipxnet</i> F3
RIP routing	set location <i>denver rip</i> on
MTU	set location <i>denver mtu</i> 1500
Idle timer	set location <i>denver idle</i> 2
Dial group	set location <i>denver group</i> 2
Username	set location <i>denver username</i> sf
Telephone number	set location <i>denver telephone</i> 5551212
Password	set location <i>denver password</i> anypasswd
High-water mark	set location <i>denver high_water</i> 0
Maximum ports	set location <i>denver maxports</i> 1



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

After you configure location table settings as shown in Table 12-12, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring location table parameters, refer to Chapter 8, “Configuring Dial-Out Connections.”

Use the dialer to connect between the two offices as instructed in the next section. Once everything is working properly, you can change the location type from manual to on-demand on both routers and reset the ports.

Testing the Setup

You should test the configuration before setting either of the locations for on-demand dialing. To test the configuration, follow these steps:

1. Enter the following commands on the PortMaster in Denver to connect from location *denver* to location *sf*:

```
Command> set console s1  
Command> set debug 0x51  
Command> set debug isdn on  
Command> dial sf
```

2. Monitor the dial-and-connect sequence between the two locations.

3. If everything connects as expected, do the following:

- a. Turn off debugging on the console.

```
Command> set debug isdn off  
Command> reset console
```

- b. Reset the port on the Office Router in Denver and change the location type of location *sf* to on-demand.

```
Command> reset s1  
Command> set location sf on_demand
```

4. **If you notice a problem, do the following:**
 - a. Reset the port on the PortMaster in Denver.
 - b. Change the settings you think are causing the problem.
 - c. Dial San Francisco again.
 - d. Repeat this procedure until the connection is made correctly.
5. **Repeat Steps 1 through 4, dialing from San Francisco to Denver.**

Troubleshooting an ISDN BRI Connection

Most ISDN configurations come up with little trouble if you have configured the PortMaster using information from your telephone company. However, if you are having problems, use the information in this section to try to debug your configuration.

To display ISDN debug information on the console, enter the following commands:

```
Command> set console s1  
Command> set debug isdn on
```

To turn off debugging, enter the following commands:

```
Command> set debug isdn off  
Command> reset console
```

If you are having trouble with an ISDN connection, verify the following:

- The error counters should be 0 except for a small number of abnormal termination errors resulting from plugging cables in or out. If your error counters are nonzero, the problem is external to the PortMaster.
- Verify that you are using the correct cables and that they are attached securely to the correct port.
- Verify that the ISDN status LED is on solid; otherwise, refer to the hardware configuration guide for more information. This LED indicates connectivity to the ISDN switch.
- Verify your configuration as described in this chapter.
- Contact your carrier to review the ISDN switch type, SPIDs, and the status of their line.

- To view the PPP negotiation, enter the following commands:

```
Command> set console
Command> set debug 0x51
```

For more information about the interpreting the results of the debug command, refer to the *PortMaster Troubleshooting Guide*.

After you verify that the PPP negotiation is correct, enter the following commands to turn off the debug utility:

```
Command> set debug off
Command> reset console
```

Interpreting ISDN BRI Port Status

Table 12-13 describes how to interpret the output of the **show S10** command for ISDN BRI ports.

Table 12-13 ISDN BRI Port Status

Port Status	Modem Status	Description
NO-SERVICE	DCD- CTS- TELCO- NT1-	No SPID is set.
NO-SERVICE	DCD- CTS- TELCO- NT1+	Port has either no cable or no circuit connecting it to the telephone company.
NO-SERVICE	DCD- CTS+ TELCO+ NT1+	Cable and ISDN circuit are functioning, but the SPID is not registered.
IDLE	DCD- CTS+ TELCO+ NT1+	SPID is registered and ready to use
ESTABLISHED	DCD- CTS+ TELCO+ NT1+	Port is connecting or providing device service, but no carrier is sensed.
ESTABLISHED	DCD+ CTS+ TELCO+ NT1+	Port is connected.
ESTABLISHED	DCD+ CTS- TELCO+ NT1+	Port is connected with a V.120 asynchronous connection, but the other end of the connection is providing flow control information.

Frame Relay is a method of encapsulating network information that allows for fast delivery and high line utilization. PortMaster routers support Frame Relay over synchronous ports.

This chapter uses an example to demonstrate how to configure the PortMaster to connect to a synchronous line using Frame Relay. This chapter also explains how to configure Frame Relay subinterfaces

The following topics are discussed:

- “Overview of Frame Relay” on page 13-1
- “Frame Relay Configuration on the PortMaster” on page 13-4
- “Configuration Steps for a Frame Relay Connection” on page 13-7
- “Troubleshooting a Frame Relay Configuration” on page 13-11
- “Frame Relay Subinterfaces” on page 13-12

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Frame Relay

Synchronous ports on PortMaster products can be configured to support Frame Relay connections. As opposed to a dedicated or leased line, a Frame Relay connection can be thought of as a virtual switch.

Frame Relay is a switched digital service that supports multiple virtual circuits, simultaneously connected to a site by a single physical circuit. Each site requires only one physical circuit into the Frame Relay network—usually referred to as a cloud—but can have several virtual circuits to reach other sites attached to the cloud.

PVCs and DLCIs

PortMaster products support permanent virtual circuits (PVCs). PVCs are used to form a connection between any two devices attached to a Frame Relay cloud. Each PVC is given a unique number on each physical circuit along the path between the two devices. This unique number is called a data link connection identifier (DLCI). The DLCI is automatically changed to the PVC number of the next physical circuit as it passes through each switch along the path. A DLCI is different from a network address because it identifies a circuit in both directions, not a particular endpoint. A frame contains only one DLCI, not a source and destination.

In general, the only DLCI numbers you see are those numbers assigned to the physical circuits on the perimeter of the Frame Relay cloud.

Line Speed

The physical circuit between point A and the network must be ordered with a certain line speed. This speed is the physical maximum bandwidth for your connection to the Frame Relay network. Expansion beyond this limit is not possible without a hardware change and a new circuit installation.

Port Speed

The connection into the telecommunications provider's Frame Relay network must be ordered at a particular port speed, which is the maximum bandwidth rate that the telecommunications provider accepts from your connection. This number must be less than or equal to the line speed. This speed is the maximum rate at which you can transmit data to any of your PVCs under any circumstances. The port speed differs from line speed only in that it can be upgraded through software without a circuit installation or hardware change.

CIR and Burst Speed

Each PVC has a property known as committed information rate (CIR), which represents the guaranteed minimum bandwidth available to the particular PVC under all conditions. In some implementations, an additional property can be assigned to a PVC, known as "burst speed" or "maximum burst." This speed represents the highest rate at which data is allowed to flow over a given PVC, regardless of bandwidth availability.

Discarding Frames

The PortMaster pushes as much data out of the serial port as it can at port speed for any PVC that has traffic, regardless of CIR. The Frame Relay switch passes as much of the data as possible on to the next link. However, once a particular PVC has transmitted its CIR-worth of bits each second, the switch marks any additional frames as “discard eligible.” If the switch receives more frames than it can pass along, the frames are automatically discarded in the following order:

- Frames that would be marked discard eligible even if they are forwarded
- Frames received that were marked as discard eligible

If the switch must discard other frames, the behavior is undefined. In this case, the Frame Relay network is improperly configured because the CIR total exceeds the line speed or port speed.

Ordering Frame Relay Service

In general, when ordering Frame Relay service for a private network, order large-bandwidth physical circuits (T1) with port speed appropriate to your application, and a CIR that is high enough to provide minimally acceptable performance for your application. In most cases, ordering according to these criteria provides service that is close to your port speed. The CIR is a guaranteed minimum throughput, not a maximum limit. Port speed is the maximum limit.

LMI Types

The following Frame Relay terms relate to network management. The Frame Relay specification supports automatic network status updates, which are exchanged between adjacent devices in the Frame Relay network. These status updates are known as the Local Management Interface (LMI). Two forms of LMI are available in the PortMaster: Cisco/Stratacom LMI, which is commonly referred to as LMI, and ANSI T1.617 Annex D LMI, which is commonly referred to as Annex-D.

Generally, your telecommunications provider offers three LMI options for your physical circuit: LMI, Annex-D, or none. Because LMI exists only between your router and the switch to which your physical circuit connects, it does not need to match what the remote ends of your PVCs are using. However, your circuit LMI must match the configuration on your PortMaster. Generally, Annex-D is recommended, because it is a more feature-rich and robust version of LMI.

Frame Relay Configuration on the PortMaster

You configure Frame Relay by selecting the Frame Relay protocol, setting the IP address of the port, and specifying the DLCIs during the synchronous port configuration.

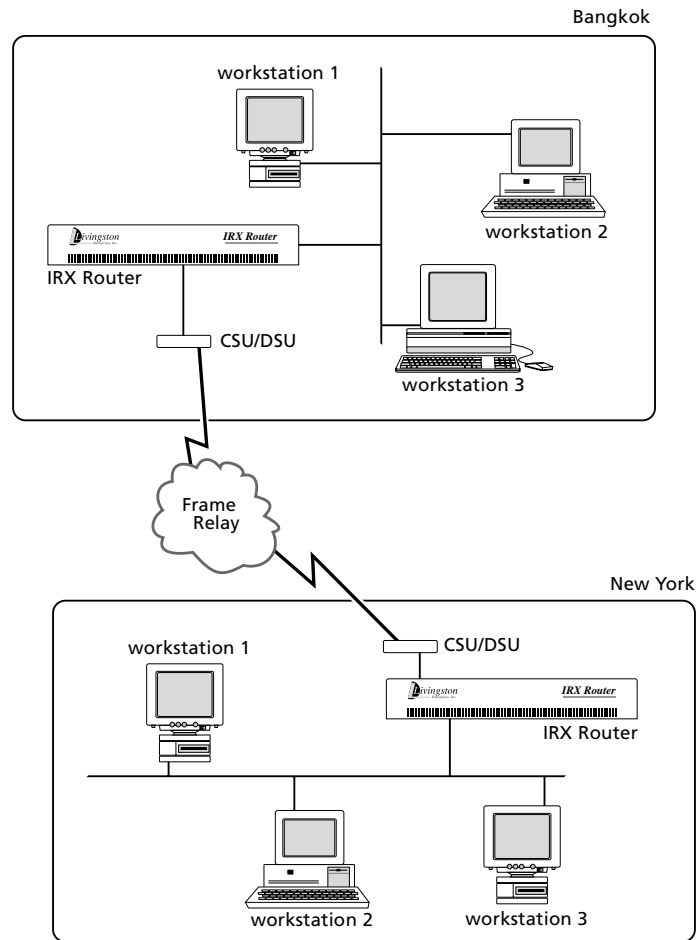
Alternatively, the PortMaster can discover DLCIs dynamically with LMI or Annex-D and learn the IP addresses of the other routers through Inverse ARP if the other routers on your Frame Relay cloud support Inverse ARP as specified in RFC 1490. In this configuration, the PortMaster sends an LMI status request every 10 configurable seconds by default. Every sixth request is a full status request, and the others are keepalives. In this configuration, the port state is `CONNECTING` until it receives three replies from the switch; then the port state becomes `ESTABLISHED`. After six unanswered requests, the PortMaster resets the port.

Figure 13-1 shows an example of a Frame Relay connection.



Note – All synchronous ports require an external clock signal to regulate the port speed.

Figure 13-1 Frame Relay Configuration



11820004

Enabling LMI

You can specify whether the PortMaster accepts Local Management Interface (LMI) frames from the attached Frame Relay switch. If LMI is enabled on the switch, you must enable LMI on the PortMaster. The default keepalive value is 10 seconds. However, if your telephone company chooses another keepalive value, change this value as they instruct you. Enabling LMI causes the DLCI list to be completed automatically. If the attached switch uses an interval keepalive timer different from the Frame Relay default, be sure the keepalive timer on the PortMaster matches that of the attached switch.



Note – Contact your Frame Relay carrier to determine which keepalive they are using, LMI or Annex-D.

To enable LMI, use the following command:

```
Command> set W1 lmi Seconds
```

Enabling Annex-D

The PortMaster also accepts the Annex-D polling interval. The Annex-D default value is 10 seconds. However, if your telephone company chooses another keepalive value, change this value as they instruct you. Enabling LMI causes the DLCI list to be completed automatically. Setting the keepalive value to 0 (zero) seconds, or enabling LMI, disables Annex-D.



Note – Contact your Frame Relay carrier to determine which keepalive they are using, LMI or Annex-D.

To enable Annex-D, use the following command:

```
Command> set W1 annex-d Seconds
```

Listing DLCIs for Frame Relay Access

If LMI or Annex-D is not used, you must enter the DLCI list manually. The DLCI list is a list of DLCIs that are accessible through the Frame Relay network by this interface. The PortMaster uses Inverse ARP to learn the IP addresses of routers attached to the PVCs represented by the specified DLCIs, if those routers support Inverse ARP. Alternatively, you can specify IP addresses by appending a colon (:) and IP address after the DLCI.

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

To enter the DLCI list manually, use the following command:

```
Command> set W1 dlci DlcI_list
```

For information on Frame Relay subinterfaces see “Frame Relay Subinterfaces” on page 13-12.

Configuration Steps for a Frame Relay Connection

The example described in this chapter connects a PortMaster router located in a main office (Bangkok) with a PortMaster router located in a branch office (New York) using Frame Relay on a synchronous interface.

To install your PortMaster, follow the instructions in the hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

- 1. Configure the following settings for the PortMaster in Bangkok:**
 - a. Configure global settings (page 13-8).
 - b. Configure Ethernet interface settings (page 13-8).
 - c. Configure synchronous port settings (page 13-9).
- 2. Configure the following settings for the PortMaster in New York:**
 - a. Configure Ethernet interface settings (page 13-10).
 - b. Configure synchronous port settings (page 13-10).
- 3. Troubleshoot the configuration (page 13-11).**

You can additionally configure Frame Relay subinterfaces. For information on Frame Relay subinterfaces see “Frame Relay Subinterfaces” on page 13-12.



Note – You must configure the Ethernet interface before configuring the PortMaster for a Frame Relay connection. Refer to Chapter 4, “Configuring the Ethernet Interface,” for more information.

Configuring the PortMaster in Bangkok

Configure the settings for the PortMaster in Bangkok with the values in the following sections.

Configuring Global Settings

Configure the global settings on the PortMaster in Bangkok to the values shown in Table 13-1.

Table 13-1 Global Values

Parameter	Command
Gateway	set gateway 192.168.20.2

After you configure the global settings shown in Table 13-1, enter the following command to save the configuration:

Command> **save all**

For more information about global parameters, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet interface settings on the PortMaster in Bangkok to the values shown in Table 13-2.

Table 13-2 Ethernet Values

Parameter	Command
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0

After you configure the Ethernet interface as shown in Table 13-2, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet parameters, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Parameters

Configure the synchronous WAN port W1 to the values shown in Table 13-3.

Table 13-3 Synchronous WAN Port Values

Setting	Command
Port type	set w1 network <i>hardwired</i>
Protocol	set w1 protocol <i>frame</i>
Port IP address	set w1 address <i>192.168.20.1</i>
Netmask	set w1 netmask <i>255.255.255.0</i>
Modem control	set w1 cd on
RIP routing	set w1 rip <i>broadcast</i>
Annex-D	set w1 annex-d <i>10</i> (LMI can be used instead of Annex-D.)
DLCI list	set w1 dlci <i>16:192.168.20.2</i> (You do not need to set a DLCI list if the remote router supports Inverse ARP.)

After you configure the synchronous WAN port as shown in Table 13-3, enter the following commands to reset the port and save the configuration:

```
Command> reset w1  
Command> save all
```

For more information on synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring the PortMaster in New York

Configure the settings for the PortMaster in New York with the values in the following sections. You do not need to specify a gateway for the PortMaster in New York because it is on the Internet.

Configuring Ethernet Interface Settings

Configure the Ethernet interface settings to the values shown in Table 13-4.

Table 13-4 Ethernet Values

Setting	Command
IP address	set ether0 address 92.168.1.1
Netmask	set ether0 netmask 255.255.255.0
Broadcast address	set ether0 broadcast <i>high</i>
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 13-4, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet parameters, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Settings

Configure the synchronous WAN port W1 to the values shown in Table 13-5.

Table 13-5 WAN Port Parameter Values

Setting	Command
Port type	set w1 network <i>hardwired</i>
Protocol	set w1 protocol <i>frame</i>
Port IP address	set w1 address 92.168.1.20.2
Netmask	set w1 netmask 255.255.255.0
Modem control	set w1 cd on
RIP routing	set w1 rip <i>listen</i>
Annex-D	set w1 annex-d 10 (LMI can be used instead of Annex-D)

Table 13-5 WAN Port Parameter Values (Continued)

Setting	Command
DLCI list	set w1 dlci 16:192.168.20.1 (You do not need to set a DLCI list if the remote router supports Inverse ARP.)

After you configure the synchronous WAN port as shown in Table 13-5, enter the following commands to reset the port and save the configuration:

```
Command> reset w1  
Command> save all
```

If LMI or Annex-D is set, the PortMaster receives DLCI information in the full status update messages from the Frame Relay switch. The PortMaster then attempts to discover IP addresses of other routers using Inverse ARP. You can set DLCI lists statically as well. The **show arp frm1** command lists both the static and dynamic DLCI lists for the S1 port.

If Annex-D is available from your carrier for a new connection, it is preferable to LMI.

To connect to Cisco routers using Frame Relay, the Cisco router must be set to use **encapsulation frame-relay ietf** for the serial interface; otherwise, the Cisco **frame-relay map** command for your DLCI must have the **ietf** keyword appended.

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Troubleshooting a Frame Relay Configuration

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you are having problems, use the information in this section to debug your configuration.

If you are having trouble with a Frame Relay connection, do the following:

- Wait a few moments. The process of establishing a Frame Relay link, learning the DLCI list, and learning the IP address through Inverse ARP can sometimes take a few moments.
- The error counters should be 0 except for abort errors. If your counters are nonzero, the problem is external to the PortMaster.

- Verify that you are using the correct cables and that they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Lucent cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing the clock signal to the PortMaster. The CSU/DSU can generate the clock signal or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- Enter the following two commands to view the LMI or Annex-D keepalives:

```
Command> set console s1  
Command> set debug 0x51
```

After you verify that the proper keepalives are being received, enter the following commands to turn off the debug utility:

```
Command> set debug off  
Command> reset console
```

- If you have a Cisco router on the other end of your connection, verify that it is set for **encapsulation frame-relay ietf** for the serial interface; otherwise, the Cisco **frame-relay map** command for your DLCI must have the **ietf** keyword appended.

Frame Relay Subinterfaces

PortMaster routers support a feature called DLCI bundling to allow the splitting of one synchronous port with multiple DLCIs into a maximum of 32 Frame Relay subinterfaces. In this configuration, the DLCIs are divided between the subinterfaces through the use of the location table and the DLCI table. Each subinterface must have its own subnet or assigned network. The PortMaster has a limit of 512 total active interfaces, which can be further limited by available memory.

The port you are configuring must be set for network hardwired use and Frame Relay, and must be in the same dial group as the location.

Configuring Subinterfaces

The following sections describe how to configure a Frame Relay subinterface.

Adding a Location

To configure a Frame Relay subinterface, you add a location for each interface, configure it with the frame protocol, and associate it with a dial group. Then associate a synchronous port with the same dial group. For example, to create a location called **sub1**, enter the following commands:

```
Command> add location sub1
Command> set location sub1 protocol frame
Command> set location sub1 group 1
Command> set s1 group 1
```

The rest of the location table entries are set as described in Chapter 8, “Configuring Dial-Out Connections,” including setting an IP address, routing, and filtering for each interface.

Creating a DLCI Entry

The next step in configuring the subinterfaces is to create an entry in the DLCI table. Entries can be followed with an optional IP address or hostname. The keyword **ipxdlci** is available for IPX networks.

To create a DLCI table entry for the subinterface **sub1**, enter the following commands:

```
Command> add ipdlci sub1 16
Command> add ipdlci sub1 19 192.168.2.19
Command> add ipdlci sub1 20 192.168.2.20
Command> add ipxdlci sub1 21 0e0a001e
```

To remove an entry, enter the following commands:

```
Command> delete dlci sub1
Command> delete ipxdlci sub1 21
```

Displaying DLCI Entries

DLCI entries that are added or deleted are linked to the location table. Use the **show location Locname** command to display the DLCI entries.

Troubleshooting Subinterfaces

Packets received on a subinterface can be identified as belonging to that subinterface only if the DLCI is properly entered in the DLCI table for that location. If you are having problems, do the following:

- Wait a few moments. Subinterfaces come up after the primary interface. This process can take a few moments.
- Check the list of DLCIs tied to each location using the **show location** *Locname* command.
- Verify the DLCI list on a location using the **show arp** *Interface* command, replacing *Interface* with the name of the interface. A list of interfaces can be shown with the **ifconfig** command.
- Always reset the port after changing the DLCI list.
- Verify that all DLCIs are accounted for by checking the DLCI list for your primary interface. If you enter the wrong DLCI for the subinterface, the DLCI for the subinterface is applied to the primary interface if LMI or Annex-D is in use.
- Enter the following two commands to view the LMI or Annex-D keepalives:

```
Command> set console s1
```

```
Command> set debug 0x51
```

After you verify that the proper keepalives are being received, enter the following commands to turn off the debug utility:

```
Command> set debug off
```

```
Command> reset console
```

- If you have a Cisco router on the other end of your connection, verify that it is set for **encapsulation frame-relay ietf** for the serial interface; otherwise, the Cisco **frame-relay map** command for your DLCI must have the **ietf** keyword appended.

Example: Configuring a Frame Relay Subinterface

This set of example commands configures a PortMaster IRX-111 router with Frame Relay packets coming into port S1 with DLCIs 16, 17, and 18. Port S1 has already been configured for Frame Relay, so that portion is not shown here. The following commands split the Frame Relay port into a primary subinterface for DLCI 18 and a secondary subinterface for DLCIs 16 and 17.

```
Command> set s1 group 1

Command> add location sub1
Command> set location sub1 protocol frame
Command> set location sub1 group 1
Command> set location sub1 address 192.168.3.1
Command> set location sub1 netmask 255.255.255.0
Command> set location sub1 rip on

Command> add dlci sub1 16
Command> add dlci sub1 17

Command> save all
Command> reset s1
```


This chapter uses an example to demonstrate how to configure the PortMaster to connect two local area networks (LANs) via synchronous V.25bis dialing applications such as ISDN, terminal adapters, or switched 56Kbps.

This chapter discusses the following topics:

- “Overview of Synchronous V.25bis Dial-Up Connections” on page 14-1
- “Configuration Steps for a Synchronous V.25bis Connection” on page 14-3
- “Troubleshooting a Synchronous V.25bis Connection” on page 14-13

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Synchronous V.25bis Dial-Up Connections

PortMaster products support dial-on-demand ISDN and switched 56Kbps connections using synchronous ports and the PPP protocol. ISDN speeds of up to 64Kbps are possible with an outside carrier and an external terminal adapter (TA). Speeds of up to 128Kbps are possible if the terminal adapter supports B channel bonding. Contact your service provider for specific information about the required terminal adapter.

Switched 56Kbps connections require an external CSU/DSU. ISDN and switched 56Kbps connections can be initiated on an as-needed basis or they can remain active all the time. A dial-out location must be specified in the location table for dial-out connections, and a dial-in user must be specified in the user table for dial-in connections. PAP is available for dial-in authentication, when a router dials in to your PortMaster. CHAP is available for dial-in and dial-out authentication.

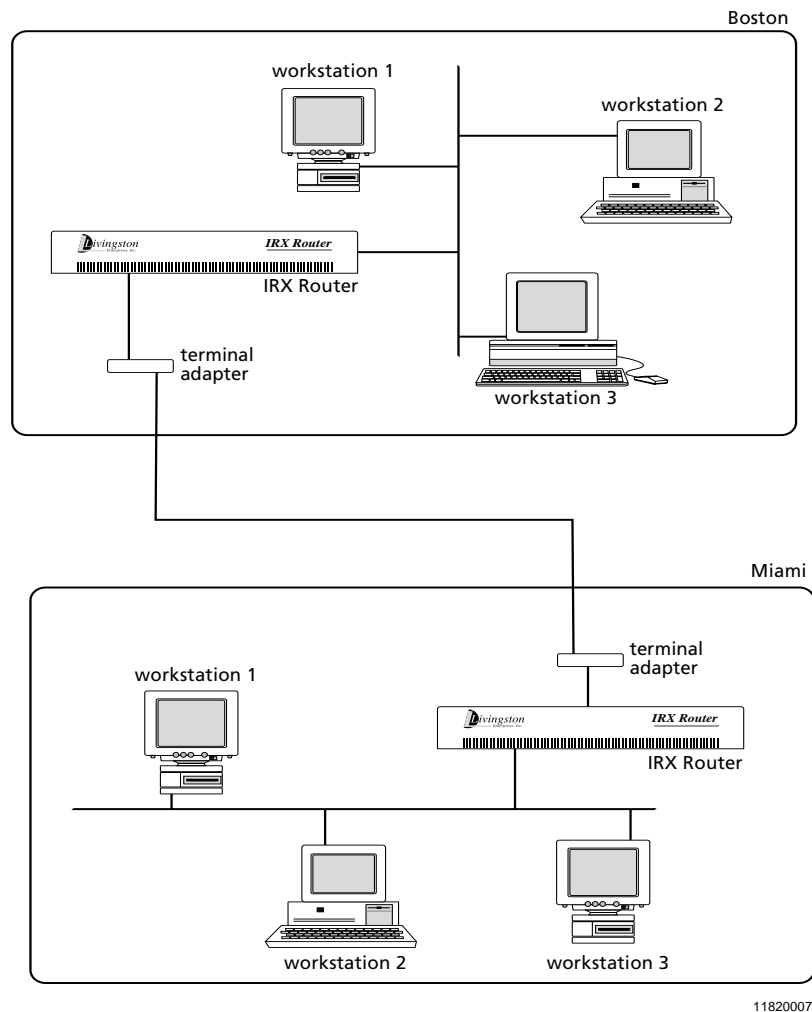
When connecting an asynchronous ISDN terminal adapter to an asynchronous port using AT commands to dial, configure the PortMaster just as you would for a modem. Refer to Chapter 15, “Using Office-to-Office Connections,” and Chapter 16, “Using Internet Connections,” for more information.

In this configuration, keep in mind that a 115.2Kbps asynchronous DTE rate can support only a single 64Kbps B channel, because a byte of asynchronous data requires 10 bits—including stop and start bits—for transmission, but a byte of synchronous data

requires only 8 bits. A 115.2Kbps DTE rate cannot properly support two 64Kbps B channels because the terminal adapter is unable to buffer the excess data when the incoming data for an ISDN line is 128Kbps.

Figure 14-1 shows an example of an ISDN or switched 56Kbps connection.

Figure 14-1 Example of an ISDN or Switched 56Kbps Connection



Configuration Steps for a Synchronous V.25bis Connection

This example connects a PortMaster located in Boston with a PortMaster located in Miami using a synchronous interface that is initiated on-demand by an ISDN or switched 56Kbps connection.

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the installation guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

1. Configure the following settings for the PortMaster in Boston:

- a. Global settings (page 14-4)
- b. Ethernet interface settings (page 14-4)
- c. Synchronous port settings (page 14-5)
- d. Dial-in users (page 14-5)
- e. Dial-out locations (page 14-6)

2. Configure the following settings for the PortMaster in Miami:

- a. Global settings (page 14-8)
- b. Ethernet interface settings (page 14-8)
- c. Synchronous port settings (page 14-9)
- d. Dial-in users (page 14-10)
- e. Dial-out locations (page 14-11)

3. Test the configuration (page 14-12).

4. Troubleshoot the configuration (page 14-13).

Configuring the PortMaster in Boston

The PortMaster in Boston is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Miami.

Configuring Global Settings

Configure the global settings to the values shown in Table 14-1.

Table 14-1 Global Values

Setting	Command
IP gateway	set gateway <i>192.168.1.1</i>
System name	set sysname <i>boston</i>

After you configure the global settings shown in Table 14-1, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet interface settings to the values shown in Table 14-2.

Table 14-2 Ethernet Values

Setting	Command
IP address	set ether0 address <i>192.168.200.1</i>
Netmask	set ether0 netmask <i>255.255.255.0</i>
IPX network	set ether0 ipxnet <i>F1</i>
IPX frame type	set ether0 ipxframe ethernet_802.2
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 14-2, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Settings

Configure the synchronous WAN port parameters with the values shown in Table 14-3.

Table 14-3 Synchronous WAN Port Values

Setting	Command
Port type	set w1 network twoway
Modem control	set w1 cd on
Dial group	set w1 group 1

After you configure the synchronous WAN port as shown in Table 14-3, enter the following commands to reset the port and save the configuration:

```
Command> reset w1  
Command> save all
```

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring a Dial-In User

A user account must be set up on the PortMaster router in Boston so the PortMaster in Miami can dial in when traffic is queued. The new user *miami* should be configured on the PortMaster router in Boston with the values shown in Table 14-4.

Table 14-4 User Table Values

Setting	Command
Username	add netuser miami
Password	set user miami password anypasswd
Protocol	set user miami protocol ppp
User IP address	set user miami destination 192.168.1.1
Netmask	set user miami netmask 255.255.255.0

Table 14-4 User Table Values (Continued)

Setting	Command
IPX network	set user <i>miami</i> ipxnet F3
RIP routing	set user <i>miami</i> rip on
MTU	set user <i>miami</i> mtu 1500

After you configure user table settings as shown in Table 14-4, enter the following command to save the configuration:

Command> **save all**

No compression is used on synchronous lines. For more information about configuring user table settings, refer to Chapter 7, “Configuring Dial-In Users.”

Configuring a Dial-Out Location

A location entry on the PortMaster in Boston must be created for the location identified as *miami*. This allows the PortMaster in Boston to call the PortMaster in Miami when network traffic is queued. The new location *miami* should be configured on the router in Boston with the values shown in Table 14-5.

Table 14-5 Location Table Values

Setting	Command
Location name	add location <i>miami</i>
Type	set location <i>miami</i> manual (Set the location for manual dialing until after the configuration has been tested. Once the configuration is verified, change the connection type to on-demand.)
Protocol	set location <i>miami</i> ppp
IP destination	set location <i>miami</i> destination 192.168.1.1
Netmask	set location <i>miami</i> netmask 255.255.255.0
IPX network	set location <i>miami</i> ipxnet F3
RIP routing	set location <i>miami</i> rip on
MTU	set location <i>miami</i> mtu 1500

Table 14-5 Location Table Values (Continued)

Setting	Command
Idle timer	set location <i>miami</i> idle 5
Dial group	set location <i>miami</i> group 1
Username	set location <i>miami</i> username <i>miami</i>
Telephone number	set location <i>miami</i> telephone 5551212
Password	set location <i>miami</i> password <i>anypasswd</i>
High-water mark	set location <i>miami</i> high_water 0
Maximum ports	set location <i>miami</i> maxports 1



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

After you configure location table settings as shown in Table 14-5, enter the following command to save the configuration:

Command> **save all**

For more information about configuring location table settings, refer to Chapter 8, “Configuring Dial-Out Connections.”

Configuring the PortMaster in Miami

The PortMaster in Miami is being configured for a V.25bis dial-up synchronous connection to the PortMaster in Boston.

Configuring Global Settings

Configure the following global settings to the values shown in Table 14-6.

Table 14-6 Global Value

Setting	Command
IP gateway	set gateway <i>192.168.1.2</i> (This is the address of the next upstream router.)
Default routing	set default on
System name	set sysname <i>miami</i>

After you configure the global settings shown in Table 14-6, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet settings to the values shown in Table 14-7.

Table 14-7 Ethernet Values

Setting	Command
Protocol	set ether0 ipx enable
IP address	set ether0 address <i>192.168.1.1</i>
Netmask	set ether0 netmask <i>255.255.255.0</i>
IPX network	set ether0 ipxnet <i>F2</i>
IPX frame type	set ether0 ixpframe ethernet_802.2
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 14-7, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Settings

Configure the synchronous WAN port with the values shown in Table 14-8.

Table 14-8 Synchronous WAN Port Values

Setting	Command
Port type	set w1 network twoway
Transport protocol	set w1 protocol ppp
Netmask	set w1 netmask 255.255.255.0
Modem control	set w1 cd on
Group	set w1 group 1

After you configure the synchronous WAN port as shown in Table 14-8, enter the following commands to reset the port and save the configuration:

Command> **reset w1**
Command> **save all**

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring a Dial-In User

A user account must be set up on the PortMaster router in Miami so the PortMaster in Boston can dial in when traffic is queued. The new user *boston* should be configured on the PortMaster in Miami with the values shown in Table 14-9.

Table 14-9 User Table Values for Miami

Setting	Command
Username	add netuser <i>boston</i>
Password	set user <i>boston</i> password <i>anypasswd</i>
Protocol	set user <i>boston</i> protocol ppp
User IP address	set user <i>boston</i> address <i>192.168.200.1</i>
Netmask	set user <i>boston</i> netmask <i>255.255.255.0</i>
IPX network	set user <i>boston</i> ipxnet <i>F3</i>
RIP routing	set user <i>boston</i> rip on
MTU	set user <i>boston</i> mtu <i>1500</i>

No compression is used on synchronous lines.

After you configure user table settings as shown in Table 14-9, enter the following command to save the configuration:

Command> **save all**

For more information about configuring user table parameters, refer to Chapter 7, “Configuring Dial-In Users.”

Configuring a Dial-Out Location

A location entry on the PortMaster in Miami must be created for the location identified as *boston*. This allows the PortMaster router in Miami to call the PortMaster router in Boston when network traffic is queued. The new location *boston* should be configured on the PortMaster in Miami with the values shown in Table 14-10.

Table 14-10 Location Table Values

Parameter	Command
Location name	add location <i>boston</i>
Type	set location <i>boston</i> manual (Set the location for manual dialing until after the configuration has been tested. Once the configuration is verified, change the connection type to on-demand.)
Protocol	set location <i>boston</i> ppp
IP destination	set location <i>boston</i> destination <i>192.168.200.1</i>
Netmask	set location <i>boston</i> netmask <i>255.255.255.0</i>
IPX network	set location <i>boston</i> ipxnet <i>F3</i>
RIP routing	set location <i>boston</i> rip on
MTU	set location <i>boston</i> mtu <i>1500</i>
Idle timer	set location <i>boston</i> idle <i>5</i>
Dial group	set location <i>boston</i> group <i>1</i>
Username	set location <i>boston</i> username <i>boston</i>
Telephone number	set location <i>boston</i> telephone <i>5551212</i>
Password	set location <i>boston</i> password <i>anypasswd</i>

Testing the Configuration

The configuration should be tested before the location *boston* is set for continuous dialing. To test the configuration, follow these steps:

1. **Enter the following commands to connect from the office in Miami to location *boston*.**

```
Command> set console w1
Command> set debug 0x51
Command> dial boston
```

2. **Monitor the dial-and-connect sequence between the two locations.**

3. **If everything connects as expected, do the following:**

- a. Turn off debugging on the console.

```
Command> set debug off
Command> reset console
```

- b. Reset the port on the Office Router in Miami and change the location type of location *boston* to on-demand.

```
Command> reset w1
Command> set location boston on_demand
```

4. **If you notice a problem, do the following:**

- a. Reset the port.
- b. Check your configuration.
- c. Dial Boston again.
- d. Repeat this procedure until the connection is made correctly.

5. **When you have configured the PortMaster correctly, reset the port and save the configuration.**

```
Command> reset w1
Command> save all
```

Troubleshooting a Synchronous V.25bis Connection

Most synchronous configurations come up with very little trouble if you have configured the PortMaster using information from your carrier. If you have problems, use the information in this section to debug your configuration.

If you are having trouble with a V.25bis dial-up connection to location *Locname*, verify the following:

- The error counters should be 0 except for a small number of abnormal termination errors resulting from plugging cables in or out. If your error counters are nonzero, the problem is external to the PortMaster.
- Verify that you are using the correct cables and that they are attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch is set to V.35 for Lucent cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU or synchronous terminal adapter is providing the clock to the PortMaster. The CSU/DSU or terminal adapter can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU or synchronous terminal adapter is configured properly.
- To view the PPP negotiation, use the following commands:

```
Command> set console w1  
Command> set debug 0x51  
Command> dial Locname
```

For more information about the interpreting the results of the debug command, refer to the “PortMaster Troubleshooting Guide.”

After you verify that the PPP negotiation is correct, enter the following commands to turn off the debug utility:

```
Command> set debug off  
Command> reset console
```

- Contact your carrier to review your configuration and the status of their line.

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

This chapter also briefly describes how to configure multiline load balancing and ISDN BRI on-demand connections for office-to-office use.

The following topics are discussed:

- “Overview of Example Configuration” on page 15-1
- “Configuration Steps for an Office-to-Office Connection” on page 15-3
- “Setting the Console Port for Multiline Load Balancing” on page 15-13
- “Using ISDN for On-Demand Connections” on page 15-15

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Example Configuration

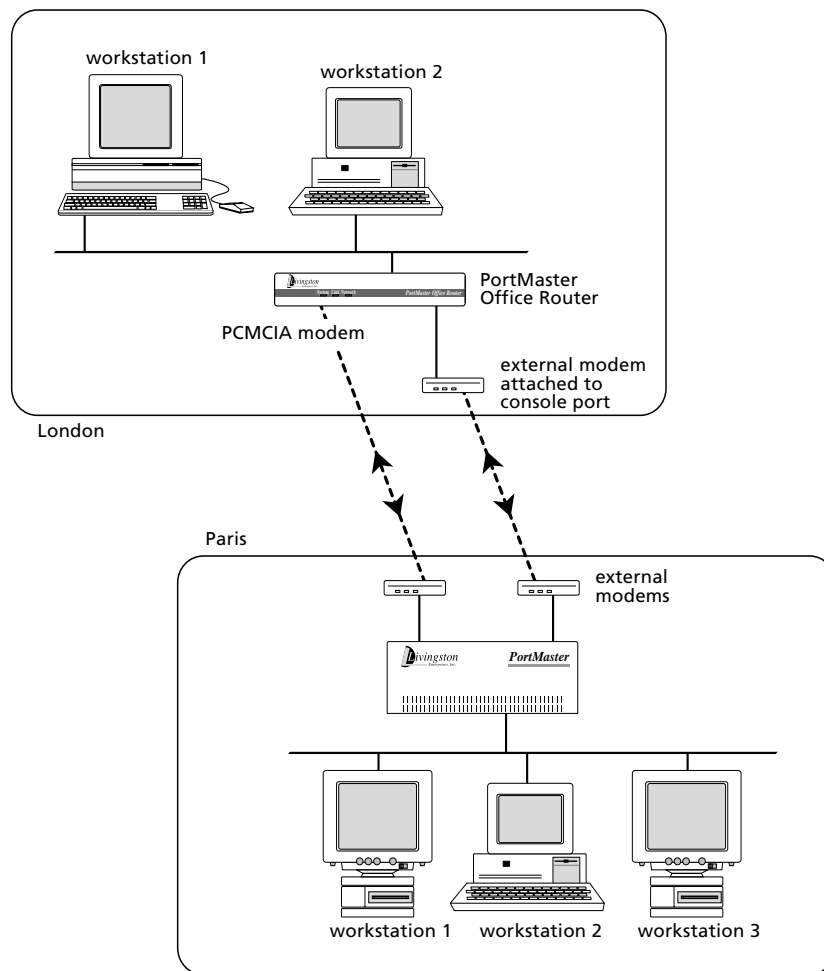
The example described in this chapter connects a PortMaster Office Router located in a branch office in London with a PortMaster 2 in the headquarters in Paris. These models are used as an example; you can use any PortMaster for this configuration.

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

A dial-on-demand link establishes a connection with the specified location when network traffic is queued. The PortMaster PCMCIA Office Router OR-M is designed to support a dial-on-demand connection with another office using the PCMCIA modem port S1. Figure 15-1 shows an example of this configuration. The console port S0 can be

used as a console, or with an external modem and a straight-through cable connected, as an additional dial on-demand port for multiline load balancing during peak traffic periods.

Figure 15-1 Office-to-Office Dial-On-Demand Configuration



11820008

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

The example in this chapter uses the PCMCIA asynchronous modem port on the OR-M. To use the ISDN port on the OR-U, see “Using ISDN for On-Demand Connections” on page 15-15.

Configuration Steps for an Office-to-Office Connection

The example described in this chapter connects a PortMaster router located in a branch office (London) with a PortMaster router located in the main office (Paris) using a dial-on-demand modem configuration.

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the installation guide.

Once you have assigned an IP address to the PortMaster, continue with the steps. The following values shown in this chapter apply only to this example; when you are configuring your PortMaster, use values appropriate for your network.

- 1. Configure the following settings for the PortMaster PCMCIA Office Router in the London office:**
 - a. Global settings (page 15-4).
 - b. Ethernet interface settings (page 15-4).
 - c. PCMCIA serial port settings (page 15-5).
 - d. Dial-in users (page 15-6).
 - e. Dial-out locations (page 15-7).
- 2. Configure the following settings for the PortMaster in the Paris office:**
 - a. Ethernet interface settings (page 15-8).
 - b. Dial-out port settings (page 15-9).
 - c. Dial-in users (page 15-10).
 - d. Dial-out locations (page 15-11).
- 3. Test the configuration (page 15-12).**
- 4. If necessary, configure the console port for multiline load balancing (page 15-13).**

Alternatively, you can configure a PortMaster Office Router for ISDN dial-on-demand connections. See page 15-15 for instructions.

Configuring the Office Router in London

Configure the following settings on the PortMaster PCMCIA Office Router in the London office to enable London office users to access the main office network in Paris on demand.

Configuring Global Settings

Configure the global settings shown in Table 15-1. The values shown in the table only apply to this example. When you are configuring your PortMaster, use values appropriate for your network.

Table 15-1 Global Values

Setting	Command
IP gateway	set gateway 192.168.1.1
System name	set sysname london

After you configure the global settings shown in Table 15-1, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet settings shown in Table 15-2.

Table 15-2 Ethernet Values

Setting	Command
IPX network	set ether0 ipxnet F3
IPX frame type	set ether0 ipxframe ethernet_802.2
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0

Table 15-2 Ethernet Values (Continued)

Setting	Command
Broadcast address	set ether0 broadcast high

After you configure the Ethernet interface as shown in Table 15-2, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring PCMCIA Serial Port Settings

The PCMCIA modem port on the PortMaster Office Router is designated S1. Configure the port with the values shown in Table 15-3. You must install the PCMCIA modem to configure port S1.

Table 15-3 PCMCIA S1 Port Values

Setting	Command
Port type	set s1 network twoway
Speed 1	set s1 speed 1 115200
Speed 2	set s1 speed 2 115200
Speed 3	set s1 speed 3 115200
Modem control	set s1 cd on
Hardware flow control	set s1 rts/cts on
Software flow control	set s1 xon/xoff off
Idle timer	set s1 idle 5
Dial group	set s1 group 1

Leave all the other settings at their default values.

After you configure the port as shown in Table 15-3, enter the following commands to reset the port and save the configuration:

```
Command> reset s1
Command> save all
```

For more information about asynchronous ports, refer to Chapter 5, “Configuring an Asynchronous Port.” For more information about configuring modems, refer to Chapter 10, “Using Modems.”

Dial-In User Settings for London

You must set up a user account on the Office Router in the London office so the PortMaster 2 in the Paris office can dial in when traffic is queued at the main office. The new user *paris* should be configured with the values shown in Table 15-4.

Table 15-4 User Table Values

Setting	Command
Username	add netuser <i>paris</i>
Password	set user <i>paris</i> password <i>anypasswd</i>
Protocol	set user <i>paris</i> protocol ppp
User IP address	set user <i>paris</i> destination <i>192.168.1.1</i>
Netmask	set user <i>paris</i> netmask <i>255.255.255.0</i>
IPX network number	set user <i>paris</i> ipxnet <i>F2</i>
RIP routing	set user <i>paris</i> rip on
MTU	set user <i>paris</i> mtu <i>1500</i>
Compression	set user <i>paris</i> compression on

After you configure the user table as shown in Table 15-4, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring user table settings, refer to Chapter 7, “Configuring Dial-In Users.”

Dial-Out Location Settings for London

You must create a location entry on the PortMaster Office Router in the London office for the Paris office. This entry allows the Office Router in the London office to call the PortMaster 2 in the Paris office when network traffic is queued. The new location *paris* should be configured with the values shown in Table 17-5.

Table 15-5 Location Table Values

Setting	Command
Location name	add location <i>paris</i>
Type	set location <i>paris</i> manual
Protocol	set location <i>paris</i> protocol ppp
IP destination	set location <i>paris</i> destination 192.168.1.1
Netmask	set location <i>paris</i> netmask 255.255.255.0
IPX network	set location <i>paris</i> ipxnet F2
RIP routing	set location <i>paris</i> rip on
MTU	set location <i>paris</i> mtu 1500
Compression	set location <i>paris</i> compression on
Idle timer	set location <i>paris</i> idle 5
High-water mark	set location <i>paris</i> high_water 0
Dial group	set location <i>paris</i> group 1
Telephone	set location <i>paris</i> telephone 5551212
Username	set location <i>paris</i> username London
Password	set location <i>paris</i> password anypasswd
Maximum ports	set location <i>paris</i> maxports 1



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

After you configure the location table as shown in Table 15-5, enter the following command to save the configuration:

Command> **save all**

For more information about configuring location table settings, refer to Chapter 8, “Configuring Dial-Out Connections.”

Configuring the PortMaster in Paris

In the example, the remote machine is a PortMaster 2 Communications Server in the Paris office.

Configuring Ethernet Interface Settings

Configure the Ethernet settings for the Paris office shown in Table 15-6.

Table 15-6 Ethernet Values

Setting	Command
IP address	set ether0 address 192.168.1.0
IPX network	set ether0 ipxnet F1
IPX frame type	set ether0 ipxframe ethernet_802.2
Netmask	set ether0 netmask 255.255.255.0
Broadcast address	set ether0 broadcast high

After you configure the Ethernet interface as shown in Table 15-6, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Dial-Out Port Settings

For all ports on the PortMaster in Paris that you want enabled for dial-in and dial-out (two-way service) to the Office Router in the London office, enter the values shown in Table 15-7.

Table 15-7 Two-Way Port Values

Setting	Command
Port type	set s1 network twoway
Speed 1	set s1 speed 1 115200
Speed 2	set s1 speed 2 115200
Speed 3	set s1 speed 3 115200
Modem control	set s1 cd on
Hardware flow control	set s1 rts/cts on
Software flow control	set s1 xon/xoff/off
Idle timer	set s1 idle 5
Dial group	set s1 group 1

Leave all the other settings at their default values.

After you configure the port as shown in Table 15-7, enter the following commands to reset the port and save the configuration:

```
Command> reset s1  
Command> save all
```

For more information about asynchronous ports, refer to Chapter 5, “Configuring an Asynchronous Port.”

Configuring a Dial-In User

A user account must be set up on the PortMaster in Paris so the Office Router in the London can dial in when traffic is queued. The new user **london** should be configured with the values shown in Table 15-8.

Table 15-8 User Table Values

Setting	Command
Username	add netuser <i>london</i>
Password	set user <i>london</i> password <i>anypasswd</i>
Protocol	set user <i>london</i> protocol ppp
User IP address	set user <i>london</i> destination <i>192.168.200.1</i>
Netmask	set user <i>london</i> netmask <i>255.255.255.0</i>
IPX network	set user <i>london</i> ipxnet <i>F2</i> (When configuring the IPX network number for the dial-in user, you must set a number that is different from the one on the Ethernet at either end.)
RIP routing	set user <i>london</i> rip on
MTU	set user <i>london</i> mtu <i>1500</i>
Compression	set user <i>london</i> compression on

After you configure the user table as shown in Table 15-8, enter the following command to save the configuration:

Command> **save all**

For more information about configuring user table settings, refer to Chapter 7, “Configuring Dial-In Users.”

Configuring Dial-Out Location Settings

You must create a location entry on the PortMaster in Paris for the London office. This entry allows the PortMaster in Paris to call the PortMaster in the London office when network traffic is queued. Configure a new location *london* with the values shown in Table 15-9.

Table 15-9 Location Table Values

Setting	Command
Location name	add location <i>london</i>
Protocol	set location <i>london</i> protocol ppp
IP destination	set location <i>london</i> destination <i>192.168.200.1</i>
Netmask	set location <i>london</i> netmask <i>255.255.255.0</i>
IPX network	set location <i>london</i> ipxnet <i>F2</i> (When configuring the IPX network number for the location, you must set a number that is different from the one on the Ethernet at either end.)
RIP routing	set location <i>london</i> rip on
MTU	set location <i>london</i> mtu <i>1500</i>
Compression	set location <i>london</i> compression on
Idle timer	set location <i>london</i> idle <i>5</i>
High-water mark	set location <i>london</i> high_water <i>0</i>
Dial group	set location <i>london</i> group <i>0</i>
Telephone number	set location <i>london</i> telephone <i>5551212</i>
Username	set location <i>london</i> username <i>paris</i>
Password	set location <i>london</i> password <i>anything</i>
Maximum ports	set location <i>london</i> maxports <i>1</i>



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

After you configure the location table as shown in Table 15-9, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring location table settings, refer to Chapter 8, “Configuring Dial-Out Connections.”

Testing the Setup

You should test the configuration before setting either of the locations for on-demand dialing. To test the configuration, follow these steps:

1. **Enter the following commands to connect from the Paris office to the London office:**

```
Command> set console s1  
Command> set debug 0x51  
Command> dial london
```

2. **Monitor the dial-and-connect sequence between the two locations.**

3. **If everything connects as expected, reset the port on the Office Router in the Paris office, turn off debugging, and change the location type to on-demand.**

```
Command> reset s1  
Command> set debug off  
Command> set location london on_demand
```

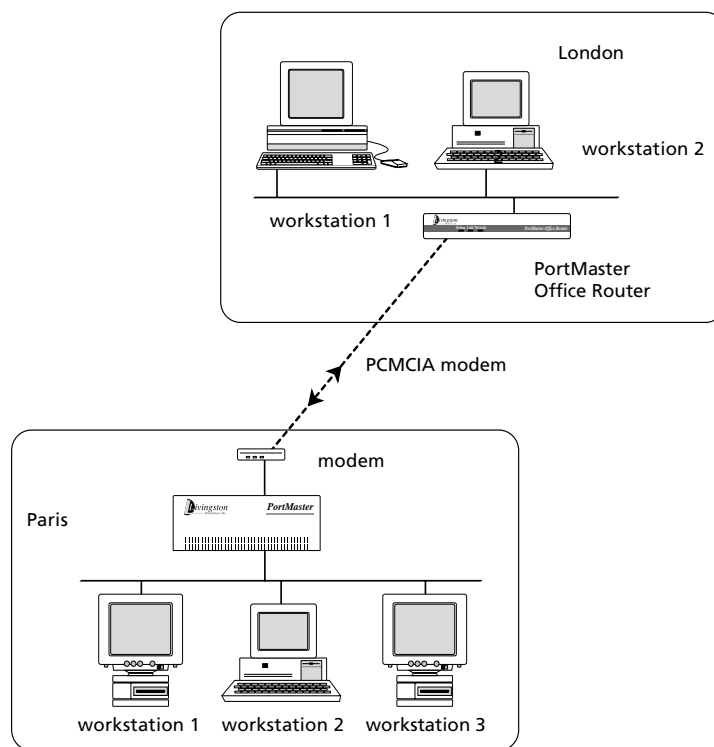

- 4. If you notice a problem, do the following:**
 - a. Reset the port on the Office Router in the Paris office.
 - b. Change the settings you think are causing the problem.
 - c. Dial the London office again.
 - d. Repeat this procedure until the connection is made correctly.
- 5. Repeat Steps 1 through 4, dialing from the London office to the Paris office.**

Setting the Console Port for Multiline Load Balancing

Multiline load balancing is used to add additional lines when network traffic is heavy. If more than one line to the same location is established, the PortMaster balances the traffic among the lines. To configure the Office Router for multiline load balancing, you must attach an external modem to the console port.

In this example the console port is being configured for use as another serial port. Once you set this configuration, the port is no longer available for the system console. Figure 15-2 shows the multiline load balancing configuration.

Figure 15-2 Multiline Load Balancing



11820009

To enable multiline load balancing, you must configure the S0 port using the same settings shown for the PCMCIA port in Table 15-3. In addition, when you configure the location *paris* on the Office Router in the London office, use the values shown in Table 15-10 for the maximum number of ports and the high-water mark. See “Dial-Out Location Settings for London” on page 15-7 for the other values.

Table 15-10 Location Settings for Load Balancing

Setting	Command
Maximum ports	set location <i>paris</i> maxports 2
High-water mark	set location <i>paris</i> high_water 100

The value of the high-water mark depends on the type of traffic and how many bytes of traffic you want queued before the second line is used.

Using ISDN for On-Demand Connections

Using the ISDN BRI port on the PortMaster ISDN Office Router (OR-U) is very similar to using the PCMCIA port on the OR-M, except that you must do the following:

- Configure the ISDN switch type as a global setting.
- Set the SPID on the port.
- Do not set the port speed, flow control, or modem control.
- Set the telephone number with the **set location telephone** command.
- Set the user name with the **set location username** command.
- Set the password with the **set location password** command.

For more information about ISDN connections, see Chapter 12, “Using ISDN BRI.” For information about locations, see Chapter 8, “Configuring Dial-Out Connections.”

This chapter uses an example to demonstrate how to configure the PortMaster to establish a continuous connection to an Internet service provider (ISP), shown in Figure 18-1. This connection creates a gateway from your office to the Internet using a dial-out connection through one of the serial ports on your PortMaster. Internet connections can also be set for on-demand operation.

The following topics are discussed:

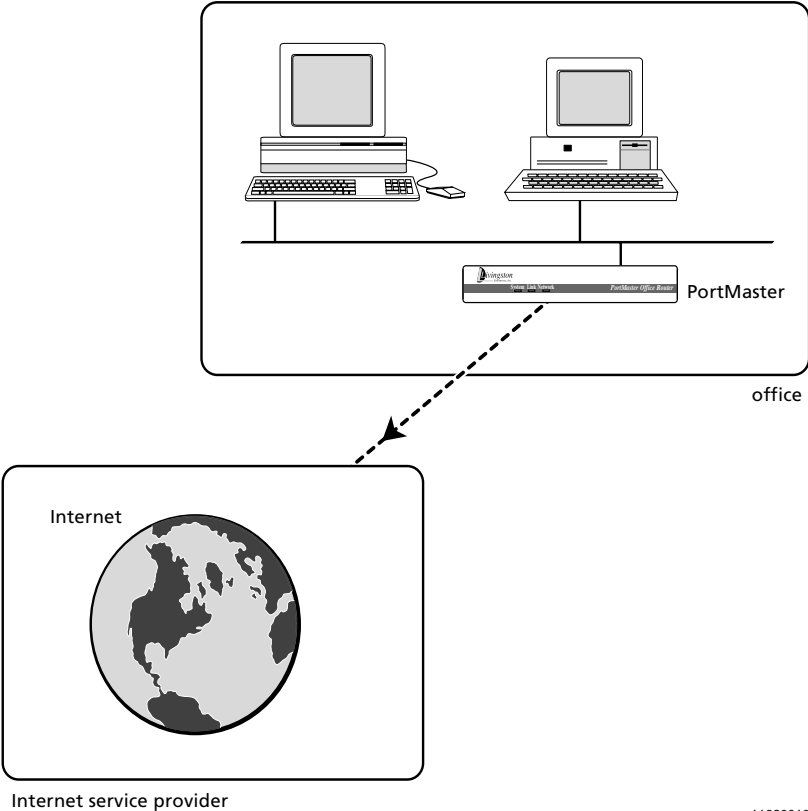
- “Overview of Continuous Internet Connections” on page 16-3
- “Configuration Steps for an Internet Connection” on page 16-3
- “Providing Network Filtering” on page 16-10
- “Using ISDN for Internet Connections” on page 16-11

For information on related topics, refer to the following chapters:

Topic	Chapter
On-demand connections	<ul style="list-style-type: none">• Chapter 8, “Configuring Dial-Out Connections”• Chapter 15, “Using Office-to-Office Connections”
Configuring a PortMaster for an ISDN connection	<ul style="list-style-type: none">• Chapter 11, “Configuring the PortMaster 3”• Chapter 12, “Using ISDN BRI”
Frame Relay connections	<ul style="list-style-type: none">• Chapter 13, “Using Frame Relay
Synchronous leased lines	<ul style="list-style-type: none">• Chapter 19, “Using Synchronous Leased Lines

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Figure 16-1 Continuous Internet Connection



11820010

Overview of Continuous Internet Connections

You can configure two types of continuous connections:

- Dial-up

A continuous dial-up connection starts as soon as the PortMaster boots and is redialed whenever the telephone connection is dropped. If you use a continuous dial-out link from the S1 serial port, one location table entry is needed for the ISP.

- Dedicated circuit—also known as a network hardwired connection

The network hardwired configuration is typically used if you are using a leased analog or digital line or an asynchronous-to-synchronous converter. If you use a network hardwired port, no entries are needed in the location table.

This example provides configuration information for both types of continuous connections.

For this example, IPX packets are not transmitted to or from the ISP.

You can also connect to an ISP with a dial-on-demand configuration, as described in Chapter 15, “Using Office-to-Office Connections.” However, dial-on-demand ISP connections do not allow Internet users access to your site when the dial-up connection is not established.

Configuration Steps for an Internet Connection

The example described in this chapter connects a PortMaster router located in an office (*office1*) with an ISP (*isp1*) using Frame Relay on a synchronous interface.

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the installation guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

- 1. Configure the following settings for the PortMaster in Office 1:**
 - a. Global settings (page 16-4).
 - b. Ethernet interface settings (page 16-4).

- c. Serial port settings (page 16-5 or page 16-6).
- d. Dial-out location (page 16-7).

2. Test the configuration (page 16-8 or page 16-9).

3. Set network filtering (page 16-10).

Alternatively, you can configure a PortMaster with an ISDN port for an Internet connection. See “Using ISDN for Internet Connections” on page 16-11.

Configuring Global Settings

Configure the global settings to the values shown in Table 16-1.

Table 16-1 Global Settings Values

Setting	Command
Default IP gateway	set gateway 192.168.5.6

For more information about global settings, see Chapter 3, “Configuring Global Settings.”

After configuring the global settings, enter the following command to save the configuration:

```
Command> save all
```

Configuring Port Settings

You must configure settings for your Ethernet port and settings for either a dial-out or hardwired connection on your asynchronous port.

Ethernet Interface Settings

Set the Ethernet parameters to the values shown in Table 16-2.

Table 16-2 Ethernet Port Parameter Values

Setting	Command
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0
Broadcast address	set ether0 broadcast high

After configuring the Ethernet interface, enter the following commands to reset it and save the configuration:

```
Command> reset ether0  
Command> save all
```

For more information on Ethernet interface parameters, refer to Chapter 4, “Configuring the Ethernet Interface.”

Serial Port Settings for Dial-Out

For continuous dial-out on a serial port, configure the port with the values shown in Table 16-3.

Table 16-3 Serial Port Values for Continuous Dial-Out

Setting	Command
Port type	set sl network dialout
Protocol	set sl protocol ppp
Speed 1	set sl speed 1 115200
Speed 2	set sl speed 2 115200
Speed 3	set sl speed 3 115200
Modem control	set sl cd on
Hardware flow control	set sl rts/cts on
Software flow control	set sl xon/xoff off
Dial group	set sl group 1

Leave all other settings at their default values.

After configuring the serial port, enter the following commands to reset the port and save the configuration:

```
Command> reset s1
Command> save all
```

For more information about asynchronous ports and configuring modems, refer to Chapter 5, “Configuring an Asynchronous Port.”

Serial Port Settings for a Hardwired Connection

To establish a hardwired connection on a serial port, configure the port with the values shown in Table 16-4.

Table 16-4 Serial Port Values for a Hardwired Port

Setting	Command
Port type	set s1 network hardwired
Protocol	set s1 protocol ppp
MTU	set s1 mtu 1500
Speed 1	set s1 speed 1 115200
Modem control	set s1 cd on
Hardware flow control	set s1 rts/cts on
Software flow control	set s1 xon/xoff off
IP destination	set s1 destination 192.168.5.6
Netmask	set s1 netmask 255.255.255.0
RIP routing	set s1 rip off
Compression	set s1 compression on

Leave all other settings at their default values. After configuring the serial port, enter the following commands to reset the port and save the configuration:

```
Command> reset s1
Command> save all
```

For more information about asynchronous ports, refer to Chapter 5, “Configuring an Asynchronous Port.”

Configuring a Dial-Out Location

If you are using a continuous dial-out link, a location entry on the PortMaster must be created for the location identified as *isp1*. This entry allows the PortMaster to establish a connection with the ISP as soon as it is booted. The new location *isp1* should be configured with the values shown in Table 16-5, or as instructed by your ISP.

Table 16-5 Location Table Values

Setting	Command
Location name	add location <i>isp1</i>
Type	set location <i>isp1</i> manual (Change to continuous after testing the configuration.)
Protocol	set location <i>isp1</i> protocol ppp
IP destination	set location <i>isp1</i> destination 192.168.5.6
Netmask	set location <i>isp1</i> netmask 255.255.255.0
RIP routing	set location <i>isp1</i> rip broadcast
MTU	set location <i>isp1</i> mtu 1500
Compression	set location <i>isp1</i> compression on
Input filter	set location <i>isp1</i> ifilter <i>internet.in</i>
Output filter	set location <i>isp1</i> ofilter <i>internet.out</i>
Idle timer	set location <i>isp1</i> idle 0
High-water mark	set location <i>isp1</i> high_water 0
Dial group	set location <i>isp1</i> group 1
Telephone number	set location <i>isp1</i> telephone 5551212
Username	set location <i>isp1</i> username <i>office</i> (This value is provided by your ISP.)

Table 16-5 Location Table Values (Continued)

Setting	Command
Password	set location <i>isp1</i> password <i>passwd</i> (This value is provided by your ISP.)
Maximum ports	set location <i>isp1</i> maxports <i>1</i>



Note – Configuring the maximum ports setting to a value higher than 0 causes the PortMaster to dial out to a continuous location, or become available for dial-out to an on-demand location. By configuring the maximum ports setting last, you ensure that the PortMaster will not attempt to make a connection with a location until you have configured all the settings for that location.

You can also authenticate using CHAP if it is supported by the ISP.

After configuring the location table settings, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring locations, see Chapter 8, “Configuring Dial-Out Connections.”

Testing the Continuous Dial-Out Setup

The configuration should be tested before the location *isp1* is set for continuous dialing. To test the configuration, follow these steps:

1. Enter the following commands to connect from your office to location *isp1*:

```
Command> set console
Command> set debug 0x51 -x
Command> dial isp1
```

2. Monitor the dial-and-connect sequence between the two locations.

3. If everything connects as expected, reset the port, turn off debugging, and change the location type to continuous.

```
Command> reset s1
Command> set debug off
Command> set location isp1 continuous
```

4. If you notice a problem, do the following:

- a. Reset the port.
- b. Check your configuration.
- c. Dial the ISP again.
- d. Repeat this procedure until the connection is made correctly.

Contact your ISP if you are unable to connect as expected. The ISP might be able to provide additional information.

5. When you have configured the PortMaster correctly, enter the following commands to reset the port and save the configuration:

```
Command> reset s1  
Command> save all
```

Testing the Network Hardwired Setup

To test a network hardwired connection, follow these steps:

1. Reset the newly configured serial port.

```
Command> reset s1
```

The network hardwired connection should be established within a few seconds.

2. Verify that the port status is ESTABLISHED by entering the following command:

```
Command> show s1
```

3. If there is a problem, check your configuration.

Contact your ISP if you are unable to connect as expected.

4. When you have configured the PortMaster correctly, reset the port and save the configuration.

```
Command> reset s1  
Command> save all
```

Providing Network Filtering

Your connection to the Internet can be vulnerable to attack from other Internet users. Therefore, Lucent recommends that you add an input filter to the location *isp1* for the continuous dial-out connection. For a hardwired connection, you should attach an input filter to the hardwired port.



Note – This section describes an example filter that might not protect your network from all forms of attack. For more information about filters, refer to “Additional References” in the preface and Chapter 9, “Configuring Filters.” Refer to the *ChoiceNet Administrator’s Guide* and the *RADIUS Administrator’s Guide* for more information on network security.

The filter named **internet.in** contains the following rules:

```
deny 192.168.200.0/24 0.0.0.0/0 log
permit tcp estab
permit 0.0.0.0/0 mail.edu.com/32 tcp dst eq 25
permit 0.0.0.0/0 ftp.edu.com/32 tcp dst eq 21
permit 0.0.0.0/0 www.edu.com/32 tcp dst eq 80
permit tcp src eq 20 dst gt 1023
permit udp dst eq 53
permit tcp dst eq 53
permit icmp
```

If you have not configured a name server for the PortMaster, use IP addresses instead of hostnames when creating filters.

Table 16-6 provides a line by line description the filter.

Table 16-6 Description of Internet Filter

Rule	Description
1.	Denies any incoming packets claiming to be from your own network (192.168.200.0). This rule blocks IP spoofing attacks and logs the spoofing attempt.
2.	Permits already established TCP connections.
3.	Permits SMTP connections to the mail server mail.edu.com .
4.	Permits FTP connections to the host ftp.edu.com .
5.	Permits WWW HTTP connections to the Web server www.edu.com .

Table 16-6 Description of Internet Filter (Continued)

Rule	Description
6.	Permits an FTP data channel back to outgoing FTP requests.
7.	Permits the Domain Name Service (DNS).
8.	Permits DNS zone transfers. (You might want to restrict this rule to allow only connections to your name servers.)
9.	Permits ICMP packets.

If your domain name server is outside your local network, refer to “Input and Output Filters for FTP Packets” on page 9-11.

Using ISDN for Internet Connections

Using the ISDN port on a PortMaster is very similar to using the serial port, except that you must do the following:

- Configure the ISDN switch type as a global setting.
- Set the SPID on the port.
- Do not set the port speed, flow control, or modem control.
- Set the telephone number with the **set location telephone** command.
- Set the username with the **set location username** command.
- Set the password with the **set location password** command.

For more information see Chapter 12, “Using ISDN BRI,” and Chapter 8, “Configuring Dial-Out Connections.”

This chapter uses an example to demonstrate how to configure a PortMaster for remote dial-in access to local hosts and networks. Although the example shows how Internet service providers (ISPs) can provide dial-in access to their users, this application can be used by academic environments, corporate telecommuters, or anyone else needing remote access to a host or network.

In this example, multiple asynchronous ports are configured with modems for answering incoming calls from users who then access a networked host connected via Ethernet to a PortMaster 2E Communications Server.

The following topics are described:

- “Overview of Dial-In Configuration” on page 17-1
- “Configuration Steps for Dial-In Access” on page 17-4

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Dial-In Configuration

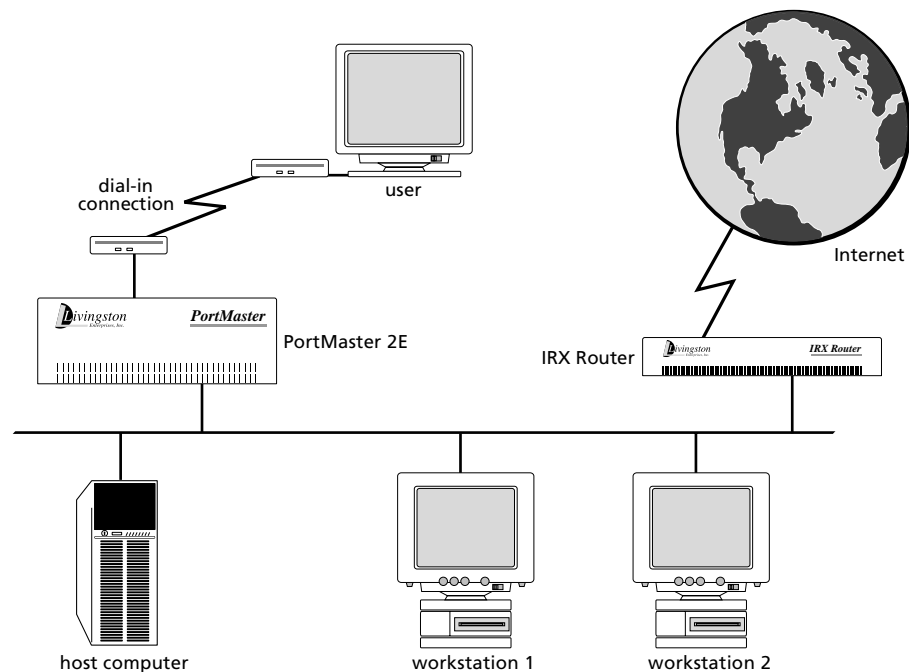
The PortMaster configuration described in this example allows up to seven 30-port PortMaster Communications Servers to be connected together to provide up to 210 dial-in asynchronous ports. The PortMaster Communications Server allows dial-in users to access a host for shell accounts and/or PPP, SLIP, or Compressed SLIP (CSLIP) connections.

ISPs can use this example to configure their PortMaster products to allow dial-in users to access hosts and networks. The number of ports used is a function of the number of expected subscribers. One port per 10 subscribers is the typical ratio, but peak usage and average usage per port should be monitored closely to determine the need for additional ports. RADIUS Accounting can help you to evaluate port usage. See the *RADIUS Administrator's Guide* for more information.

The same application can be used by companies to allow remote users to access their own accounts on the corporate network. Once the PortMaster authenticates users, they can access network resources as if they were connected to the corporate network directly.

Although this example uses seven PortMaster 2E Communications Servers, many more can be used. With more than seven PortMaster Communications Servers, the configuration is the same except that the assigned pools must be arranged differently.

Figure 17-1 Dial-In User Configuration



11820011

Example Configuration

The example described in this chapter uses the values shown in Table 17-1. Change variable values to values that reflect your network.

Table 17-1 Example Configuration Variables

Variable Description	Value
Address type	Class C assigned by your provider
Network IP address	192.168.1.0
IP address and name of router connecting to the Internet	192.168.1.1 (gw.edu.com)
IP address and name of host running RADIUS	192.168.1.2 (rk2.edu.com)
IP address and name of host running DNS	192.168.1.2 (rk2.edu.com)
IP address of RADIUS accounting server	192.168.1.2 (rk2.edu.com)
IP address of RADIUS backup accounting server	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host running backup RADIUS	192.168.1.3 (rk3.edu.com) (Optional)
IP address of host that shell users log in to	192.168.1.4 (rk4.edu.com) (Optional)
IP addresses reserved for future hosts	192.168.1.5 through 192.168.1.15, 192.168.1.23 through 192.168.1.32
IP address and name of first PortMaster	192.168.1.16 (pm1.edu.com)
IP addresses and names for additional PortMasters	192.168.1.17 through 192.168.1.22 (pm2.edu.com through pm7.edu.com)
Reserved pool of assigned addresses for PortMaster 1	192.168.1.33 through 192.168.1.62
Reserved pool of assigned addresses for PortMaster 2	192.168.1.65 through 192.168.1.94
Reserved pool of assigned addresses for PortMaster 3. Continue until PortMaster 7.	192.168.1.97 through 192.168.1.126

Table 17-1 Example Configuration Variables (Continued)

Variable Description	Value
Reserved pool of assigned addresses for PortMaster 7	192.168.1.225 through 254

You can set the assigned pool numbers a little closer together as long as they do not overlap; however, having the pools fall within bit boundaries makes packet filters easier to write.



Note – This example uses a PortMaster 2E Communications Server. If you are using a PortMaster 25, the numbers of assigned pools can be moved closer together.

Configuration Steps for Dial-In Access

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of your installation guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the first PortMaster, continue with the following steps:

1. **Connect modems to the PortMaster 2E (page 17-5).**
2. **Configure global settings (page 17-5).**
3. **Configure Ethernet interface settings (page 17-6).**
4. **Configure asynchronous port settings (page 17-6).**
5. **Configure modems for the asynchronous ports (page 17-6).**
6. **Configure users via RADIUS settings if you have more than one hundred users (page 17-8).**
7. **Configure login users if you are not using RADIUS (page 17-9).**
8. **Configure network users if you are not using RADIUS (page 17-9).**
9. **Repeat Steps 1 through 8 for each additional PortMaster in your topology.**



Note – This example describes how to configure the first PortMaster, **pm1.edu.com**. Use a similar configuration for the remaining PortMaster devices.

Connecting Modems

Use the following steps to connect modems to the first PortMaster:

1. **Connect your modems to the serial ports using straight-through modem cables.**

Modems slower than 14.4Kbps are not recommended for network users.

2. **Make sure that the modem cables are securely fastened and that you provide enough room for the modems to stay cool.**

Configuring Global Settings

Configure the global settings on the first PortMaster to the values shown in Table 17-2.

Table 17-2 Global Values

Setting	Command
Default host	set host 192.168.1.4
Alternate host	set host 2 any other available host
IP gateway	set gateway 192.168.1.1
Default routing	set default off
Name service	set namesvc dns
Name server	set nameserver 192.168.1.2
Domain	set domain edu.com
System name	set sysname pm1
Loghost	set loghost 192.168.1.2
Assigned address	set assigned 192.168.1.33

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

After you configure the global settings as shown in Table 17-2, enter the following command to save the configuration:

Command> **save all**

Configuring Ports

You must configure each port you are using for dial-in on the first PortMaster, plus its attached modem.

Configuring Ethernet Port Settings

Set the Ethernet port on the first PortMaster to the values shown in Table 17-3.

Table 17-3 Ethernet Values

Setting	Command
IP address	set ether0 address 192.168.1.16
Netmask	set ether0 netmask 255.255.255.0
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 17-3, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Serial Modem Port Settings

The serial modem ports are designated S0 through S29 on the PortMaster. Use the **set all** command to set the same values for each serial port. The port values shown in Table 17-4 can be set on all asynchronous ports on the first PortMaster. Use the modem

table described in Chapter 10, “Using Modems,” to configure the attached modems, or set each port as a host device as described in Chapter 18, “Accessing Shared Devices,” and configure each modem individually.



Note – V.34 modems should lock the DTE rate at 115200bps unless your modem manual instructs otherwise. V.32bis modems should lock the DTE rate at 57600bps. Use the fastest DTE interface speed supported by your modem.

A list of modems and their initialization strings appears in Chapter 10, “Using Modems.” The recommended configuration for this example has the following features:

- Raises carrier when a call comes in
- Resets itself when DTR is dropped
- Locks the DTE rate
- Uses hardware flow control (RTS/CTS)
- Automatically answers on the first ring

If you have already configured your modems on another machine, you should connect to the modem through the PortMaster and set the modem back to the factory default. Then use the recommended modem string to properly configure each modem.

Table 17-4 Serial Port Values for All Ports

Setting	Command
Port type	set all login network dialin
Security	set all security on
Modem type	set all modem <i>usr-v34</i>
Speed 1	set all speed 1 <i>115200</i>
Speed 2	set all speed 2 <i>115200</i>
Speed 3	set all speed 3 <i>115200</i>
Modem control	set all cd on
Hardware flow control	set all rts/cts on
Software flow control	set all xon/xoff off

After you configure the ports as shown in Table 17-4, enter the following commands to reset the ports and save the configuration:

```
Command> reset all
Command> save all
```

Configuring Users

Because no more than approximately one hundred users can be configured in the user table and stored in nonvolatile memory on the PortMaster, you should use RADIUS for user authentication when configuring multiple PortMaster Communication Servers to handle more than a few dozen users each. This example assumes the use of RADIUS.

If you are not using RADIUS, configure dial-in and network users in the user table.

RADIUS Settings

Table 17-5 lists the RADIUS setting for the first PortMaster. For information about RADIUS parameters, refer to the *RADIUS Administrator's Guide* or access the information via FTP from <ftp://ftp.livingston.com/pub/le/radius/radius.install>.

Table 17-5 RADIUS Values

Setting	Command
Secret	set secret <i>anyvalue</i>
Authentication server	set authentic <i>192.168.1.2</i>
Alternate authentication server	set alternate <i>198.168.1.3</i> (This setting is optional. This secondary server must have a RADIUS database identical to that on the primary authentication server.)
Accounting server	set accounting <i>192.168.1.2</i>
Alternate accounting server	set accounting 2 <i>192.168.1.3</i> (This setting is optional.)

After configuring RADIUS settings as shown in Table 17-5, use the following command to save the configuration:

```
Command> save all
```

Dial-In Login Users



Note – Use the instructions in this section only if you are not using RADIUS and you are not using pass-through logins.

A user account must be set up on the PortMaster for each authorized user. You should configure each new user *user1*, *user2*, and so on, with the values shown in Table 17-6.

Table 17-6 User Table Values for *user1*

Setting	Command
Username	add user <i>user1</i>
Password	set user <i>user1</i> password <i>passwd</i>
Login service	set user <i>user1</i> service <i>portmaster</i> (Use the PortMaster login service if the in.pmd daemon is running on the default host; otherwise use rlogin .)

After you configure user table settings as shown in Table 17-6, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring user table values, refer to Chapter 7, “Configuring Dial-In Users.”

Dial-In Network Users



Note – Use the instructions in this section only if you are not using RADIUS.

A user account must be set up on the PortMaster for each authorized network user. Each new user *usera*, *userb*, and so on should be configured with the values shown in Table 17-7.

Table 17-7 User Table Values for *usera*

Parameter	Command
Username	add netuser <i>usera</i>
Password	set user <i>usera</i> password <i>passwd</i>
Protocol	set user <i>usera</i> protocol <i>ppp</i>
Address type	set user <i>usera</i> destination <i>assigned</i>
Compression	set user <i>usera</i> compression <i>on</i>
RIP routing	set user <i>usera</i> rip <i>off</i>

You can also use SLIP or CSLIP instead of PPP. Refer to Chapter 7, “Configuring Dial-In Users,” for more information about this configuration.

After you configure user table settings as shown in Table 17-7, enter the following command to save the configuration:

```
Command> save all
```

For more information about configuring user table values, refer to Chapter 7, “Configuring Dial-In Users.”

Testing the User Dial-In Setup

To test the configuration, follow these steps for each PortMaster set up for user dial-in access:

1. **Enter the following commands:**

```
Command> set console  
Command> set debug 0x51
```

2. **Dial in to the PortMaster you are testing, using the username and password you have created in either RADIUS, or the user table.**

- 3. If everything connects as expected, turn off debugging and save the configuration.**

```
Command> set debug off
```

```
Command> save all
```

- 4. If you notice a problem, do the following:**

- a. Reset the port.
- b. Check your configuration.
- c. Dial the PortMaster again.
- d. Repeat this procedure until the connection is made correctly.

- 5. When you have configured the PortMaster correctly, reset the ports and save the configuration.**

```
Command> reset all
```

```
Command> save all
```


This chapter uses an example to demonstrate how to configure the PortMaster to connect from networked hosts to shared devices attached to the PortMaster. This type of connection provides user access to modems, printers, and other RS-232 devices.

The following topics are described:

- “Overview of Shared Device Access Methods” on page 18-1
- “Configuration Steps for Shared Device Access” on page 18-4

See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Shared Device Access Methods

Use one of the following methods for providing access to shared devices on the PortMaster:

- Host device configuration

You use a UNIX host that supports the PortMaster **in.pmd** daemon. With this daemon, you can configure ports as host devices and access them as pseudo-tty terminals from the host using the **tip** command, UUCP, and other applications.

- Network device configuration

You configure the ports as network devices and access them via Telnet, rlogin, or a clear channel TCP connection (netdata).

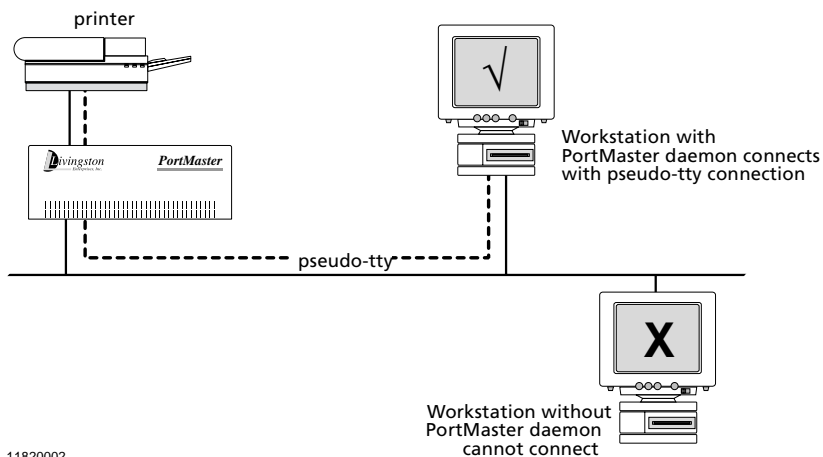
Host Device Configuration

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

Once a port is defined as a host device, you configure it with the PortMaster device service, and select a pseudo-tty terminal. The host device port can now be accessed if you establish a pseudo-tty connection to the port from a UNIX host with the PortMaster daemon software installed. In this case, the port operates as a host-controlled device.

Figure 18-1 shows a diagram of the host device configuration using the PortMaster device service and a pseudo-tty connection.

Figure 18-1 Host Device Configuration



In this configuration, a workstation with **in.pmd** installed can access a printer attached to a PortMaster port, even if the printer is on the other side of the country.

Network Device Configuration

This configuration sets the port for host device access, but uses the rlogin, Telnet, or netdata device service to access the attached device. In this configuration, the host device name is set as **/dev/network**. This configuration is used in cases where users want to use Telnet or rlogin to log in to the shared device from multiple hosts or from a host that does not support **in.pmd**.

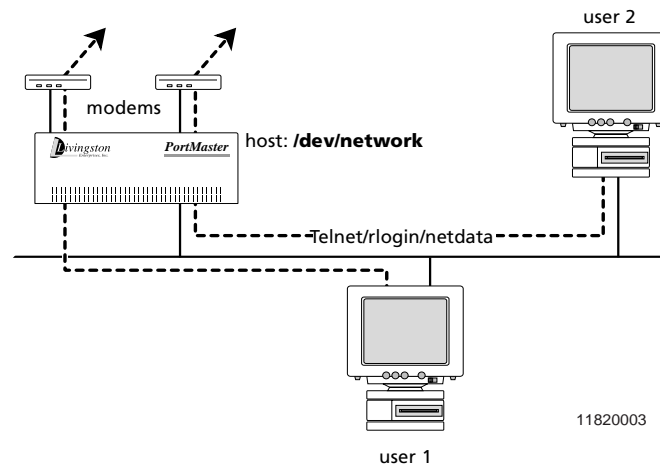
Figure 18-2 shows an example of the network device configuration.

The network user configuration is most commonly used to provide a Telnet session with the device attached to a specified PortMaster port. The example in this chapter sets ports for network access so the administrator can telnet to each modem connected to a

PortMaster port for configuration purposes. In this application, each port is identified by a unique port number assigned during the configuration process. You can also configure a pool of ports at a single TCP port number.

The netdata (TCP clear channel) device service is most often used when you want to have a custom application open a TCP connection to an RS-232 device, or to connect two serial devices across a network.

Figure 18-2 Network Device Configuration



The example described in this chapter allows a user to dial in to port S2 on the PortMaster, log in to a workstation, and access a serial printer attached to port S9 as **/dev/ttyre**, using the PortMaster device service. The workstation user can also access port S2 as **/dev/ttyrf** when it is not being used for login service.

The modem attached to port S2 is connected with a straight-through cable and uses hardware flow control and carrier detect. The DTE rate between the modem and the PortMaster is locked.

To use the PortMaster login or device service, the workstation user must install the PortMaster daemon **in.pmd** in the **/usr/etc** directory. She must also modify the **/etc/services** and **/etc/inetd.conf** files to tell the workstation where to find **in.pmd**. She must also add **/dev/ttyrf** to the **/etc/remote** file and **/dev/ttyre** to the **/etc/printcap** file.

Configuration Steps for Shared Device Access

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of the installation guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

1. **Attach the modem to port S2 with a straight-through cable.**
2. **Attach the printer to port S9 with a null modem cable if the printer is a DTE device.**

Pinouts for both cables are given in your hardware installation guide.

3. **Configure global settings (page 18-4).**
4. **Configure Ethernet port settings (page 18-5).**
5. **Configure two-way serial port (S2) settings (page 18-5).**
6. **Configure serial printer port (S9) settings (page 18-7).**
7. **Configure parallel port (P0) settings (page 18-8).**
8. **If necessary, configure network devices for Telnet access (page 18-8).**

Configuring Global Settings

Configure the global settings to the values shown in Table 18-1.

Table 18-1 Global Values

Setting	Command
Default host	set host <i>192.168.200.2</i> (This is the user's workstation.)

If you want to use the other ports for another host, use the **set S0 host** command to set ports S2 and S9 to 92.168.200.2.

After you configure global settings as shown in Table 18-1, enter the following command to save the configuration:

Command> **save all**

Configuring Port Settings

You must configure settings for your Ethernet interface, dial-in-and-out (two-way) port, and printer port. You can connect the printer to either a serial port or a parallel port.

Ethernet Interface Settings

Configure the Ethernet interface to the values shown in Table 18-2.

Table 18-2 Ethernet Values

Setting	Command
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0
Broadcast address	set ether0 broadcast high

After you configure the Ethernet interface as shown in Table 18-2, enter the following command to save the configuration:

Command> **save all**

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Two-Way Serial Port (S2) Settings

In the example, the workstation user wants to dial in to port S2 sometimes and use the **tip** command dial out through the modem connected to port S2 at other times. Configure the S2 port with the values shown in Table 18-3.

Table 18-3 Serial Port Values (S2)

Setting	Command
Port type	set s2 twoway /dev/ttyrf

Table 18-3 Serial Port Values (S2) (Continued)

Setting	Command
Speed 1	set s2 speed 1 115200
Speed 2	set s2 speed 2 115200
Speed 3	set s2 speed 3 115200
Modem control	set s2 cd on
Hardware flow control	set s2 rts/cts on
Software flow control	set s2 xon/xoff off
Host	set s2 host default
Security	set s2 security on (If you turn security on, you must also configure the user table or RADIUS.)
Login service	set s2 service_login portmaster
Device service	set s2 service_device portmaster

Leave all other settings at their default values.

After you configure port S2 as shown in Table 18-3, enter the following commands to reset the port and save the configuration:

```
Command> reset s2  
Command> save all
```

For more information about serial asynchronous ports, refer to Chapter 5, “Configuring an Asynchronous Port.”

Serial Printer Port (S9) Settings

In the example, a serial printer is connected to port S9. Configure the S9 port with the values shown in Table 18-4. If the printer is a DTE, use a null modem cable to connect to the port.

Table 18-4 Serial Port Values (S9)

Setting	Command
Port type	set s9 device /dev/ttyre
Speed 1	set s9 speed 1 9600
Speed 2	set s9 speed 2 9600
Speed 3	set s9 speed 3 9600
Modem control	set s9 cd on
Software flow control	set s9 xon/xoff on
Host	set s9 host default
Device service	set s9 service_device portmaster

Leave all other settings at their default values.

After you configured port S9 as shown in Table 18-4, enter the following commands to reset the port and save the configuration:

```
Command> reset s9  
Command> save all
```

The workstation printer subsystem should now be able to send printer jobs to **/dev/ttyre** and reach the printer.

Parallel Port (P0) Settings

You can also configure the parallel port P0 to access a printer. To configure the P0 port for a printer, use the values shown in Table 18-5.

Table 18-5 Parallel Port (P0) Values

Setting	Command
Port type	set P0 device /dev/ttyre
Host	set P0 host default
Device service	set P0 service_device portmaster

Leave all other settings at their default values.

After you have configure port P0 as shown in Table 18-5, enter the following commands to reset the port and save the configuration:

```
Command> reset P0  
Command> save all
```

Configuring a Network Device for Telnet Access

To access modems or other devices attached to PortMaster ports via Telnet, use the general configuration given earlier in this chapter but use the settings shown in Table 18-6. This example is for port S1.

Table 18-6 Serial Port Values to Allow a Telnet Connection to Ports S0 through S29

Setting	Command
Port type	set s1 device /dev/network
Modem control	set s1 cd off
Device service	set s1 service_device telnet 6001

After resetting port S1, you can access it using Telnet from your host or by entering the following commands:

```
Command> reset s1  
Command> telnet pm1 6001
```

The value *pm1* is the hostname of the PortMaster you are accessing, and *6001* is the TCP port set for the port you are accessing. You can also set several ports to the same TCP port to create a pool of ports available for Telnet access.



Note – If you are using this configuration to configure your modems, refer first to Chapter 10, “Using Modems.”

This chapter uses an example to demonstrate how to configure the PortMaster to connect to a synchronous leased line at speeds up to T1 (1.544Mbps) or E1 (2.048Mbps). This chapter also describes how to configure a dial backup connection for your synchronous line. The example described in this chapter connects a PortMaster router located in one office with a PortMaster router located in another office using a dedicated leased line.

The following topics are described:

- “Overview of Leased Line Connections” on page 19-1
- “Configuration Steps for Leased Line Connections” on page 19-3
- “Troubleshooting a Leased Line Connection” on page 19-8

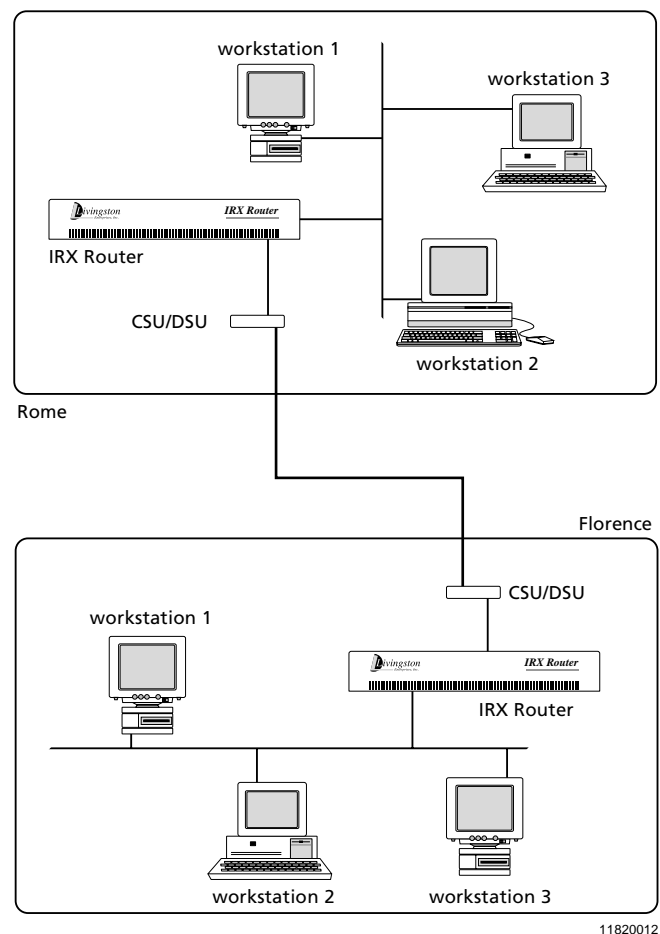
See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

Overview of Leased Line Connections

Leased line connections use leased or dedicated lines to establish a permanent connection between two routers. Once the connection is established, it remains available on a continuous basis whether there is network traffic between the two locations or not. Leased line connections require a digital service unit/channel service unit (DSU/CSU) connected between the router and the dedicated line. The DSU/CSU takes digital data in the format used by the router and translates it into the digital format used by the leased line. Leased line connections also require a carrier that provides an external clock signal.

PortMaster routers support leased line connections using synchronous ports and the PPP protocol. In this configuration, one PortMaster is usually connected to another PortMaster or other router over a leased line where each router uses its own Ethernet address for the serial link—known as IP unnumbered—and the address of the other end is discovered dynamically. In this way, a dedicated high-speed connection is established between two routers located at separate sites. Figure 19-1 shows an example of the leased line connection.

Figure 19-1 Leased Line Configuration



If you are connecting two networks together for the first time, you should make sure first that the two networks are not overlapping subnets. For more information on network numbers and subnetting, see Appendix A, “Networking Concepts.”

In the leased line configuration described in this chapter, the Ethernet address of the PortMaster routers is used as the address for the serial link in a point-to-point unnumbered serial connection. Because the PortMaster relies on an external clock

signal, you do not need to set the speed on the synchronous port. The port speed is whatever the carrier sends. If you choose to set a speed, it is used for administrative notation only and does not affect the operation of the port.

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



Note – The PortMaster also supports numbered IP interfaces on leased lines, but Lucent does not recommend this method because it wastes IP address space.

Configuration Steps for Leased Line Connections

This example connects a PortMaster Office Router in Rome with a PortMaster Office Router in Florence using a leased line connection.

To install your PortMaster, follow the instructions in your hardware installation guide. If you need additional help, refer to the troubleshooting chapter of your installation guide. The example in this chapter shows variables in *italics*. Change these values to reflect your network.

Once you have assigned an IP address to the PortMaster, continue with the following steps:

1. Configure the following settings for the PortMaster in Rome:

- a. Global settings (page 19-4)
- b. Ethernet interface settings (page 19-4)
- c. Synchronous WAN port settings (page 19-5)

2. Configure the following settings for the PortMaster in Florence:

- a. Global settings (page 19-6)
- b. Ethernet interface settings (page 19-6)
- c. Synchronous WAN port settings (page 19-7)

3. Troubleshoot the configuration, if necessary (page 19-8).

Configuring the PortMaster Office Router in Rome

Configure the settings for the PortMaster Office Router in Rome with the values in the following sections.

Configuring Global Settings

Configure the global settings to the values shown in Table 19-1.

Table 19-1 Global Values

Setting	Command
IP gateway	set gateway 192.168.1.1
System name	set sysname rome

After you configure the global settings shown in Table 19-1, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet interface on the PortMaster Office Router in Rome to the values shown in Table 19-2.

Table 19-2 Ethernet Values

Setting	Command
IP address	set ether0 address 192.168.200.1
Netmask	set ether0 netmask 255.255.255.0
IPX network	set ether0 ipxnet F1
IPX frame type	set ether0 ipxframe ethernet_802.2
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 19-2, enter the following command to save the configuration:

```
Command> save all
```

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Settings

Configure the synchronous WAN port on the PortMaster Office Router in Rome with the values shown in Table 19-3. Port S1 is used in this example. The IP address for the port is left unconfigured, accepting the default IP address value of 0.0.0.0.

Table 19-3 Synchronous WAN Port Values

Setting	Command
Port type	set s1 network hardwired
Transport protocol	set s1 protocol ppp
IP destination	set s1 destination 192.168.1.1
Netmask	set s1 netmask 255.255.255.0
IPX network	set s1 ipxnet F3
Modem control	set s1 cd off
RIP routing	set s1 rip on
MTU	set s1 mtu 1500

If you are not sure of the IP address on the other end of the connection, you can set the IP destination to 255.255.255.255 and the PortMaster will attempt to learn the address.

Leave all other settings at their default values.

After you configure the port S1 as shown in Table 19-3, enter the following command to reset the port and save the configuration:

```
Command> reset s1  
Command> save all
```

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Configuring the PortMaster Office Router in Florence

Configure the settings for the PortMaster Office Router in Florence with the values in the following sections.

Configuring Global Settings

Configure the global settings to the values shown in Table 19-4.

Table 19-4 Global Values

Setting	Command
IP gateway	set gateway 192.168.200.1
System name	set sysname office2

After you configure the global settings shown in Table 19-4, enter the following command to save the configuration:

Command> **save all**

For more information about global settings, refer to Chapter 3, “Configuring Global Settings.”

Configuring Ethernet Interface Settings

Configure the Ethernet settings to the values shown in Table 19-5.

Table 19-5 Ethernet Values

Setting	Command
IP address	set ether0 address 192.168.1.1
Netmask	set ether0 netmask 255.255.255.0
IPX network	set ether0 ipxnet F1
IPX frame type	set ether0 ipxframe ethernet_802.2
Broadcast address	set ether0 broadcast high
RIP routing	set ether0 rip on

After you configure the Ethernet interface as shown in Table 19-5, enter the following command to save the configuration:

```
Command> save all
```

For more information on Ethernet settings, refer to Chapter 4, “Configuring the Ethernet Interface.”

Configuring Synchronous WAN Port Parameters

Configure the synchronous WAN port with the values shown in Table 19-6. The IP address for the port is left unconfigured, accepting the default IP address value of 0.0.0.0.

Table 19-6 WAN Port Values

Setting	Command
Port type	set s1 network hardwired
Transport protocol	set s1 protocol ppp
IP destination	set s1 destination 192.168.200.1
Netmask	set s1 netmask 255.255.255.0
IPX network	set s1 ipxnet F3
Modem control	set s1 cd off
RIP routing	set s1 rip on
MTU	set s1 mtu 1500

If you are not sure of the IP address on the other end of the connection, you can set the IP destination to 255.255.255.255 and the PortMaster will attempt to learn the address.

Leave all other settings at their default values.

After you configure the port S1 as shown in Table 19-6, enter the following commands to reset the port and save the configuration:

```
Command> reset s1  
Command> save all
```

For more information about synchronous ports, refer to Chapter 6, “Configuring a Synchronous WAN Port.”

Troubleshooting a Leased Line Connection

Use the information in this section to debug your configuration.

If you have trouble with a leased line connection, verify the following:

- Enter the following commands to view the PPP negotiation on port S1, if this is the port you are using:

```
Command> set console s1
Command> set debug 0x51
Command> reset s1
```

For information about the interpreting the results of the debug command, refer to the *PortMaster Troubleshooting Guide*.

After you verify that the PPP negotiation is correct, enter the following commands to turn off the debug utility:

```
Command> set debug off
Command> reset console
```

- The error counters should be 0 (zero) except for abort errors. If your counters are nonzero, the problem is external to the PortMaster.



Note – CRC errors will occur if the cable is ever unplugged from the PortMaster.

- Verify that you are using the correct cable and that it is attached securely to the correct port. Not all WAN ports are capable of the same speeds.
- Verify that the DIP switch next to the synchronous port is set to V.35 for Lucent cables and that you are plugged into the correct V.35 interface on your CSU/DSU.
- Verify that the CSU/DSU is providing the clock to the PortMaster. The CSU/DSU can generate the clock or receive it from the carrier.
- Verify that the CSU/DSU is configured properly.
- If you have a Cisco router on the other end of your connection, make sure that it is running Cisco's software release 9.14(5) or later and is using PPP encapsulation, not High-Level Data Link Control (HDLC).
- If the framing errors are greater than 0, verify that the router on the other end of the connection is running the PPP protocol.

- If you still have problems, enter the following commands:

```
Command> set debug 0x51
```

```
Command> set console s1
```

Then set the CSU/DSU for local loopback. You should see the following message:

```
LCP_APPARENT_LOOP
```

For more information about the interpreting the results of the debug command, refer to the *PortMaster Troubleshooting Guide*.

- If the local loopback shows network connectivity in the local router, take the CSU/DSU out of loopback and set line loopback on the remote CSU/DSU. If the remote loopback test does not show network connectivity in the remote router, the problem is either in the configuration of one of the CSU/DSUs or in the line itself.
- When you finish, enter the following commands to turn off the debug utility:

```
Command> set debug off  
Command> reset console
```
- Contact your carrier to review your configuration and the status of their line.

This chapter describes general network concepts that you must understand before you configure your PortMaster.

This chapter discusses the following topics:

- “Network Addressing” on page A-1
- “Using Naming Services and the Host Table” on page A-8
- “Managing Network Security” on page A-9

See the *PortMaster Routing Guide* for information on routing and how Lucent’s ComOS implements routing protocols. See the glossary for unfamiliar terms.

Network Addressing

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

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

IP Addressing

IP address descriptions are found in RFC 1166, *Internet Numbers*. Refer to “Additional References” in the preface for more information. The Internet Network Information Center (InterNIC) maintains and distributes the RFC documents. The InterNIC also assigns IP addresses and network numbers to Internet Service Providers (ISPs), who in turn provide to their customers a range of addresses appropriate to the number of host devices on their network.

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

IP Address Notation

IP addresses are written in dotted decimal notation consisting of four numbers separated by dots (periods). Each number, written in decimal, represents an 8-bit octet (sometimes informally referred to as a byte) giving each number a range of 0 through 255, inclusive. When strung together, the four octets form the 32-bit IP address. Table A-1 shows 32-bit values expressed as IP addresses.

Table A-1 IP Address Notation

32-Bit Value	Dotted Decimal Notation
01100100.01100100.01100100.00001010	100.100.100.10
11000011.00100000.00000100.11001000	195.32.4.200

The largest possible value of a field in dotted decimal notation is 255, which represents an octet where all the bits are 1s.

IP Address Classes

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

The concept of classes is being made obsolete by classless interdomain routing (CIDR). Instead of dividing networks by class, CIDR groups them into address ranges. A network range consists of an IP address prefix and a netmask length. The address prefix specifies the high-order bits of the IP network address. The netmask length specifies the number of high-order bits in the prefix that an IP address must match to fall within the range indicated by the prefix.

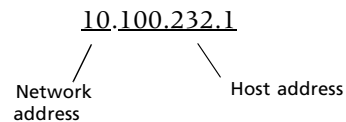
For example, 192.168.42.*x* describes a Class C network with addresses ranging from 192.168.42.0 through 192.168.42.255. CIDR uses 192.168.42.0/24 to describe the same range of addresses.

RIPv1 is an example of a protocol that uses address classes. OSPF and BGP-4 are examples of protocols that do not use address classes.

Class A Addresses

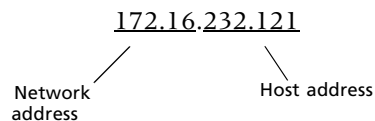
The class A IP address format allocates the highest 8 bits to the network field and sets the highest-priority bit to 0 (zero). The remaining 24 bits form the host field. Only 126 class A networks can exist (0 is reserved, and 127 is used for loopback networks), but each class A network can have almost 17 million hosts. No new class A networks can be assigned at this time.

For example:



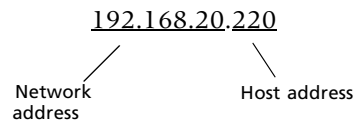
Class B Addresses

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



Class C Addresses

The class C IP address format allocates the highest 24 bits to the network field and sets the three highest-order bits to 1, 1, and 0, providing a range from 192 through 223, inclusive. The remaining 8 bits form the host field. More than two million class C networks can exist, and each class C network can have up to 254 hosts. For example:



Class D Addresses

The class D IP address format was designed for multicast groups, as discussed in RFC 988. In class D addresses, the 4 highest-order bits are set to 1, 1, 1, and 0, providing a range from 224 through 239, inclusive.

Class D addresses are currently used primarily for the multicast backbone (MBONE) of the Internet. Many routers, including those from Lucent, do not support MBONE or multicast and therefore ignore class D addresses.

Class E Addresses

The class E IP address is reserved for future use. In class E addresses, the 4 highest-order bits are set to 1, 1, 1, and 1. Routers currently ignore class E IP addresses.

Reserved IP Addresses

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

Table A-2 Reserved and Available IP Addresses

Class	IP Address	Status
A	0.0.0.0	Reserved
	1.0.0.0 through 126.0.0.0	Available
	127.0.0.0	Loopback networks on the local host
B	128.0.0.0	Reserved
	128.1.0.0 through 191.254.255.255	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 through 223.255.254.255	Available
	223.255.255.0	Reserved
D	224.0.0.0 through 239.255.255.255	Multicast group addresses
E	240.0.0.0 through 255.255.255.254	Reserved
	255.255.255.255	Broadcast

Private IP Networks

RFC 1597 reserves three IP network addresses for private networks. The addresses 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/20 can be used by anyone for setting up their own internal IP networks.

IP Address Conventions

If the bits in the host portion of an address are all 0, that address refers to the network specified in the network portion of the address. For example, the class C address 192.31.7.0 refers to a particular network. Historically, this address was used as a broadcast.

The standard for broadcast is high, which uses all 1s in the host portion (for example, 192.168.1.255); however, many networks still use all 0s. The PortMaster can be configured either way and should be set to match the other systems on your network.



Note – Do not assign an IP address with all 0s or all 1s in the host portion of the address to a host on the network, because these are reserved as broadcast addresses.

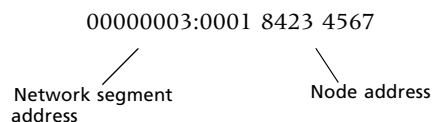
With CIDR, networks are specified with an IP prefix and netmask length—for example, 172.16.0.0/16, 192.168.1.0/24, or 192.168.200.240/28.

IPX Addressing

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

- Network segment address, expressed as 8 hexadecimal digits
These 4 bytes (32 bits) specify on which network segment the node resides.
- Node address, expressed as dotted triplets of 4-digit hexadecimal numbers
These 6 bytes (48 bits) provide the media access control (MAC) address of the node.

The two elements of the IPX address are separated by a colon. For example:



The first 8 digits represent the network segment, and the following 12 digits represent the node or MAC address of the node. All digits are expressed in hexadecimal.

Netmasks

A netmask is a four-octet number that identifies either a supernet (supernet) or a subnet (subnet). A netmask that designates a subnet is called a subnet mask.

Using Subnet Masks to Create IP Subnets

Subnet masks are used to divide networks into smaller, more manageable groups of hosts known as subnets. Subnetting is a scheme for imposing a hierarchy on hosts on a single physical network. The usual practice is to use the first few bits in the host portion of the network address for a subnet field. RFC 950, *Internet Standard Subnetting Procedure*, describes subnetting.

A subnet mask identifies the subnet field of a network address. This mask is a 32-bit number written in dotted decimal notation with all 1s (ones) in the network and subnet portions of the address, and all 0s (zeros) in the host portion. This scheme allows for the identification of the host portion of any address on the network.

Table A-3 shows the subnet masks you can use to divide a class C network into subnets.

Table A-3 Subnet Masks for a Class C Network

Length (Subnet Bits)	Number of Subnets	Number of Hosts per Subnet	Hexadecimal Subnet Mask	Dotted Decimal Subnet Mask
24	1	254	0xfffff00	255.255.255.0
25	2	126	0xfffff80	255.255.255.128
26	4	62	0xfffffc0	255.255.255.192
27	8	30	0xfffffe0	255.255.255.224
28	16	14	0xffffff0	255.255.255.240
29	32	6	0xfffffff8	255.255.255.248
30	64	2	0xfffffff0	255.255.255.252
32	256	1	0xffffffff	255.255.255.255

Subnetting, Routing, and VLSMs

Routers and hosts can use the subnet field for routing. The rules for routing on subnets are identical to the rules for routing on networks.

Releases before ComOS 3.5. Before ComOS 3.5, correct routing required all subnets of a network to be physically contiguous. The network must be set up so that it does not require traffic between any two subnets to cross another network. Also, RFC 950 implicitly required that all subnets of a network have the same number of bits in the subnet field. As a result, ComOS releases before ComOS 3.5 require the use of the same subnet mask for all subnets of a network. ComOS used the value of 255.255.255.255 for the user's *Framed-IP-Netmask* regardless of the value of the attribute.

ComOS 3.5 and Later Releases. ComOS 3.5 and subsequent releases support variable-length subnet masks (VLSMs); therefore, the restrictions in earlier ComOS releases no longer apply. The subnets of a network need not be physically contiguous and can have subnet masks of different lengths.

However, ComOS still ignores the *Framed-IP-Netmask* value by default. To ease the transition to use of VLSMs, ComOS sets **user-netmask** to **off** by default. This means that all netmasks specified in the user table or RADIUS are treated as if they were 255.255.255.255. To use VLSMs and have ComOS accept the value in *Framed-IP-Netmask*, enter the following commands:

```
Command> set user-netmask on
Command> save all
```



Caution – The VLSM feature affects both routing and proxy ARP on the PortMaster and should be used with caution.

Using Naming Services and the Host Table

Naming services are used to associate IP addresses with hostnames. Many networks use the Domain Name System (DNS) or the Network Information Service (NIS) for mapping hostnames to IP addresses. Both services are used to identify and locate objects and resources on the network. To use DNS or NIS, you must specify the IP address of the name server during the configuration process.

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



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

Managing Network Security

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

PortMaster security methods include

- Callback for remote access users
- Assignment of local passwords before connections are established
- Access control filters for host connections
- Inbound and outbound packet filtering
- IP packet filtering by protocol, source and destination address, and port
- IPX packet filtering by source and destination network, node, and socket
- SAP filtering
- PAP and CHAP authentication protocols for PPP connections
- Password security for administrative access
- Remote Authentication Dial-In User Service (RADIUS) support
- ChoiceNet filtering

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

RADIUS

RADIUS is a nonproprietary protocol invented by Lucent and described in RFC 2138 and RFC 2139. RADIUS provides an open and scalable client/server security system for distributed network environments. The RADIUS server can be adapted to work with third-party security products. Any communications server or network hardware that supports the RADIUS protocol can communicate with a RADIUS server.

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

ChoiceNet

ChoiceNet is a client/server packet-filtering application created by Lucent. ChoiceNet provides a mechanism to filter network traffic on dial-up remote access, synchronous leased line, or asynchronous connections. Filter information is stored in a central location known as the ChoiceNet server.

ChoiceNet clients can be one or more PortMaster products. ChoiceNet clients communicate with the ChoiceNet server to determine user access.

ChoiceNet can use filter names specified by the RADIUS user record. For more information about ChoiceNet, refer to the *ChoiceNet Administrator's Guide*.

TCP and UDP Ports and Services

B

Table B-1 lists common port numbers—**well-known ports**—assigned to TCP and UDP services—**well-known services**—by the Internet Assigned Network Numbers Authority (IANA). A more complete list is available in RFC 1700, “Assigned Numbers.”



Note – If you are configuring a filter on a PortMaster from the command line interface, you must use the port number. The PortMaster does not have the **/etc/services** file and cannot use NIS to get the equivalent information.

Table B-1 TCP and UDP Port Services

Service	Port	Protocol	Description
ftp-data	20	TCP	File Transfer Protocol (FTP) (default data)
ftp	21	TCP	FTP (control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer Protocol (SMTP) (email)
nickname	43	TCP	whois Internet directory service
nickname	43	UDP	whois Internet directory service
domain	53	TCP	Domain Name System (DNS)
domain	53	UDP	DNS
tftp	69	UDP	Trivial File Transfer Protocol (TFTP)
gopher	70	TCP	Gopher
gopher	70	UDP	Gopher
finger	79	TCP	Finger Protocol
finger	79	UDP	Finger Protocol
www-http	80	TCP	World Wide Web Hypertext Transfer Protocol (HTTP)
https	443	TCP	HTTP with SSL (secure HTTP)

Table B-1 TCP and UDP Port Services (Continued)

Service	Port	Protocol	Description
kerberos	88	TCP	Kerberos authentication
kerberos	88	UDP	Kerberos authentication
pop3	110	TCP	Post Office Protocol (POP) version 3
sunrpc	111	TCP	SUN Remote Procedure Call (RPC)
sunrpc	111	UDP	SUN RPC
auth	113	TCP	Authentication service
auth	113	UDP	Authentication service
nntp	119	TCP	Network News Transfer Protocol (NNTP)
ntp	123	TCP	Network Time Protocol (NTP)
ntp	123	UDP	NTP
snmp	161	TCP	Simple Network Management Protocol (SNMP)
snmp	161	UDP	SNMP
snmptrap	162	TCP	SNMP system management messages
snmptrap	162	UDP	SNMP system management messages
imap3	220	TCP	Interactive Mail Access Protocol (IMAP) version 3
imap3	220	UDP	IMAP version 3
exec	512	TCP	Remote process execution
login	513	TCP	Remote login
who	513	UDP	Remote who daemon (rwhod)
cmd	514	TCP	Remote command (rsh)
syslog	514	UDP	System log facility
printer	515	TCP	Line printer daemon (LPD) spooler
talk	517	TCP	Terminal-to-terminal chat
talk	517	UDP	Terminal-to-terminal chat

Table B-1 TCP and UDP Port Services (Continued)

Service	Port	Protocol	Description
ntalk	518	TCP	Newer version of Terminal-to-terminal chat
router	520	UDP	Routing Information Protocol (RIP)
uucp	540	TCP	UNIX-to-UNIX Copy Protocol (UUCP)
uucp	540	UDP	UUCP
uucp-rlogin	541	TCP	Variant of UUCP/TCP
uucp-rlogin	541	UDP	Variant of UUCP/IP
klogin	543	TCP	Kerberized login
klogin	543	UDP	Kerberized login
pmd	1642	TCP	PortMaster daemon in.pmd
pmconsole	1643	TCP	PortMaster Console Protocol
radius	1645	UDP	Remote Authentication Dial-In User Service (RADIUS)
radacct	1646	UDP	RADIUS accounting
choicenet	1647	UDP	ChoiceNet

Glossary

A

abort error

An error indicating an attempted and failed connection.

acceptance policy

A set of rules that determine the path and route information the PortMaster accepts from a BGP peer for further processing. See also **policy**.

address

A number used to identify a computer or other device on a network or internetwork. See also **IP address**; **MAC address**.

address resolution

A method for translating one type of address into another—for example, an IP address into a media access control (MAC) address.

Address Resolution Protocol

See **ARP**.

adjacency

A relationship between two routers on the same physical network or between the endpoints of a virtual link that controls the distribution of routing protocol packets by limiting their exchange to those routers or endpoints.

advertisement policy

A set of rules that determine the path and route information the PortMaster advertises to a BGP peer. See also **policy**.

agent

A software program installed in a managed network device. An agent stores management information and responds to the manager's request for this information.

aggregation

The process of combining multiple prefixes from one or several routes so that a single prefix and route can be advertised. Route aggregation reduces the amount of information that a device running BGP must store and exchange with its BGP peers. See also **summarization**.

Annex-D

The ANSI T1.617 Frame Relay Annex-D version of the Local Management Interface (LMI) protocol. The Annex-D protocol has a more robust feature set than the proprietary Cisco/Stratacom LMI, but was developed later. Recent versions of the PortMaster software support either type of LMI. Earlier versions supported only the Cisco/Stratacom version. See also **LMI**.

area

In OSPF, a contiguous collection of networks and hosts. Each area runs a separate copy of the shortest-path-first (SPF) algorithm and has its own topological database.

area border router

In OSPF, a router that attaches to the backbone and one other area. An area border router runs separate copies of the shortest-path-first (SPF) algorithm for each area it attaches to. Area border routers condense the topological information of their attached areas and distribute it over the backbone to the other areas.

ARP

Address Resolution Protocol. A protocol that discovers the unique physical hardware address of a node or a LAN from its IP address. When an ARP request is sent to the network, naming the IP address, the machine with that IP address returns its physical address so that it can receive the transmission.

ASCII

American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.

autonomous system

A collection of routers under the control of a single technical administration, using one or more Interior Gateway Protocols (IGPs)—such as OSPF—to route packets within itself, and an Exterior Gateway Protocol (EGP)—such as BGP—to route packets to other autonomous systems. An autonomous system typically uses a common BGP policy and always presents a consistent view of network reachability to other autonomous systems.

autonomous system border router

In OSPF, a router that exchanges information with routers from other autonomous systems. Autonomous system border routers are also used to import routing information about RIP, direct, or static routes from non-OSPF attached interfaces.

autonomous system path list

In BGP, the list of autonomous systems that a packet must traverse to reach a given set of IP address destinations located within a single autonomous system destination. The list can consist of **sequences**, which are series of autonomous systems that must be traversed in the order specified, and **sets**, which are collections of autonomous systems one of more of which must be traversed in any order to the destination.

For example, an autonomous system path list might consist of *Sequence 1, 2, 3, Set 4, 5, Sequence 6, 7*. This list indicates that a packet traverses autonomous systems 1, 2, and 3 in order, then one or both of autonomous systems 4 and 5 in any order, and finally autonomous systems 6 and 7 in order. Autonomous system 7 is the destination autonomous system.

B

backbone

A network topology consisting of a single length of cable with multiple network connection points.

backbone area

In OSPF, an area consisting of networks and routers not contained in any area and autonomous system border routers. The backbone area is responsible for distributing routing information between areas. This backbone area must be contiguous either physically or through a virtual link. The number reserved for the backbone area is 0.0.0.0.

backbone router

In OSPF, a router that has an interface into the backbone area by a direct attachment or a virtual link.

Basic Rate Interface

See **BRI**.

baud

The number of discrete signal events per second occurring on a communications channel. Although not technically accurate, baud is commonly used to mean bit rate.

B channel

Bearer channel. A 64Kbps synchronous channel that is part of an ISDN Basic Rate Interface (BRI).

BGP

Border Gateway Protocol. A routing protocol for exchanging network reachability information among autonomous systems. A routing device can use this information to construct a “map” of autonomous system connectivity. Version 4 of this protocol (BGP-4), which supports classless interdomain routing (CIDR) and route aggregation, is the predominant routing protocol used to propagate routes between autonomous systems on the Internet. BGP uses TCP as its transport protocol.

BGP-4

Version 4 of BGP. See also **BGP**.

BONDING

Bandwidth on Demand Interoperability Group. A method for combining two B channels into a single 128Kbps channel.

booting

The process in which a device obtains information and begins to process it to attain a state of normal operation.

BOOTP

Bootstrap Protocol. A protocol based on UDP and IP that enables a booting host to dynamically configure itself without user supervision. BOOTP provides a way for a host on a network to acquire its assigned IP address, the IP address of a boot server host, and a file to load into memory and run.

Bootstrap Protocol

See BOOTP.

Border Gateway Protocol

See **BGP**.

bps

Bits per second. A unit for measuring the data rate.

BRI

Basic Rate Interface. An ISDN interface that consists of two 64Kbps B channels for voice or data and one 16Kbps D channel for signaling. Compare **PRI**.

broadcast address

A special address reserved for sending a message to all stations. Generally, a broadcast address is a media access control (MAC) destination address of all 1s (ones).

broadcast packets

Packets that are sent to all network nodes.

C

callback

A port configuration allowing the PortMaster to call back dial-in users before providing access. Callback provides an extra layer of security and can simplify telephone charges.

CCITT

Consultative Committee for International Telegraph and Telephone. International organization formerly responsible for the development of communications standards. Now called the ITU-T. See also **ITU-T**.

CD

Carrier Detect. A signal that indicates whether an interface is active. Also, a signal generated by a modem indicating that a call has been connected.

Challenge Handshake Authentication Protocol

See **CHAP**.

channelized T1

An access link operating at 1.544Mbps that is subdivided into 24 channels of 56Kbps each for dial-in use.

channel service unit

See **CSU**.

CHAP

Challenge Handshake Authentication Protocol. A Point-to-Point Protocol (PPP) authentication method for identifying a dial-in user. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. See also **PAP**.

CIDR

Classless interdomain routing. A technique supported by BGP-4 that eliminates the necessity for network address classes by explicitly advertising the length (netmask) associated with each prefix.

CIR

Committed information rate. The minimum bandwidth guaranteed to be available if required on a virtual circuit. This value is also known as *guaranteed bandwidth*.

classless interdomain routing

See **CIDR**.

client/server environment

An environment where a computer system or process requests a service from another computer system. For example, a workstation can request services from a file server across a network.

cluster

A group of internal BGP peers that share a common set of route reflectors. See also **cluster ID**; **route reflection**; **route reflector**. Compare **confederation**.

cluster ID

An identifier, in dotted decimal format, that uniquely identifies a BGP route reflection cluster within an autonomous system. All route reflectors within the cluster must be configured with the same cluster ID. Internal peers that are not reflectors within the cluster must not be configured with a cluster ID. The cluster ID is typically set to the BGP router ID of one of the route reflectors within the cluster. See also **cluster**; **route reflection**; **route reflector**.

CMAS

Confederation member autonomous system. A subdivision of an autonomous system that is recognized only by other peers within the confederation and not by peers external to the confederation. Within the confederation, each BGP peer treats only the peers in its own CMAS as internal peers. Peers in different CMASs are treated as external peers.

committed information rate

See **CIR**.

community

A label that identifies a group of BGP destinations for the purpose of policy enforcement. Assembling destinations into identifiable “communities” lets BGP peers base policy decisions on the identity of the group rather than on individual destinations. The community identifier, which consists either of one 32-bit value or two 16-bit values, is advertised in update messages between BGP peers.

community string

A character string assigned to a Simple Network Management Protocol (SNMP) agent to restrict read and write access to the SNMP variables.

ComOS

The operating system for PortMaster communications servers, routers, and access servers.

confederation

In BGP, an autonomous system that has been subdivided into smaller autonomous systems called *confederation member autonomous systems*. (CMASs). A confederation appears like a single autonomous system to other autonomous systems and is recognized only by other confederation members. Subdivision of an autonomous system into a confederation changes the peer relationships of confederation members in different CMASs from internal to external. Use of confederations in an autonomous system requires that all routers in the autonomous system belong to a CMAS; however, the policies used by BGP peers can change across confederation boundaries.

Confederations are one method for avoiding the overhead of having all peers within an autonomous system fully communicate to—be fully meshed with—each other. Route reflection clusters provide an easier method, but require the use of identical policies on all peers within the autonomous system. See also **route reflection**.

confederation member

Any router running BGP and recognizing that its autonomous system is subdivided into smaller autonomous systems called *confederation member autonomous systems*. (CMASs). The CMASs are recognized only by confederation members and not by peers external to the confederation. Subdivision of an autonomous system into a confederation changes the peer relationships of confederation members in different CMASs from internal to external.

confederation member autonomous system

See **CMAS**.

console port

A serial port on a PortMaster attached to a terminal or PC through which you enter commands to communicate with ComOS.

CRC error

Cyclic redundancy check error. These errors can indicate problems with source station hardware, receivers, retiming modules and/or repeaters, bridges, cabling, or transceivers.

CSU

Channel service unit. An ancillary device needed to adapt the V.35 or X.21 interface to a port on a telephone carrier switch. The CSU is placed between the data terminal equipment (DTE) and the switch.

cyclic redundancy check

See **CRC error**.

D

data communications equipment

See **DCE**.

data link connection identifier

See **DLCI**.

data service unit

See **DSU**.

Data Set Ready

See **DSR**.

data terminal equipment

See **DTE**.

Data Terminal Ready

See **DTR**.

DCE

Data communications equipment. Devices and connections of a communications network that make up the network end of the interface between the network and the user. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal to synchronize data transmission between DCE and DTE devices. Modems and interface cards are DCEs.

DDE

Dynamic data exchange. A form of interprocess communication that uses shared memory to exchange data between applications. Applications can use a one-time data transfer or ongoing exchanges.

degree of preference

In BGP, an arbitrary rating number that the PortMaster assigns to every route it receives from a BGP peer. A higher number indicates a greater preference for a route when more than one exists to a destination. A route from an internal peer is assigned the local preference number that the PortMaster learned with the route. For a route learned from an external peer, the PortMaster calculates a number based on the autonomous system path length; the shortest path is preferred. You can use a routing policy rule to override the calculated or learned value and assign your own degree of preference to a route. See also **local preference**.

destination

In BGP, the final autonomous system in the autonomous system path whose IP address prefixes and associated netmasks are reported in the network layer reachability information (NLRI) field of an update message. A destination and its path comprise a BGP route. See also **path**; **route**.

DHCP

Dynamic Host Configuration Protocol. The underlying protocol for a network administration software tool that enables network managers to set up servers to automatically supply IP addresses and configuration settings to clients. DHCP extends and enhances the BOOTP protocol by providing reusable IP addresses and allocating IP addresses based on subnet, client ID string, or media access control (MAC) address.

dialback

See **callback**.

dial group

A number that is used to associate dial-out locations with ports.

digital service unit

See **DSU**.

direct memory access

See **DMA**.

DLCI

Data link connection identifier. A unique number that represents a particular permanent virtual circuit (PVC) on a particular physical segment of the Frame Relay network. As the frame is passed through each switch, the DLCI is remapped automatically by the switch as necessary.

DMA

Direct memory access. Transfer of data from a peripheral device, such as a hard disk drive, into a computer memory without mediation by a microprocessor.

DNS

Domain Name System. The system used on the Internet for translating the names of network hosts into IP addresses.

DRAM

Dynamic random access memory. A type of semiconductor random access memory (RAM) that stores information in integrated circuits containing capacitors.

DSR

Data Set Ready. The circuit that is activated when data communications equipment (DCE) is powered up and ready for use. See also **DCE**.

DSU

Digital service unit or data service unit. An ancillary device needed to adapt the physical interface on a data terminal equipment (DTE) device—such as a V.35 interface on a port—to a transmission facility—such as leased line or a Frame Relay switch. If the DTE lacks complete digital line interface capability, the DSU can be located with the channel service unit (CSU) on the customer's site and known as a CSU/DSU. See also **CSU**.

DTE

Data terminal equipment. A device at the user end of the interface between the network and the user. The DTE connects to a data network through a data communications equipment (DCE)—such as a modem or an interface card. DTEs convert user information into data signals for transmission, and reconvert received data signals into user information. Compare **DCE**.

DTR

Data Terminal Ready. The circuit that is activated to inform the data communications equipment (DCE) when the data terminal equipment (DTE) is ready to send and receive data. See also **DCE**; **DTE**.

dynamic data exchange

See **DDE**.

Dynamic Host Configuration Protocol

See **DHCP**.

dynamic random access memory

See **DRAM**.

E**E1**

Digital WAN carrier facility used predominantly in Europe that carries data at a rate of 2.048Mbps. E1 lines can be leased for private use from common carriers. Compare **T1**.

easy-multihome

A specialized, predefined BGP policy that simplifies the use of PortMaster routers in straightforward multihomed environments. When you define easy-multihome for a peer, you restrict what the PortMaster handles from the peer to information that is no more than two autonomous system hops away from the PortMaster. Only information that meets this criterion is accepted from the peer, put into the routing table used to forward packets to their destinations, and advertised to other peers. If you define easy-multihome for a peer, you must also define a default route on each router in your autonomous system to point them to destinations more distant than two hops. See also **multihome routing; policy**.

EBGP

Exterior BGP. The BGP used between peers in different autonomous systems, or, when confederations are in use, between peers in different confederation member autonomous systems (CMASs). Unlike internal BGP peers, EBGP peers need not have full connectivity with one another.

endpoint discriminator

A 12-digit identifier used to associate multiple chassis in a Multichassis PPP domain.

echo test

A diagnostic test used to check network reachability in which an Internet Control Message Protocol (ICMP) Echo Request packet or Simple Network Management Protocol (SNMP) test packet is sent to elicit a standard response.

Ethernet

A network communications system developed and standardized by Digital Equipment Corporation, Intel, and Xerox using baseband transmission, carrier sense multiple access/carrier detect (CSMA/CD) access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration of Ethernet into the Open System Interconnection (OSI) model and extends the physical layer and media with repeaters and implementations that operate on fiber optic cable, broadband, and unshielded twisted pair.

external peer

A peer that resides in a different autonomous system—or, when confederations are in use, in a different confederation member autonomous system (CMAS)—from the current PortMaster.

Exterior BGP

See **EBGP**.

F

File Transfer Protocol

See **FTP**.

filter

Generally, a process or device that screens network traffic for certain characteristics, such as source address, destination address, or protocol, and determines whether to forward or discard that traffic based on the established criteria.

filter table

A database used to store filters.

Flash RAM

See **nonvolatile RAM**.

flow control

A technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed. Flow control can be software-based, or hardware-based.

FRAD

Frame Relay access device. A network device that links any non-Frame Relay connection to a Frame Relay WAN.

frame

A packaging structure for network data and control information. A frame consists of a destination address, source address, length field, data, padding, and frame check sequence. The 802.3 standard for Ethernet specifies that the minimum size data frame is 64 bytes and the maximum size data frame is 1518 bytes.

Frame Relay

An industry-standard switched data link layer protocol that handles multiple virtual circuits using high-level data link layer control (HDLC) encapsulation between connected devices. It is used across the interface between user devices (for example, hosts and routers) and network equipment (for example, switching nodes). Frame Relay is more efficient than X.25, the protocol it replaced.

Frame Relay access device

See **FRAD**.

FTP

File Transfer Protocol. A TCP/IP protocol used to transfer files between network hosts.

G

gateway

A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

graphical user interface

See **GUI**.

GUI

Graphical user interface. A software interface based on pictorial representations and menus of operations and files.

H

hardwired

A continuous connection between two sites. A port on a PortMaster that is configured for hardwired use cannot be simultaneously used for any other type of connection.

hello

Protocol used by OSPF routers to acquire neighbors and to synchronize their topological databases.

high-water mark

The number of bytes of queued network traffic required to open an additional dial-out line to a remote location.

hop

The transmission of a data packet between two network nodes—for example, between two routers.

hop count

Measurement of the distance between a source and destination that is used as a metric to compare routes. If a packet traverses six routers between source and destination nodes, the hop count for the packet will be 6 when it arrives at its destination node.

host

A single, addressable device on a network. Computers, networked printers, and routers are hosts.

hunt group

A group of multiple telephone circuits that allows telephone calls to find an idle circuit to establish a link.

I

IBGP

Interior BGP. The BGP used between peers in the same autonomous system, or, when confederations are in use, between peers in the same confederation member autonomous system (CMAS). All IBGP peers must maintain direct BGP connections to—be **fully meshed** with—every other internal peer, but need not be physically attached to one another.

ICMP

Internet Control Message Protocol. The part of the Internet Protocol (IP) that allows for generation of error messages, test packets, and informational messages related to IP. This protocol is used by the ping function to send an ICMP Echo Request to a network host, which replies with an ICMP Echo Reply.

in-band signaling

Signaling over the data path.

injection policy

A set of rules that determine the path and route information the PortMaster takes from BGP and places into its routing table used to forward packets to their destinations. The PortMaster uses the information to determine how packets it receives are forwarded to their ultimate destinations. See also **policy**.

interface

Connection and interaction between hardware, software, and the user. The interface between components in a network is called a protocol. On the PortMaster, the virtual connection between a PortMaster port and the network to which it is connected is called an interface. The connection can be permanent as with the Ethernet interface or network hardwired ports, or it can be temporary, as with ports used for dial-in or dial-out connections.

Integrated Services Digital Network

See **ISDN**.

Interior BGP

See **IBGP**.

internal peer

A peer that resides in the same autonomous system—or, when confederations are in use, in the same confederation member autonomous system (CMAS)—as the current PortMaster.

internal router

In OSPF, a router with all of its directly connected interfaces or physical networks belonging to the same area and containing no virtual connections to the backbone area.

International Organization for Standards

See **ISO**.

internetwork

A network of networks.

Internet

The world-wide internetwork consisting of several large national backbone networks and several regional and campus networks.

Internet Control Message Protocol

See **ICMP**.

Internet Protocol

See **IP**.

Internet Network Information Center

See **InterNIC**.

InterNIC

Internet Network Information Center. An organization that provides information and services related to networking technologies.

IP

Internet Protocol. The protocol defined in RFC 791.

IP address

A 32-bit number assigned by the system administrator, usually written in the form of four decimal fields separated by periods—for example, 192.9.200.1. Any computing device that uses IP must be assigned an Internet or IP address. Part of the Internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address.

IP address prefix

An IP address number that, when paired with a netmask length, represents a range of addresses rather than a single IP network. For example, the prefix and netmask length 128.0.0.0/8 describe all networks whose IP addresses begin with 128. See also **netmask length**.

IP Control Protocol

See **IPCP**.

IPCP

IP Control Protocol. A protocol used by the Point-to-Point Protocol (PPP) for establishing and configuring an IP link over PPP.

IPX

Internet Packet Exchange. Internet protocol defined by Novell, Inc.

IPXWAN

IPX Wide Area Network protocol. The protocol used to establish and configure an IPX link over the Point-to-Point Protocol (PPP), as described in RFC 1634.

IPX Wide Area Network

See **IPXWAN**.

ISDN

Integrated Services Digital Network. A digital communications standard designed to allow the transmission of voice, data, images, and video over existing copper phone lines.

ISO

International Organization for Standards. The international organization that sets standards for network communication protocols.

ITU-T

International Telecommunication Union Telecommunication Standardization Sector. International organization that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT. See also **CCITT**.

K

KB

Kilobyte(s). 1024 bytes.

Kb

Kilobit(s). 1024 bits.

Kbps

Kilobits per second.

keepalive message

A periodic message sent between BGP peers to keep their BGP sessions open. If a preset amount of time elapses between keepalive messages from a peer, the PortMaster identifies the peer as no longer operational and drops the session—and any information learned from that peer.

L

LAN

Local area network. A local collection, usually within a single building or several buildings, of personal computers and other devices connected by cabling to a common transmission medium, allowing users to share resources and exchange files. Compare **WAN**.

latency

1) The delay between the time a device requests access to a network and the time it is granted permission to transmit. 2) The delay between the time when a device receives a frame and the time that frame is forwarded out the destination port.

LCP

Link Control Protocol. The protocol used by the Point-to-Point Protocol (PPP) for establishing, configuring, and testing the data link connection.

LED

Light-emitting diode.

line speed

The speed of the physical wire attached to the interface or interface hardware. The line speed is 10Mbps for Ethernet and 1.544Mbps for T1. Fractional T1 is often implemented with a wire speed of T1 (1.544Mbps) and a lower port speed. Upgrading line speed is generally a hardware change. See also **port speed**.

Link Control Protocol

See **LCP**.

link state advertisement

See **LSA**.

LMI

Local Management Interface. A protocol used to communicate link status and permanent virtual circuit (PVC) status in Frame Relay. Two types of LMI are available on Frame Relay: the original proprietary Cisco/Stratacom LMI, and the ANSI T1.617 Annex-D LMI. Although the PortMaster supports both, LMI on the PortMaster refers to the Cisco/Stratacom implementation. See also **Annex-D**.

local area network

See **LAN**.

Local Management Interface

See **LMI**.

local preference

In BGP, the degree-of-preference number that the PortMaster assigns to every external route it advertises to an internal or confederation-member BGP peer. A higher number indicates a greater preference for a route when more than one exists to a destination. Internal and confederation-member peers receiving this route use this local preference rather than calculating their own degree of preference for a route. You can use a routing policy rule to override this value and assign your own local preference to a route you advertise. See also **degree of preference**.

location

A dial-out destination.

location table

A database on the PortMaster where location settings are stored. See **location**.

lockstep

A feature of BGP on the PortMaster that ensures consistency of routing information between the BGP and non-BGP routers within its autonomous system. Lockstep forces the PortMaster to advertise a route learned from an internal BGP peer only when it has learned the same route via an Interior Gateway Protocol (IGP)—OSPF or RIP—or a static route. See also **transit service**.

LSA

Link state advertisement. The state of the router links (interfaces), networks, summaries, or autonomous system external links of an OSPF router that it periodically advertises. Link states are also advertised when a link state changes.

M

MAC address

Media access control address. A unique 48-bit binary number—usually represented as a 12-digit hexadecimal number—encoded in the circuitry of a device to identify it on a LAN.

Management Information Base

See **MIB**.

management station

A workstation or PC capable of retrieving and analyzing statistical information from networked Simple Network Management Protocol (SNMP) agents.

master

In Multichassis PPP, the PortMaster through which an initial connection for a given user is made. Every master also has a corresponding slave. Masters are for a given connection only, and a PortMaster that functions as a master for one user's connection can be a slave for a different user's connection. See also **slave**.

maximum transmission unit

See **MTU**.

MB

Megabyte(s). 1,048,576 bytes.

Mbps

Megabits per second. A unit for measuring data rates.

MD5

Message digest algorithm 5. The algorithm used for message authentication in Simple Network Management Protocol (SNMP) v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. ComOS uses the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

media access control address

See **MAC address**.

message digest algorithm 5

See **MD5**.

MIB

Management Information Base. A set of variables that a Simple Network Management Protocol (SNMP)-based management station can query from the SNMP agent of a network device.

modem

Modulator-demodulator. A device that converts the digital signals used by computers to analog signals that can be transmitted over telephone lines.

modem table

A database resident on the PortMaster containing configuration information for commonly used modems.

MTU

Maximum transmission unit. The largest frame or packet that can be sent through a port on a PortMaster without fragmentation.

Multichassis PPP

Multilink PPP over two or more chassis.

Multilink PPP

A protocol defined in RFC 1990 that allows a PortMaster to automatically bring up additional ISDN B channels as bandwidth needs increase. See also **Multichassis PPP**.

multiexit discriminator

In BGP, an arbitrary rating number that the PortMaster can use to enforce the use of preferred exit and entry points when multiple connections exist between its autonomous system and another. The PortMaster assigns the multiexit discriminator to any route that it advertises to its external peers, and forwards any multiexit discriminator it learns from its external peers on to its internal peers. A lower number indicates a greater preference for a route when more than one exists to a destination through multiple peers within the same neighboring autonomous system. You can use a routing policy rule to override this value and assign your own multiexit discriminator to a route that you learn or advertise.

multihome routing

In BGP, the process of choosing among multiple exit points to route packets out of a single autonomous system, typically to the Internet. Routers in a multihomed autonomous system usually store large amounts of network reachability information to help them select the best exit point. See also **easy-multihome**.

multiline load balancing

The ability of a PortMaster to add additional lines when network traffic is heavy. If more than one line to a remote location is established, the PortMaster balances the traffic among the lines. Distinct from Multilink PPP.

N

name server

A server connected to a network that resolves hostnames into network addresses.

name service

The software system that provides a database of authorized users for a computer, subnet, or network. The system can reside on one device, or be distributed across several devices in a network.

neighbor

- (1) In OSPF, two routers that have interfaces to a common network are neighbors. On multiaccess networks, neighbors are dynamically discovered by the OSPF Hello protocol.
- (2) In Multichassis PPP, PortMasters in the same Multichassis PPP domain.

netmask

A 32-bit number that distinguishes the portion of an IP address referring to the network or subnet from the portion referring to the host. Compare **subnet mask**.

netmask length

A number between 0 and 32 preceded by a slash (/) and following an IP address prefix. The netmask length indicates the number of high-order bits in the prefix that an IP address must match to fall within the range indicated by the prefix. For example, the prefix and netmask length 128.0.0.0/8 describe all networks whose IP addresses begin with 128. See also **IP address prefix**.

network

A collection of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances.

network handle

A number assigned to an active socket that can be used to close the socket manually, rather than by a request from the client.

network interface card

See **NIC**.

Network Information Service

See **NIS**.

network layer reachability information

See **NLRI**.

network management

In the Open System Interconnection (OSI) model, the five functional application areas of accounting management, configuration management, fault management, performance management, and security management.

NIC

Network interface card. A card that provides network communication capabilities to and from a computer system. A NIC is also known as an *adapter*.

NIS

Network Information Service. A protocol developed by Sun Microsystems for the administration of network-wide databases.

NLRI

Network layer reachability information. The part of a BGP route containing the IP address prefixes and associated netmask lengths that are reachable via the path described in the route. The networks indicated by these prefixes and netmasks reside in the destination autonomous system—the final one listed in the path.

node

A device, such as a PC, server, switching point, bridge, or gateway, connected to a network at a single location. A node can also be called a *station*. See **host**.

nonvolatile RAM

See **NVRAM**.

notification message

A message sent between BGP peers to inform the receiving peer that the sending peer must terminate the BGP session because an error occurred. The message contains information that explains the error. See also **keepalive message**; **open message**; **update message**.

not-so-stubby-area

See **NSSA**.

NSSA

Not-so-stubby-area. In OSPF, an area similar to a stub area except that Type 1 and Type 2 external routes can be learned from it. Any external routes learned from an NSSA are translated into Type 1 and Type 2 external routes for the backbone area or other areas that accept external routes. Like stub areas, NSSAs can have default costs set for them but cannot have external routes advertised into them.

NT1

Network termination 1 device. The device that provides an interface between the ISDN Basic Rate Interface (BRI) line used by the telephone company and a customer's terminal equipment. The NT1 also provides power for the terminal equipment, if necessary. In North America, where ISDN BRI is a U loop, the customer must supply the NT1 device; in Japan and the European countries where BRI is an S/T bus, the telephone company supplies the NT1. The PortMaster integrates the NT1 device into its ISDN BRI ports that are U interfaces.

NVRAM

Nonvolatile random access memory. Nonvolatile storage that can be erased and reprogrammed electronically, allowing software images to be stored, booted, and rewritten as necessary.

O**ODI**

Open Datalink Interface. A Novell specification that isolates the protocol stack from the network adapter drivers to provide hardware independence for network connectivity.

Open Datalink Interface

See **ODI**.

open message

A message sent between BGP peers to establish communication. See also **keepalive message**; **notification message**; **update message**.

Open Shortest Path First

See **OSPF**.

OSPF

Open Shortest Path First. A link-state interior gateway routing protocol designed for a hierarchical routing structure. OSPF chooses routes on a best-path, least-cost basis and supports variable-length subnet masks (VLSMs) for "classless" networking, allows up to 255 hops between routers, and provides packet authentication. See also **RIP**.

out-of-band connection

A remote connection, or a connection outside connected networks, established over a modem. This type of connection is useful when network communications are not available.

P

packet

A unit of data sent across a network.

PAP

Password Authentication Protocol. An authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike the Challenge Handshake Authentication Protocol (CHAP), PAP passes unencrypted passwords. PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. See also **CHAP**.

parity check

A process for checking the integrity of a character. A parity check appends a bit to a character or word to make the total number of binary 1 digits in the character or word (excluding the parity bit) either odd (for odd parity) or even (for even parity).

partition

Electronic isolation of an Ethernet device from network communications.

Password Authentication Protocol

See **PAP**.

path

In BGP, a autonomous system path list and a collection of attributes that provide descriptions of and explain how to reach a given collection of IP address destinations in a single autonomous system. A path and its destination comprise a BGP route. See also **destination; autonomous system path list; route**.

peer

(1) In BGP, a router with which a BGP speaker exchanges open messages, notification messages, update messages, and keepalive messages. A PortMaster can have both internal and external peers. See also **internal peer; external peer**.

(2) In Multichassis PPP, the relationship between a master and slave. A peer is distinct from a *neighbor*.

permanent virtual circuit

See **PVC**.

physical circuit

A physical connection between two devices.

ping

Packet Internet Groper. A program that is useful for testing and debugging networks. Ping sends an ICMP echo packet to the specified host and waits for a reply. Ping reports success or failure and sometimes statistics about its operation.

Point-to-Point Protocol

See **PPP**.

policy

In BGP, the rule or set of rules the PortMaster follows for accepting, injecting, and/or advertising BGP routes to its BGP internal and external peers. You assign policies to a peer when you add it to the PortMaster during configuration. You can use the default policy **easy-multihome**, or create and assign your own policies. One policy can handle all three functions, or you can create separate policies for acceptance, injection, and advertisement. See also **acceptance policy**; **advertisement policy**; **injection policy**.

port

The physical channel or connection through which data flows.

port speed

The rate at which data is accepted by the port at the end of the wire. For example, when a T1 line exists between a site and a telecommunications provider, the telecommunications provider accepts only the number of bits per second ordered by the customer into the port on its equipment. Upgrading port speed is generally a software change.

PPP

Point-to-Point Protocol. A protocol that provides connections between routers and between hosts and networks over synchronous and asynchronous circuits. See also **SLIP**.

PRI

Primary Rate Interface. The ISDN interface to primary rate access. Primary rate access consists of a single 64Kbps D channel plus 23 (T1) or 30 (E1) 64Kbps B channels for voice or data. Compare **BRI**.

Primary Rate Interface

See **PRI**.

propagation

The process of translating and forwarding routes from one routing protocol into another. Route propagation is also known as route *redistribution*. Lucent Remote Access recommends using route filters in propagation rules to ensure that you redistribute information without creating routing loops. Compare **summarization**.

provisioning

The process of supplying telecommunications service and equipment to a user. In ISDN provisioning, for example, a telephone service provider configures its own switch that connects via an ISDN line to the user's ISDN hardware. Because switch configuration varies according to hardware, telephone company, switch, and available ISDN line, user and provider must work together to establish the correct settings.erc

proxy Address Resolution Protocol

See **proxy ARP**.

proxy ARP

Proxy Address Resolution Protocol. A variation of the ARP protocol in which a router or other device sends an ARP response to the requesting host on behalf of another node. Proxy ARP can reduce the use of bandwidth on slow-speed WAN links. See also **ARP**.

PVC

Permanent virtual circuit. A circuit that defines a permanent connection in a switched digital service such as Frame Relay. Frame Relay is the only switched digital service that uses PVCs supported by PortMaster products.

R

RADIUS

Remote Authentication Dial-In User Service. A client/server security protocol created by Lucent.

RARP

Reverse Address Resolution Protocol. A protocol used in network routers that provides a method for finding IP addresses based on media access control (MAC) addresses. Compare **ARP**.

Remote Authentication Dial-In User Service

See **RADIUS**.

Request for Comments

See **RFC**.

Reverse Address Resolution Protocol

See **RARP**.

RFC

Request for Comments. One of a series of documents that communicate information about the Internet. Most RFCs document protocol specifications, such as those for IP and BGP. Some RFCs are designated as standards.

RIP

Routing Information Protocol. A protocol used for the transmission of IP or IPX routing information.

rlogin

Remote login. A terminal emulation program, similar to Telnet, offered in most UNIX implementations.

route

A way for a packet to reach its target via the Internet. A BGP route provides a path of autonomous systems—plus any path attributes—to a single destination autonomous system that contains particular IP address prefixes and associated netmasks. Packets whose targets fall within the networks identified by these prefixes and netmasks can use this BGP route. BGP peers advertise routes to each other in **update messages**.

router

A device that connects two or more networks and can direct traffic based on addresses.

route reflection

In BGP, a method for maintaining path and attribute information across an autonomous system, while avoiding the overhead of having all peers within an autonomous system fully communicate to—be fully meshed with—each other. To reduce the number of links, all internal peers are divided into clusters, each of which has one or more route reflectors. A route received by a route reflector from an internal peer is transmitted to its clients, which are the other peers in the cluster that are not route reflectors. Route reflection requires that all internal peers use identical policies.

Confederations are another way to avoid configuring a fully meshed set of peers in a single autonomous system. In contrast to route reflection clusters, confederations require all routers in the autonomous system to operate as confederation members. However, confederations provide a finer control of routing within the autonomous system by allowing for policy changes across confederation boundaries. See also **cluster**; **cluster ID**; **confederation**; **route reflector**.

route reflector

A router configured to transmit routes received from internal BGP peers to one or more other internal peers within its same cluster. These peers are called the route reflector's *clients*. See also **cluster**; **cluster ID**; **route reflection**.

router ID

One of the interface addresses configured on a BGP speaker. The router ID is chosen as the address that uniquely identifies the BGP speaker on the Internet.

Routing Information Protocol

See **RIP**.

routing table

A database of routes to particular network destinations, stored on a router or other device. The routing table stored on the PortMaster contains the following information for each route: IP address and netmask length of the destination, IP address of the gateway, source of the route (if any), type of route, hop-count metric, and PortMaster interface used to forward packets along the route.

RS-232 interface

A standard for data communication using serial data and control signals.

runt packet

A packet with a frame size between 8 and 63 bytes with frame check sequence (FCS) or alignment errors. The runt packet is presumed to be a fragment resulting from a collision.

S

SAP

Service Advertisement Protocol. An IPX protocol that provides a means of informing network clients, via routers and servers, of available network resources and services. See also **IPX**.

Serial Line Internet Protocol

See **SLIP**.

serial port

A bidirectional channel through which data flows one bit at a time. Asynchronous serial ports most often use 10 bits for a character of data including 1 start bit, 8 data bits, and 1 stop bit.

server

A computer or a specialized device that provides and manages access to shared network resources, such as hard disks and printers.

Service Advertisement Protocol

See **SAP**.

service profile identifier

See **SPID**.

Simple Network Management Protocol

See **SNMP**.

slave

In Multichassis PPP, a PortMaster through which a subsequent connection for a particular user is made. (The port through which the connection is made is called the **slave port**.) Every slave has a corresponding master. Slaves are for a given connection only, and a PortMaster that functions as a slave for one user's connection can be a master for a different user's connection. See also **master**.

SLIP

Serial Line Internet Protocol. The protocol, obsoleted by the Point-to-Point Protocol (PPP), for point-to-point serial connections using TCP/IP. See also **PPP**.

SNMP

Simple Network Management Protocol. A protocol defined in RFC 1157, used for communication between management consoles and network devices.

speaker

A single BGP router that is able to communicate with other routers that run BGP. When two BGP speakers communicate with each other, they are called BGP *peers*.

SPID

Service profile identifier. A number used by some service providers to define the services to which an ISDN device subscribes. The ISDN device uses the SPID when accessing the switch that initializes the connection to a service provider.

station

See **host**.

stub area

In OSPF, an area into which no external routes are imported. A stub area cannot contain autonomous system border routers and cannot be a transit area for virtual links. Summary advertisements external to the area are by default imported into the stub area but might be squelched to further reduce area database size. In this case, the default route advertisement by the autonomous system border routers handle all routes external to the area.

subnet mask

A 32-bit netmask used to indicate the bits of an IP address that are being used for the subnet address. Compare **netmask**.

summarization

The process of combining routing information from one routing protocol into another for advertisement. For example, the PortMaster summarizes non-BGP route information it receives internally via the Interior Gateway Protocol (IGP) OSPF or RIP, or via a static route, into BGP for advertisement to BGP internal and external peers. Summarized routing information must comply with BGP advertisement policy rules before advertisement. Compare **propagation**.

SVC

Switched virtual circuit. A connection established between two physical circuits, such as an ordinary telephone call. The call creates a virtual circuit between the originator and the party called.

switched virtual circuit

See **SVC**.

T

T1

Digital WAN carrier facility used to transmit data formatted for digital signal level 1 (DS-1) at 1.544Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS) coding. Compare **E1**.

TCP/IP

An open network standard that defines how devices from different manufacturers communicate with each other over interconnected networks. TCP/IP protocols are the foundation of the Internet.

Telnet

The Internet standard protocol, described in RFC 854, for remote terminal connection service.

terminal adapter

A device that provides ISDN compatibility to non-ISDN devices. An asynchronous terminal adapter turns an asynchronous bit stream into ISDN and is treated by the PortMaster as if it were a modem. A synchronous terminal adapter takes a synchronous bit stream and turns it into ISDN, typically supports V.25bis dialing, and connects to a PortMaster synchronous port. Some terminal adapters can be configured for either synchronous or asynchronous operation.

terminal emulator

A program that makes a PC screen and keyboard act like the video display terminal of another computer.

TFTP

Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) that transfers files but does not provide password protection or user directory capability. TFTP can be used by diskless devices that keep software in ROM and use it to boot themselves. The PortMaster can be booted from the network by means of Reverse Address Resolution Protocol (RARP) and TFTP.

transit service

In BGP, the function provided by an autonomous system that is in the path of a route but not the origination or destination. To provide reliable transit service, an autonomous system must ensure that its BGP and non-BGP routers agree on the interior routes and exit and entry points for each transit route through the autonomous system. The PortMaster synchronizes routing information between the BGP and non-BGP routers within its autonomous system by means of the **lockstep** feature. See also **lockstep**.

Trivial File Transfer Protocol

See **TFTP**.

two-way

Relating to a port configuration that allows both incoming and outgoing calls.

U

UDP

User Datagram Protocol. A connectionless protocol defined in RFC 768. UDP exchanges datagrams but does not provide guaranteed delivery.

U interface

The ISDN interface defined as the connection between the network termination 1 device (NT1) and the telephone company local loop. The U interface standard is set by each country. The U interface described in PortMaster documentation refers to the U.S. definition.

UNIX

A multiuser, multitasking operating system originally developed by AT&T that runs on a wide variety of computer systems.

UNIX-to-UNIX Copy Program

See **UUCP**.

update message

A message sent between BGP peers to convey network reachability information in two parts. The first part lists the IP address prefixes and associated netmasks for one or more routes that the PortMaster is withdrawing from service because it can no longer reach them. The second part of an update message consists of a single BGP route. See also **route**.

User Datagram Protocol

See **UDP**.

UUCP

UNIX-to-UNIX Copy Program. Interactive communication system for connecting two UNIX computers to send and receive data.

V

V.120

An ITU-T standard for performing asynchronous rate adaptation into ISDN.

V.25bis

An ITU-T standard defining how to dial on synchronous devices such as ISDN or switched 56Kbps.

V.32bis

An ITU-T standard that extends the V.32 connection range from 4800bps to 14.4Kbps. V.32bis modems fall back to the next lower speed when line quality is impaired, and fall back further as necessary. They fall forward to the next higher speed when line quality improves.

V.34

An ITU-T standard that allows data rates as high as 28.8Kbps.

V.35

The ITU-T standard for data transmission at 48Kbps over 60kHz-to-108kHz group band circuits. It includes the 35-pin V.35 connector specifications normally implemented on a modular RJ-45 connector.

variable-length subnet mask

See **VLSM**.

virtual circuit

A logical connection between two endpoints on a switched digital network. Virtual circuits can be switched or permanent. A switched virtual circuit (SVC) is used when you make an ordinary telephone call, an ISDN connection, or a V.25 switched 56Kbps connection. A permanent virtual circuit (PVC) is used in Frame Relay. See also **PVC**; **SVC**.

virtual connection

In Multichassis PPP, a connection made when a slave forwards all the packets it receives for a particular connection to its corresponding master for processing.

virtual port

In Multichassis PPP, a port corresponding to the physical port of the slave.

virtual private network

See **VPN**.

VLSM

Variable-length subnet mask. A means of specifying a different subnet mask for the same network number on different subnets. VLSM often allows addresses to be assigned more efficiently. OSPF and BGP support “classless” or VLSM routes.

VPN

Virtual private network. A restricted network that uses public wires to connect nodes. A VPN provides a way to encapsulate, or “tunnel,” private data cheaply, reliably, and securely through a public network, usually the Internet. IP packets are encapsulated in a VPN protocol. VPNs use encryption and other security mechanisms to prevent unauthorized users from accessing the network and intercepting the data.

W

WAN

Wide area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay is an example of a WAN. Compare **LAN**.

Command Index

A

add dlci 13-15
add filter 9-5
add location 8-3, 12-14, 12-19, 13-15, 14-6,
14-11, 15-7, 15-11, 16-7
add location sub1 13-13
add modem 10-3
add netmask 3-28
add netuser 7-2, 12-13, 12-18, 14-5, 14-10,
15-6, 15-10, 17-10
add route Ippaddress 3-25
add route Ipxnetwork 3-26
add subinterface 4-7
add user 7-2, 17-9

D

delete filter 9-8
delete route Ippaddress 3-25
delete route Ipxnetwork 3-26
delete user 7-3
dial 8-14, 12-20, 14-12, 14-13, 15-12, 16-8

R

reboot 11-11
reset 6-7
reset all 10-6
reset console 11-16, 12-20, 12-21, 12-22,
13-12, 13-14, 14-12, 14-13, 19-8
reset S0 5-9, 5-21, 5-25, 10-6, 12-13, 12-20
reset V0 11-15

reset W1 6-11

S

save all 5-9, 5-13, 5-16, 5-19, 5-21, 5-25,
6-11, 11-11, 12-5, 12-6, 13-15
save route 3-26
set accounting 17-8
set all 17-6
set all cd 17-7
set all databits 5-4
set all idletime 5-8
set all login 5-9
set all login network dialin 17-7
set all modem 10-6, 17-7
set all override 5-3
set all rts/cts 5-4, 17-7
set all security 17-7
set all speed 5-4, 10-7, 17-7
set all termtype 5-9, 5-11
set all xon/xoff 5-4
set alternate 17-8
set assigned 17-5
set assigned_address 3-12
set authentic 17-8
set call-check 3-30
set chap 3-30
set compression 6-11
set console 3-9, 5-7, 11-16, 12-20, 12-21,
12-22, 13-12, 13-14, 14-12, 14-13,
15-12, 16-8, 17-10, 19-8

set debug 12-20, 12-22, 13-12, 13-14, 14-12,
14-13, 15-12, 16-8, 17-10, 19-8
set debug isdn 12-5, 12-20, 12-21, 14-12
set debug mcppp 11-16
set debug mcppp-event 11-16
set debug mdp-events 11-16
set debug mdp-status 11-16
set debug off 11-16
set default 3-6, 12-16, 14-8, 17-5
set domain 3-8, 17-5
set endpoint 11-15
set Ether0 address 3-28, 4-3, 12-12, 12-16,
13-8, 13-10, 14-4, 14-8, 15-4, 15-8,
16-5, 17-6, 18-5, 19-4, 19-6
set Ether0 broadcast 4-4, 12-12, 12-16, 13-10,
14-4, 14-8, 15-5, 15-8, 16-5, 17-6,
18-5, 19-4, 19-6
set Ether0 ifilter 4-3
set Ether0 ip 4-5
set Ether0 ipx 4-6, 12-12, 12-16, 14-8
set Ether0 ipxframe 4-6, 12-12, 12-16, 14-4,
14-8, 15-4, 15-8, 19-4, 19-6
set Ether0 ipxnet 4-5, 12-12, 12-16, 14-4,
14-8, 15-4, 15-8, 19-4, 19-6
set Ether0 netmask 4-4, 12-12, 12-16, 13-8,
13-10, 14-4, 14-8, 15-4, 15-8, 16-5,
17-6, 18-5, 19-4, 19-6
set Ether0 ofilter 4-3
set Ether0 ospf 4-8
set Ether0 rip 3-28, 4-1, 12-12, 12-16, 13-10,
14-4, 14-8, 17-6, 19-4, 19-6
set filter 9-6
set filter icmp 9-6
set filter tcp 9-7
set filter udp 9-7
set gateway 3-6, 3-28, 12-11, 12-16, 13-8,
14-4, 14-8, 15-4, 16-4, 17-5, 19-4,
19-6
set host 17-5, 18-4
set ipxfilter 9-7
set ipxgateway 3-26
set isdn_switch 12-11, 12-16
set isdn-msn 12-8
set isdn-switch 11-5, 12-5
set Line0 e1 11-2
set Line0 encoding 11-6, 11-11
set Line0 fractional 11-2
set Line0 framing 11-6, 11-11
set Line0 group 11-3
set Line0 group channels 11-2
set Line0 inband 11-2, 11-11
set Line0 isdn 11-2
set Line0 loopback 11-7
set Line0 pcm 11-7
set Line0 signaling 11-3, 11-4, 11-11
set Line0 t1 11-2
set line2 clock 11-12
set line2 fractional 11-13
set location address 13-15
set location analog 11-9
set location chap 8-11
set location compression 8-9, 15-7, 15-11, 16-7
set location continuous 8-4, 16-8
set location destination 8-6, 12-14, 12-19,
14-6, 14-11, 15-7, 15-11, 16-7
set location group 8-8, 12-15, 12-19, 13-15,
14-7, 14-11, 15-7, 15-11, 16-7
set location high_water 8-13, 12-15, 12-19,
14-7, 15-7, 15-11, 15-14, 16-7
set location idle 12-15, 12-19, 14-7, 14-11,
15-7, 15-11, 16-7
set location idletime 8-10
set location ifilter 8-13, 16-7
set location ipxnet 8-6, 12-15, 12-19, 14-6,
14-11, 15-7, 15-11

set location manual 8-5, 12-14, 12-19, 14-6,
 14-11, 15-7, 16-7
 set location map 8-11
 set location maxports 8-12, 12-15, 12-19, 14-7,
 15-7, 15-11, 15-14, 16-8
 set location mtu 8-8, 12-15, 12-19, 14-6,
 14-11, 15-7, 15-11, 16-7
 set location multilink 12-7
 set location netmask 8-6, 12-14, 12-19, 13-15,
 14-6, 14-11, 15-7, 15-11, 16-7
 set location ofilter 8-13, 16-7
 set location on_demand 8-4, 12-20, 14-12,
 15-12
 set location password 8-5, 12-9, 12-15, 12-19,
 14-7, 14-11, 15-7, 15-11, 15-15,
 16-8, 16-11
 set location ppp 14-6, 14-11
 set location protocol 8-5, 12-14, 12-19, 13-15,
 15-7, 15-11, 16-7
 set location rip 8-7, 12-15, 12-19, 13-15, 14-6,
 14-11, 15-7, 15-11, 16-7
 set location subl 13-13
 set location telephone 8-5, 12-9, 12-15, 12-19,
 14-7, 14-11, 15-7, 15-11, 15-15,
 16-7, 16-11
 set location username 8-5, 12-9, 12-15, 12-19,
 14-7, 14-11, 15-7, 15-11, 15-15,
 16-7, 16-11
 set location voice 8-10, 12-8
 set loghost 3-10, 17-5
 set M0 11-8
 set M0 lastcall 11-9
 set maximum pmconsole 3-9
 set nameserver 3-8, 17-5
 set namesvc 3-8, 17-5
 set netbios 3-29
 set P0 device 18-8
 set P0 host 18-8
 set P0 service_device 18-8
 set pap 3-30, 5-19
 set password 3-2
 set pool 3-13
 set reported_ip 3-13
 set S0 access 9-15
 set S0 cd 5-25, 10-8, 15-5, 15-9, 16-5, 16-6,
 18-6, 18-7, 18-8, 19-5, 19-7
 set S0 compression 5-21, 5-24, 16-6
 set S0 databits 5-4
 set S0 destination 5-21, 16-6, 19-5, 19-7
 set S0 device 5-13, 18-7, 18-8
 set S0 directory 12-6
 set S0 dn 12-6
 set S0 dtr_idle 5-25
 set S0 extended 5-5
 set S0 group 5-5, 12-13, 12-17, 13-15, 15-5,
 15-9, 16-5
 set S0 hangup 10-9
 set S0 host 5-9, 18-6, 18-7
 set S0 idle 15-5, 15-9
 set S0 idletime 5-8
 set S0 ifilter 5-21
 set S0 ipxnet 5-21, 19-5, 19-7
 set S0 login 5-9
 set S0 map 5-21
 set S0 message 5-6
 set S0 modem 10-6
 set S0 MTU 5-21
 set S0 mtu 16-6, 19-5, 19-7
 set S0 netmask 16-6, 19-5, 19-7
 set S0 network 5-16, 5-21, 12-13, 12-17, 15-5,
 15-9, 16-5, 16-6, 19-5
 set S0 network hardwired 19-7
 set S0 network twoway 5-19
 set S0 ofilter 5-21

set S0 override 5-3
set S0 parity 10-8
set S0 prompt 5-5
set S0 protocol 5-21, 16-5, 16-6, 19-5, 19-7
set S0 rip 5-21, 5-23, 16-6, 19-5, 19-7
set S0 rts/cts 5-4, 5-19, 10-9, 15-5, 15-9, 16-5,
16-6, 18-6
set S0 security 5-6, 18-6
set S0 service_device 5-13, 5-25, 18-6, 18-7,
18-8
set S0 service_login 5-9, 18-6
set S0 speed 5-4, 10-7, 15-5, 15-9, 16-5, 16-6,
18-6, 18-7
set S0 spid 12-5, 12-13, 12-17
set S0 termtype 5-9
set S0 twoway 5-25, 18-5
set S0 username 5-7
set S0 xon/xoff 5-4, 10-9, 16-5, 16-6, 18-6,
18-7
set sapfilter 9-8
set secret 17-8
set serial-admin 3-12
set subinterface 4-7
set syslog 3-10
set syslog Facility.Priority 3-11
set sysname 3-2, 12-11, 12-16, 14-4, 14-8,
15-4, 17-5, 19-4, 19-6
set telnet 3-9, 5-25
set user address 12-14, 12-18, 14-10
set user compression 7-9, 12-14, 12-18, 15-6,
15-10, 17-10
set user destination 7-6, 14-5, 15-6, 15-10,
17-10
set user dialback 7-10, 7-13
set user host 7-11
set user idle 7-4
set user ifilter 7-9, 7-11
set user ipxnet 7-6, 12-14, 12-18, 14-6, 14-10,
15-6, 15-10
set user map 7-7
set user maxports 7-8, 12-8
set user mtu 7-8, 12-14, 12-18, 14-6, 14-10,
15-6, 15-10
set user netmask 7-6, 12-14, 12-18, 14-5,
14-10, 15-6, 15-10
set user ofilter 7-10
set user password 7-4, 12-13, 12-18, 14-5,
14-10, 15-6, 15-10, 17-9, 17-10
set user protocol 7-5, 12-13, 12-18, 14-5,
14-10, 15-6, 15-10, 17-10
set user rip 7-6, 12-14, 12-18, 14-6, 14-10,
15-6, 15-10, 17-10
set user service 7-13, 17-9
set user session-limit 7-4
set user-netmask A-8
set W1 address 6-8, 13-9, 13-10
set W1 annex-d 13-6, 13-9, 13-10
set W1 cd 6-6, 13-9, 13-10, 14-5, 14-9
set W1 destination 6-9
set W1 dlci 13-6, 13-9, 13-11
set W1 extended 6-4
set W1 group 6-7, 14-5, 14-9
set W1 hangup 6-7
set W1 idle 6-7
set W1 ifilter 6-11
set W1 ipxnet 6-9
set W1 lmi 13-6
set W1 netmask 6-9, 13-9, 13-10, 14-9
set W1 network 6-4, 13-9, 13-10, 14-5, 14-9
set W1 ofilter 6-11
set W1 protocol 6-8, 13-9, 13-10, 14-9
set W1 rip 6-10, 13-9, 13-10
set W1 speed 6-5
show arp 13-14

show filter 9-8
show ipxroutes 3-24
show Line0 11-2, 11-11
show location 13-13
show M0 11-9
show mcppp 11-15
show modem 10-3
show modems 11-10
show P0 2-5
show routes 3-23
show S0 2-5, 12-9
show syslog 3-12
show table filter 9-8
show table location 8-2
show table modem 10-2
show table user 7-2
show user 7-2
show W1 2-5

Subject Index

A

- access filters
 - creating 9-1
 - restricting user access to hosts 7-11
- address pools
 - creating 3-12
 - example 17-4
 - size 3-13
- addresses. See IP addresses, IPX addresses
- administrative logins, enabling and disabling 3-12
- analog modems, enabling on PortMaster 3 11-10
- Annex-D
 - defined 13-3
 - keepalives 13-6
 - use with DLCI 13-11
 - using to discover Frame Relay addresses 6-8
- asynchronous character map
 - defined 8-11
 - network user 7-7
- asynchronous ports
 - access filters 5-6
 - databits 5-4
 - destination IP address 5-22
 - destination netmask 5-22
 - device service 5-14
 - dial groups 5-5
 - DTR idle 5-25
 - extended information 5-5
 - flow control 10-8
 - input and output filters 5-25
 - IPX network number 5-22

- line hangup 10-9
- login host 5-11
- login message 5-6
- login prompt 5-5
- login service 5-10
- modem control 10-8
- MTU 5-22
- overriding settings 5-3
- parity checking 5-4, 10-8
- port type 5-9
- PPP asynchronous map 5-24
- protocol 5-22
- routing 5-23
- security 5-6
- speed 5-3, 10-7
- terminal type 5-11
- uses of 5-1
- using as console port 5-7

- authentication 1-2
 - process 2-4
 - See also RADIUS
- automatic login 5-6

B

- bandwidth on demand 8-11, 8-12
- Basic Rate Interface. See ISDN
- bidirectional communications 5-25
- boot process 2-1
- boundaries of routes 3-28
- BRI. See ISDN
- broadcast 4-4
- broadcast address, setting for Ethernet interface 4-4

broadcast packets, type 20 3-29
broadcast, high and low 4-4
burst speed 13-2

C

callback
 configuration tip 1-3
 login users 7-13
 manual dial-out 8-4
 network users 7-10
call-check, setting 3-30
carrier detect. See DCD
CHA authentication 3-29
Challenge Handshake Authentication Protocol. See CHAP authentication
channel rate 11-3
channelized T1 11-3, 11-4
 example configuration 11-12
 questions to ask the telephone company 11-11
CHAP authentication 5-19, 8-10, 16-8
ChoiceNet 1-2, A-10
CIDR A-2, A-6
Cisco routers, setting for Frame Relay 13-11
class A IP addresses A-3
class B IP addresses A-3
class C IP addresses A-4
class D IP addresses A-4
class E IP addresses A-4
cloud, Frame Relay 13-1
COMMAND port status 2-6
committed information rate, Frame Relay 13-2
community strings 3-21
ComOS, overview 1-1
compression 5-23, 6-11, 7-8, 8-8
configuration
 basic steps 1-4
 planning 1-2
CONNECTING port status 2-6
connection types 8-3

console port 5-7
contact information
 Europe, Middle East, and Africa xxiv
 mailing lists xxv
 North America, Latin America, and Asia Pacific xxiv
 technical support xxiii
continuous connections 8-3, 8-4
continuous Internet connections 16-3

D

daemons. See in.pmd
data carrier detect. See DCD
data link connection identifier. See DLCI
data over voice 8-10, 12-8
databits, setting 5-4
DCD, for port behavior 6-6, 10-8
debugging
 digital modems 11-17
 Frame Relay 13-12
 ISDN BRI 12-21
 leased line 19-8
 Multichassis PPP events 11-17
 synchronous v.25 bis connection 14-13
 See also troubleshooting
destination IP address, setting 5-22
destination netmask for asynchronous ports 5-22
device services 5-14
 netdata 5-15
 PortMaster 5-14
 Telnet 5-15
 using with in.pmd daemon 18-3
devices, shared 5-11
dial groups 5-5, 6-7, 8-8
dialback. See callback
dial-in access 5-2, 17-1
 configuration tip 1-3
dial-in users

- configuration tip 1-3
- defining 12-13, 14-5, 14-10
- ISDN connections 12-18
- maximum ports 7-8
- network users 17-10
- dial-in-only access 5-16
- dial-on-demand connections 8-4
- dial-out
 - configuration tip 1-3
 - connection types 8-3
- dial-out ports
 - configuration 16-5
 - configuration tip 1-3
 - multiline load balancing 8-12
- dial-out-only access 5-17
- dial-up connections, continuous 16-3
- digital modems 11-9
- directory number 11-8, 12-6
- disconnecting a dial-in user 5-7, 6-7
- DISCONNECTING port status 2-6
- DLCI
 - learning 13-5
 - use with PVCs 13-2
- DLCI bundling 13-12
- DLCI list 13-6
- DNS A-8, B-1
 - outside local subnet 9-12
 - setting 3-8
 - using instead of the host table 3-7
- documentation, related xvii
- Domain Name System. See DNS
- DSR value 5-26
- DTR idle 5-25
- DTR, for hangup 6-7, 10-9
- dynamically setting the IP address 3-12

E

E & M wink start protocol 11-3

- E1 channel groups 11-2
- E1 lines
 - encoding method 11-7
 - framing format 11-6
 - grouping fractional 11-2
 - pulse code modulation 11-8
 - setting use 11-2
- encoding method 11-7
- endpoint discriminator, setting for Multichassis PPP 11-16
- escaping PPP characters 5-24
- ESTABLISHED port status 2-6
- Ethernet
 - 802.2 4-6
 - 802.2_II 4-6
 - 802.3 4-6
 - filters 9-2
 - II 4-6
 - subinterfaces 4-7
- Ethernet interface
 - broadcast address 4-4
 - enabling IPX traffic 4-5
 - IP address 4-3
 - IP traffic 4-4
 - IPX frame type 4-6
 - IPX network number 4-5
 - NetBIOS 3-29
 - parameter descriptions 4-1
 - routing 4-1, 6-9, 7-6, 8-7
 - subnet mask 4-4
- extended information
 - asynchronous ports 5-5
 - synchronous ports 6-4

F

- filters
 - access filters 5-6, 9-15

- adding rules 9-5
- asynchronous ports 5-25
- attaching 9-4
- authentication queries 9-13
- ChoiceNet 1-2, A-10
- creating 9-5
- deleting 9-8
- displaying 9-8
- DNS outside local subnet 9-12
- empty rule set 9-3
- Ethernet interface 4-2, 9-2
- examples 9-9
- filter table 9-3
- filtering options 9-2
- for dial-out 8-13
- FTP 9-11
- hardwired port 9-10
- ICMP packets 4-3
- input 4-2, 6-11, 7-9, 8-13, 9-4, 16-10
- Internet 9-10
- IP 9-6
- IPX rules 9-7
- location filters 9-5
- logging results 9-14
- network access 9-13
- output 4-3, 6-11, 7-10, 8-13, 9-4
- packet filtering 9-2
- packet filters 7-9
- permit and deny 9-9
- removing 4-3, 6-11, 7-10
- RIP packets 9-12
- SAP filters 9-8
- security 9-1
- storing 9-3
- synchronous ports 6-10
- TCP and UDP port services B-1

- TCP options 9-6, 9-7
- UDP packets 4-3
- user filters 9-5
- flow control 5-4
 - hardware 10-2, 10-8
 - software 10-8
- foreign exchange station protocol 11-4
- fractional E1, enabling 11-2
- fractional T1
 - enabling 11-2
 - on the T1 expansion card 11-14
- Frame Relay
 - Annex-D 13-3, 13-6
 - burst speed 13-2
 - committed information rate 13-2
 - description 13-1
 - discarding frames 13-3
 - DLCI list 13-6
 - LMI 13-3, 13-5
 - ordering service 13-3
 - port speed 13-2
 - PVC 13-2
 - subinterfaces 13-12
 - troubleshooting 13-11
 - troubleshooting subinterfaces 13-14
- frame size, setting with MTU 8-8
- framing format 11-6
- FTP filters 9-11
- FXS loop start protocol 11-4

G

- gateways
 - route for IP 3-25
 - route for IPX 3-25
 - setting the default 3-5
- global parameters
 - default gateway 3-5

- default routing 3-6
- gateway for IP 3-25
- gateway for IPX 3-25
- host table 3-7
- IP address assignment 3-12
- name service 3-7
- password 3-2
- route destinations for IP 3-24
- route destinations for IPX 3-25
- static routes 3-24
- subnet mask table 3-26
- system logging 3-9
- system name 3-2
- Telnet 3-9
- ticks 3-26

H

- hanging up a line 6-7, 10-9
- hardware flow control 5-4, 10-2, 10-8
- hardwired connections 16-3
 - port configuration 16-6
 - tip for configuring 1-3
- high-speed dedicated connections 6-1
- high-water mark 8-11, 8-12
- hop count
 - for IP and IPX gateway routes 3-6
 - in IP static route 3-25
- host device configuration 5-12, 5-14
- host table 3-7, A-9
- HOSTNAME port status 2-6
- hostname resolution 3-8
- hosts, SNMP 3-22
- hotswapping, modems 11-10

I

- IDLE port status 2-6
- idle timer

- asynchronous ports 6-7
- dial-out locations 8-10
- disabling 7-4
- users 7-4
- in.pmd 1-1, 2-5, 5-13, 5-14, 5-18
- inband signaling
 - E & M wink start protocol 11-3
 - FXS loop start protocol 11-4
- initialization steps 2-3
- initialization strings 10-4
- INITIALIZING port status 2-6
- Internet
 - input filter example 9-10
 - restrictive filter example 9-13
- Internet connections 5-2, 16-1, 16-11
- IP address pools, static netmasks 3-27
- IP addresses
 - address pools 3-12, 17-4
 - class A A-3
 - class B A-3
 - class C A-4
 - class D A-4
 - class E A-4
 - classes A-2
 - conventions A-6
 - description A-1
 - destination 5-22, 7-5, 8-6
 - negotiating 5-22, 6-8
 - notation A-2
 - private IP networks A-5
 - reported 3-13
 - reserved addresses A-5
 - setting for Ethernet interface 4-3
 - subnetting A-7
 - synchronous ports 6-8
- IP traffic, setting on Ethernet interface 4-4
- IPX

- default gateway, setting 3-6
- displaying routing table entries 3-24
- enabling traffic 4-5
- encapsulation 4-6
- frame type 4-6
- network address 6-9
- packets, filtering 9-4, 9-7
- IPX addresses, conventions A-6
- IPX network number 7-5, 7-6, 8-6
 - asynchronous ports 5-22
 - Ethernet interface 4-5
- IPX route destinations 3-25
- ISDN
 - BRI ports 12-2
 - BRI, definition 12-1
 - data over voice 8-10, 12-8
 - dial-in users, defining 12-13, 12-18
 - directory number 11-8, 12-6
 - encoding method for PRI line 11-7
 - framing format for PRI line 11-6
 - multiline load balancing 12-7
 - Multilink PPP 12-7
 - multiple subscriber network 12-8
 - on-demand connections 15-15, 16-11
 - port limits 12-8
 - provisioning 12-3
 - pulse code modulation for PRI line 11-8
 - SPID 12-5
 - supported PRI switches 11-6
 - switch type 12-4
 - TID 12-6
 - troubleshooting 12-21
- ISP-provided dial-in access 17-1

K

- keepalive timer

- Annex-D 13-6
- LMI 13-5

L

- leased line connections 19-1
 - troubleshooting 19-8
- line hangup 10-9
- line speed, Frame Relay 13-2
- LMI
 - enabling 13-5
 - keepalives 13-5
 - types 13-3
 - use with DLCI 13-11
- Local Management Interface. See LMI
- location table
 - adding a location 8-3
 - CHAP 8-10
 - compression 8-8
 - connection types 8-3
 - destination IP address 8-6
 - dial group 8-8
 - dial groups 5-5, 6-7
 - displaying 8-2
 - filters 8-13
 - high-water mark 8-11
 - idle timer 8-10
 - IPX network number 8-6
 - maximum dial-out ports 8-12
 - MTU 8-8
 - multiline load balancing 8-11
 - netmask 8-6
 - password 8-5
 - protocol 8-5
 - routing 8-7
 - TCP/IP header compression 8-8
 - username 8-5

- locations
 - defining 8-1, 12-14, 14-6, 15-7, 16-7
- logging in to a remote host 5-2
- loghost, setting 3-10
- login host 5-11, 7-10
 - default 5-11
 - prompt 5-11
 - specifying 5-11
- login message 5-6
- login prompt 5-5
- login service 5-10
 - netdata 5-10
 - PortMaster 5-10
 - rlogin 5-10
 - Telnet 5-10
 - using with in.pmd daemon 18-3
- login users
 - description of 7-3
 - example 17-1
- loopback, enabling on T1 or E1 lines 11-8

M

- mailing lists, subscribing to xxv
- Management Information Base (MIB), description of 3-13
- manual connections 8-3, 8-4
- maximum transmission unit. See MTU
- mesh configuration 5-2
- metrics
 - hop count 3-25
 - ticks 3-26
- MIB 3-13
- modem switch 11-9
- modems
 - adding to modem table 10-3
 - automatic configuration 10-2
 - configuring for login 17-7
 - control 6-6, 10-8

- control signals 10-2
- digital 11-9
- digital to analog 11-10
- DSR value 5-26
- DTR idle 5-25
- hardware flow control 10-2, 10-8
- hot-swapping 11-10
- initialization strings 10-4
- line hangup 10-9
- null modem cable 10-1
- outbound traffic 10-8
- parity checking 10-8
- port speed 10-7
- RTS/CTS 10-2, 10-9
- setting speed 5-3
- synchronizing speed 10-7
- table 10-3
- monitoring,SNMP 3-21
- MSN 12-8
- MTU
 - asynchronous ports 5-22
 - dial-out locations 8-8
 - frame size 8-8
 - network users 7-7
 - packet size 8-8
- Multichassis PPP
 - displaying addresses 11-16
 - enabling on a PortMaster 3 11-16
- multiline load balancing 12-7
 - example 15-13
 - in the location table 8-11
 - port limits 12-8
 - user table 7-8
- Multilink PPP 7-8, 12-7, 12-8
- Multilink V.120 7-8, 12-8
- multiple subscriber network 12-8

N

- name resolution 3-6
- name service A-8
 - disabling 3-8
 - setting 3-7
- negotiating IP addresses 5-22, 6-8
- NetBIOS, setting 3-29
- netdata
 - device service 5-15
 - login service 5-10, 7-13
- netmask table
 - accessing 3-27
 - configuring 3-26
 - example of static netmask 3-27
 - IP address pools 3-27
- netmasks 8-6, A-7
- network device configuration 5-14, 18-2
- network security
 - description of A-9
 - RADIUS A-10
- network users
 - adding to user table 7-2
 - callback 7-10
 - description 7-3
 - protocol 7-5
- NIS A-8
 - setting 3-8
 - using instead of the host table 3-7
- NO-SERVICE port status 2-6
- NT1 device 12-1
- null modem cable 10-1

O

- office-to-office connections 5-1, 15-1
- on-demand connections 2-4, 8-3, 15-1
- overriding asynchronous port settings 5-3

P

- packet filtering 9-2
- packet size, setting with MTU 8-8
- PAP authentication 3-29, 5-19
- parity checking 5-4, 10-8
- Password Authentication Protocol. *See* PAP authentication
- PASSWORD port status 2-6
- passwords
 - deleting 3-2
 - for authentication. *See* CHAP authentication, PAP authentication
 - netuser 7-4
 - setting 3-2
 - setting for dial-out 8-5
 - user 7-2, 7-4
- permanent virtual circuits. *See* PVC
- planning your configuration 1-2
- PMconsole 1-1
- pmconsole, setting concurrent connections 3-9
- PMVision
 - overview 1-1
 - setting concurrent connections 3-9
- Point-to-Point Protocol. *See* PPP
- polling interval
 - Annex-D 13-6
 - LMI 13-5
- pool, IP address 3-12
- port idle timer 6-7
- port type 5-9
- PortMaster
 - daemon 1-1
 - device service 5-14
 - login service 5-10, 7-12
 - mailing lists xxv
 - software 1-1
- PortMaster 3
 - channel groups 11-2
 - channel rate 11-3

- displaying line status 11-1
- enabling analog modem service 11-10
- enabling modems 11-9
- enabling Multichassis PPP support 11-16
- encoding method 11-7
- framing format 11-6
- inband signaling 11-3, 11-4
- network loopback 11-8
- pulse code modulation 11-8
- switch type 11-6
- ports
 - dial groups 5-5, 6-7
 - for modem use 10-7
 - ISDN BRI 12-2
 - number used for dial-in access 17-1
 - port limits 12-8
 - printer port 18-7
 - security 5-6
 - speed 13-2
 - synchronizing speed 10-7
 - synchronous port speed 6-5
 - two-way access 18-5
 - well-known B-1
- PPP
 - address negotiation 8-6
 - asynchronous character map 5-24
 - connections 5-19
 - using for dial-in and dial-out 5-19
- printer port configuration 18-7
- prompt for login host 5-11
- protocol
 - asynchronous ports 5-22
 - location table 8-5
 - transport protocol 6-8
 - user 7-5
- provisioning, ISDN 12-3
- pseudo-tty connection 5-12, 18-2

- pulse code modulation 11-8
- PVC
 - burst speed 13-2
 - CIR 13-2
 - guaranteed maximum bandwidth 13-2
 - using with DLCIs 13-2

R

RADIUS

- example 17-8
- overview 1-2
- security 2-4
- when to use 7-1
- RADIUS protocol, description of A-10
- radiusd daemon 1-2
- RARP, finding IP address 2-1
- read and write hosts 3-22
- rebooting, for ISDN switch type 12-5
- references
 - books xxi
 - RFCs xix
- related documentation xvii
- resetting a virtual port 11-16
- RFC
 - 1058 3-26
 - 1144 5-23, 7-8, 8-9
 - 1166 A-1, A-2
 - 1213 3-14
 - 1331 5-19
 - 1332 5-19
 - 1490 13-4
 - 1597 A-5
 - 1700 9-7
 - 1717 5-19, 12-7
 - 1826 9-6
 - 1827 9-6
 - 1877 3-8

- 2003 9-6
- 2139 A-10
- 988 A-4
- RIP
 - asynchronous ports 5-23
 - network users 7-6
 - on Ethernet 4-1
 - routing, setting 8-7
 - synchronous ports 6-9
- rlogin login service 5-10, 7-12
- route boundaries 3-28
- routing
 - asynchronous ports 5-23
 - configuring the Ethernet interface 4-1, 6-9, 7-6, 8-7
 - dial-out locations 8-7
 - Frame Relay 6-1
 - ISDN 6-2
 - leased lines 6-1
 - route destinations for IP 3-24
 - route destinations for IPX 3-25
 - setting the default 3-6
 - switched 56Kbps 6-2
- routing table, displaying 3-23
- RTS/CTS 10-2, 10-9
- S**
- SAP filters 9-8
- security
 - access filters 5-6
 - management 2-4
 - network A-9
 - ports 5-6
 - using filters 9-1
- Service Advertising Protocol 9-8
- service profile identifier 12-5
- services, well-known B-1
- session limit 7-4
- setting call-check 3-30
- shared device access 5-2, 18-1
- shared devices 5-11
 - host device 18-1
 - Telnet 18-8
- Simple Network Management Protocol. See SNMP 3-13
- SLIP connections 5-19
- SNMP
 - agents 3-14
 - community strings 3-21
 - configuring 3-13
 - read and write hosts 3-22
 - viewing settings 3-23
- SNMP, monitoring 3-21
- software
 - flow control 5-4, 10-8
 - PortMaster 1-1
- SPID 12-5
- Stac LZS data compression 5-23, 7-8, 8-8
- star configuration 5-1
- static netmasks
 - example 3-27
 - using with IP address pools 3-27
- static routing, setting 3-24
- subinterfaces
 - Ethernet 4-7
 - frame relay 13-12
- subnet masks A-7
 - Ethernet interface 4-4
 - setting on Ethernet interface 4-4
 - synchronous port 6-9
- subnetting
 - connecting two networks 19-2
 - routing issues A-8
 - subnet mask A-7
- support, technical xxiii
- switch types

- BRI 12-4
- PRI 11-6
- switched 56Kbps connections 14-1
- synchronous leased lines 19-1
- synchronous ports
 - connection type 6-4
 - description 6-1
 - destination IP address 6-8
 - DLCI list 13-6
 - extended information 6-4
 - filters 6-10
 - modem control 6-6
 - port type 6-4
 - speed 6-5
 - subnet mask 6-9
- TCP header compression 6-11
- transport protocol 6-8
- See also WAN ports
- system logging
 - disabling 3-10
 - messages 3-10
 - setting 3-9
- system name, setting 3-2

T

- T1 channel groups 11-2
- T1 expansion card 11-3
 - clocking 11-13
 - for fractional T1 11-14
 - for full T1 11-14
 - troubleshooting 11-15
- T1 lines
 - encoding method 11-7
 - external clocking 11-2
 - framing format 11-6
 - grouping fractional 11-2
 - internal clocking 11-13

- pulse code modulation 11-8
- setting use 11-2
- TA 12-2
- TCP
 - default Telnet port 5-15
 - packets, filtering 9-7
 - services and ports B-1
- TCP/IP header compression 5-23, 6-11, 7-8, 8-8
- TCP/IP support, connecting without 5-25
- TCP-CLEAR channel access 5-15
- technical support, contacting xxiii
- telephone number, setting for dial-out 8-5
- Telnet
 - access to shared devices 18-8
 - device services 5-15
 - login service 5-10, 7-12
 - using as console port 3-9
 - using for administrative tasks 3-9
- terminal adapter 12-2
- terminal identifier 12-6
- terminal type, asynchronous ports 5-11
- terminal, connecting to console port 10-1
- The xxiii
- ticks, setting 3-26
- TID 12-6
- transport protocol, setting 6-8
- troubleshooting
 - Frame Relay 13-11
 - Frame Relay subinterfaces 13-14
 - ISDN 12-21
 - leased line connections 19-8
 - V.25bis 14-13
- two-way access
 - port configuration 18-5
- type 20 broadcast packets 3-29

U

- UDP

- packets, filtering 9-7
- services and ports B-1
- user login configuration 5-8
- user table
 - access filters 7-11
 - adding users 7-2
 - compression 7-8
 - displaying 7-2
 - IP address 7-5
 - IPX network number 7-6
 - login host 7-10
 - login service 7-12
 - maximum ports 7-8
 - MTU 7-7
 - packet filters 7-9
 - session limit 7-4
 - setting the protocol 7-5
 - TCP/IP header compression 7-8
 - user types 7-3
- USERNAME port status 2-6
- username, setting for dial-out 8-5
- users
 - defining dial-in network users 17-10
 - defining dial-in users 14-5, 14-10, 15-6
 - defining login users 17-9
 - deleting 7-3
 - disconnecting from virtual port 11-16
 - displaying configuration information 7-2
 - restricting access to hosts 7-11
 - session limit 7-4
- utilities for allowing concurrent connections 3-9

V

- V.25bis
 - connections 14-1
 - troubleshooting 14-13

- virtual ports
 - disconnecting users 11-16
 - resetting 11-16
- virtual switch 13-1
- VLSM A-8

W

- WAN ports
 - example configuration 19-5, 19-7
 - ISDN 12-12, 12-17
 - setting up Frame Relay 13-10
 - switched 56Kbps 14-5
 - V.25bis dialing 14-5
 - See also synchronous ports
- well-known ports B-1
- well-known services B-1