PortMaster®

Configuration Guide

Lucent Technologies
4464 Willow Road
Pleasanton, CA 94588
925-737-2100
800-458-9966

May 2000

950-1182H

Copyright and Trademarks

PortMaster, ComOS, and ChoiceNet are registered trademarks of Lucent Technologies Inc. PMVision, NavisAccess, PMconsole, IRX, and NetworkCare are trademarks 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.

This manual is dedicated to everyone who is now or ever was on the PortMaster team.

Contents

5. Configuring an Asynchronous Port

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.

For information about configuring the PortMaster 4, see the *PortMaster 4 User Manual*.

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)**—use this guide to help you understand how to configure a PortMaster and its features. Consult the *PMVision User's Guide* and PMVision online help for instructions for using PMVision.

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. 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.

- *PMVision User's Guide*

  This guide provides instructions for installing, configuring, and using the PMVision network management application, a graphical configuration and monitoring tool for PortMaster products and other devices running ComOS® software.

- *PortMaster 4 User Manual*

  This collection of the following three standalone manuals provides instructions and commands for installing, configuring, and troubleshooting PortMaster 4 products:

  – *PortMaster 4 Installation Guide*

  – *PortMaster 4 Configuration Guide*

  – *PortMaster 4 Command Line Reference*

  It also includes a comprehensive table of contents, glossary, and master indexes.

- *PortMaster Command Line Reference*

  This reference 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 for PortMaster products.

- PortMaster hardware installation guides

These guides contain complete hardware installation instructions. An installation guide is shipped with each 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 for UNIX Administrator's Guide*

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

Additional References

Consult the following Requests for Comments (RFCs) and books for more information about the topics covered in this manual.

RFCs

To find a Request for Comments (RFC) online, visit the website of the Internet Engineering Task Force (IETF) at **http://www.ietf.org/**.

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 1212, *Concise MIB Definitions*
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 1483, *Multiprotocol Encapsulation over ATM Adaption Layer 5*
RFC 1490, *Multiprotocol Interconnect Over Frame Relay*
RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
RFC 1552, *The PPP Internet Packet Exchange Control Protocol (IPXCP)*
RFC 1587, *The OSPF NSSA Option*
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 1723, *RIP Version 2*
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 1851, *The ESP Triple DES 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 1962, *The PPP Compression Control Protocol (CCP)*
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 2131, *Dynamic Host Configuration Protocol*
RFC 2132, *DHCP Options and BOOTP Vendor Extensions*
RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*
RFC 2139, *RADIUS Accounting*
RFC 2153, *PPP Vendor Extensions*
RFC 2328, *OSPF Version 2*
RFC 2364, *PPP over AAL5*
RFC 2400, *Internet Official Protocol Standards*
RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*
RFC 2405, *The ESP DES-CBC Cipher Algorithm with Explicit IV*
RFC 2451, *The ESP CBC-Mode Cipher Algorithm*
RFC 2453, *RIP Version 2*
RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*

Books

ATM and Multiprotocol Networking (Computer Communications). George C. Sackett and Christopher Metz. Boston and New York: McGraw-Hill. 1997. (ISBN 0070577242)

ATM User's Guide. William A Flanagan. New York: Flatiron Publishing. 1994. (ISBN 0-936648-40-6)

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, 3rd edition. Paul Albitz, Cricket Liu. Sebastopol, CA: O'Reilly & Associates, 1998 (ISBN: 1-56592-512-2)

Getting Connected: The Internet at 56K and Up (Nutshell Handbook). Kevin Dowd. Sebastopol, CA: O'Reilly & Associates Inc. 1996 (ISBN 1565921542)

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: ISBN 4-89052-672-2). Errata are available at **ftp://ftp.research.att.com/dist/internet_security/firewall.book**.

Frames, Packets, and Cells in Broadband Networking. William A Flanagan. New York: Telecom Library Inc. 1991. (ISBN 0-036648-31-7)

Internet Routing Architectures. Bassam Halabi. San Jose, CA: Cisco Press, 1997. (ISBN 1-56205-652-2)

Internetworking Technologies Handbook, 2nd edition (The Cisco Press Fundamental Series). Merilee Ford, H. Kim Lew, Steve Spanier, Tim Stevenson, and Kevin Downs. New York: MacMillan Publishing Company. 1998 (ISBN 1578701023)

Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture. Douglas Comer. Upper Saddle River, NJ: Prentice Hall, Inc. 1995. (ISBN 0-13-216987-8 (v.1))

Internetworking with TCP/IP: Design, Implementation, and Internals, Vol 2, 3rd edition. Douglas E. Comer and David L. Stevens. Upper Saddle River, NJ: Prentice Hall. 1998. (ISBN 0139738436)

IPv6: The New Internet Protocol, 2nd edition. Christian Huitema. Upper Saddle River, NJ: Prentice Hall, Inc. 1997. (ISBN 0138505055)

OSPF: Anatomy of an Internet Routing Protocol. John T. Moy. Reading, MA: Addison-Wesley Publishing Company. 1998 (ISBN 0-201-63472-4)

Practical Internet & UNIX Security. Simson Garfinkel and Gene Spafford. Sebastopol, CA: O'Reilly & Associates. 1996. (ISBN 1-56592-148-8)

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

TCP/IP: Architecture, Protocols, and Implementation With Ipv6 and IP Security. Sidnie Feit. Boston and New York: McGraw-Hill. 1998. (ISBN: 0070220697)

TCP/IP Illustrated: The Protocols, Vol 1. (Professional Computing Series). W. Richard Stevens. Reading, MA: Addison-Wesley Publishing Company. 1994. (ISBN 020163346-9)

TCP/IP Network Administration, 2nd edition. Craig Hunt. Sebastopol, CA: O'Reilly & Associates. 1998. (ISBN 1565923227)

Troubleshooting TCP/IP; Analyzing the Protocols of the Internet, 2 edition. Mark Miller. Foster City, CA: IDG Books Worldwide. 1996 (ISBN 1558514503)

UNIX System Security: A Guide for Users and System Administrators. David Curry. Addison Wesley. 1992. (ISBN 0-201-56327-4)

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.	• Enter **version** to display the version number. • Press **Enter**. • Open the **permit_list** file.
Italic font	Identifies a command-line placeholder. Replace with a real name or value.	• **set** *Ether0* **address** *Ipaddress* • Replace *Area* with the name of the OSPF area.
Square brackets ([ ])	Enclose optional keywords and values in command syntax.	• **set nameserver** [**2**] *Ipaddress* • **set** *S0* **destination** *Ipaddress* [*Ipmask*]
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	**set syslog** *Logtype* {[**disabled**] [*Facility.Priority*]}
Vertical bar (|)	Separates two or more possible options in command syntax.	• **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 NetworkCare 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 staff of Lucent NetworkCare™ Professional Services or your authorized sales channel partner.

New releases and upgrades of PortMaster software are available at **http://www.livingston.com/forms/one-click-dnload.cgi** or by anonymous FTP from **ftp://ftp.livingston.com/pub/le/**.

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 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 sales channel partner in this region, contact the Lucent NetworkCare EMEA Support Center Monday through Friday, 24 hours a day.

- By voice, dial +33-4-92-38-33-33.
- By fax, dial +33-4-92-38-31-88.
- By electronic mail (email), send mail to **emeacallcenter@lucent.com**.

For North America, CALA, and the Asia Pacific Region

Contact Lucent NetworkCare Monday through Friday between the hours of 7 a.m. and 5 p.m. (GMT –8).

- By voice, dial 800-458-9966 within the United States (including Alaska and Hawaii), Canada, and the Caribbean and Latin America (CALA), or +1-925-737-2100 from elsewhere.
- By email, send mail as follows:
  - From North America and CALA 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 NetworkCare Professional Services offers hands-on, technical training courses on PortMaster products and their applications. For course information, schedules, and pricing, visit the Lucent NetworkCare website at **http://www.lucent-networkcare.com/consulting/education**.

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-modems**—a discussion of problems and solutions for PortMaster 3 internal digital modems and also the external modems that work with PortMaster products. To subscribe, send email to **majordomo@livingston.com** with **subscribe portmaster-modems** 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.
- **tech-bulletin@livingston.com**—a moderated *push* list featuring technical notes, Web links, and information about the latest code and beta releases sent on a weekly basis, as well as periodic technical updates. To subscribe, complete the form at **http://www.livingston.com/tech/bulletin/index.html**.

Introduction 1

This chapter discusses the following topics:

PortMaster Software

All PortMaster products are shipped with the following software:

- **ComOS**—The communication software operating system already loaded in nonvolatile (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.
- **Other Network Management Applications**—Table 1-1 describes additional Java-based software tools and wizards that help you configure and troubleshoot a PortMaster. See **http://www.livingston.com/forms/one-click-dnload.cgi** to download these applications, which include online help.

Table 1-1 Network Management Applications

Application	Function
PMWizard	Simplifies PortMaster 3 configuration.
PMTools	Supplement certain PMVision management functions with the following utilities: **pmbackup**, **pmcommand**, **pmdial**, **pmdumpfilter**, **pmreset**, and **pmupgrade**.
ORWizard	Simplifies PortMaster ISDN Office Router configuration.
FilterEditor	Helps you create, edit, and copy filters across different PortMaster products, ChoiceNet files, and ASCII files.
PPPSmartAgent	Monitors Point-to-Point Protocol (PPP) negotiations across multiple PortMaster products, diagnoses failures, and proposes solutions.
PPPDecoder	Translates the PPP hexadecimal debug output from a PortMaster into human-readable form, based on RFC 1332, RFC 1552, RFC 1661, RFC 1700, and RFC 2153.
LocationWizard	Creates location entries for PortMaster products.
NetbootServer	Interface to TFTP and BOOTP servers that can boot a PortMaster across a network or download a new ComOS version.

- **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 on the *PortMaster Software CD* package.

- **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 for UNIX 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 the Point-to-Point Protocol (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 the Serial Line Internet Protocol (SLIP), PPP, or both?

- If you use PPP, do you want the authenticate users with the Password Authentication Protocol (PAP) or the Challenge Handshake Authentication Protocol (CHAP)?
- Do you want to use the Layer 2 Tunneling Protocol (L2TP) to provide security on the public networks linking your offices?
- Are you using a name service—Domain Name System (DNS) or Network Information Service (NIS)?
- Have you obtained a sufficient number of network addresses, or do you want to use the network address translator (NAT) software?
- Are you running IP, IPX, or both?
- Do you want to enable Simple Network Management Protocol (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 Basic Rate Interface (BRI), ISDN Primary Rate Interface (PRI), channelized T1, or E1?
- On T1 or E1 lines using ISDN PRI, do you want to implement non-facility associated signaling (NFAS) to maximize bandwidth?

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 User's Guide* 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 5, "Configuring an Asynchronous 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, T1, or E1 connection(s), if available.**

   ISDN PRI, T1, and E1 connection configuration is described in Chapter 11, "Configuring the PortMaster 3." ISDN BRI connection configuration is covered in Chapter 10, "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 for UNIX Administrator's Guide* or the *RADIUS for Windows NT 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 the Lucent ComOS network address translator (NAT) software to provide access to the Internet for hosts without public IP addresses.**

    See Chapter 13, "Configuring NAT," for instructions.

13. **Configure the Layer 2 Tunneling Protocol (L2TP) if you are setting up an L2TP tunnel to an L2TP-compatible router.**

    See Chapter 14, "Configuring L2TP," for instructions.

14. **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 12, "Configuring Filters."

15. **Configure OSPF, if you are using this protocol.**

    OSPF is described in the *PortMaster Routing Guide*.

16. **Configure BGP, if you are using this protocol.**

    BGP is described in the *PortMaster Routing Guide*.

17. **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.

How the PortMaster Works 2

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:

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 nonvolatile RAM, 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 nonvolatile RAM, 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, any model
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 nonvolatile 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. The **syslog** utility 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** *S0* **security** 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 for UNIX Administrator's Guide* for more information about RADIUS.

See Chapter 14, "Configuring L2TP," for additional security features.

Port Status and Configuration

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

```
Command> show S0|S10|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	The data carrier detect (DCD) signal has been asserted and observed on the port. • 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 or PMVision GUI is being used on the port.
NO-SERVICE	An ISDN port is not receiving service from the telephone company.

Configuring Global Settings 3

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

This chapter discusses the following topics:

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 15 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 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 3-4.

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 3-5 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 3-4. 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 3-5.

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 must 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 for UNIX 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.
nat	Packets that match NAT filter rules with the **log** keyword.

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
warning	4	Warning messages

Table 3-4 **syslog** Priority Keywords *(Continued)*

Priority	Number	Typically Used for
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 – You must reboot the PortMaster after you set or change the number of addresses in the pool 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 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 ships configuration files compatible with various network management packages along with the PMVision 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/marketing/products/pmtempl.html**. To view the file, scroll down to MIB Specifications and click **LE38** in the table.

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 3-1 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 3-1, the OID for the Livingston MIB is 1.3.6.1.4.1.307.

Figure 3-1 Management Information Base (MIB) Hierarchy

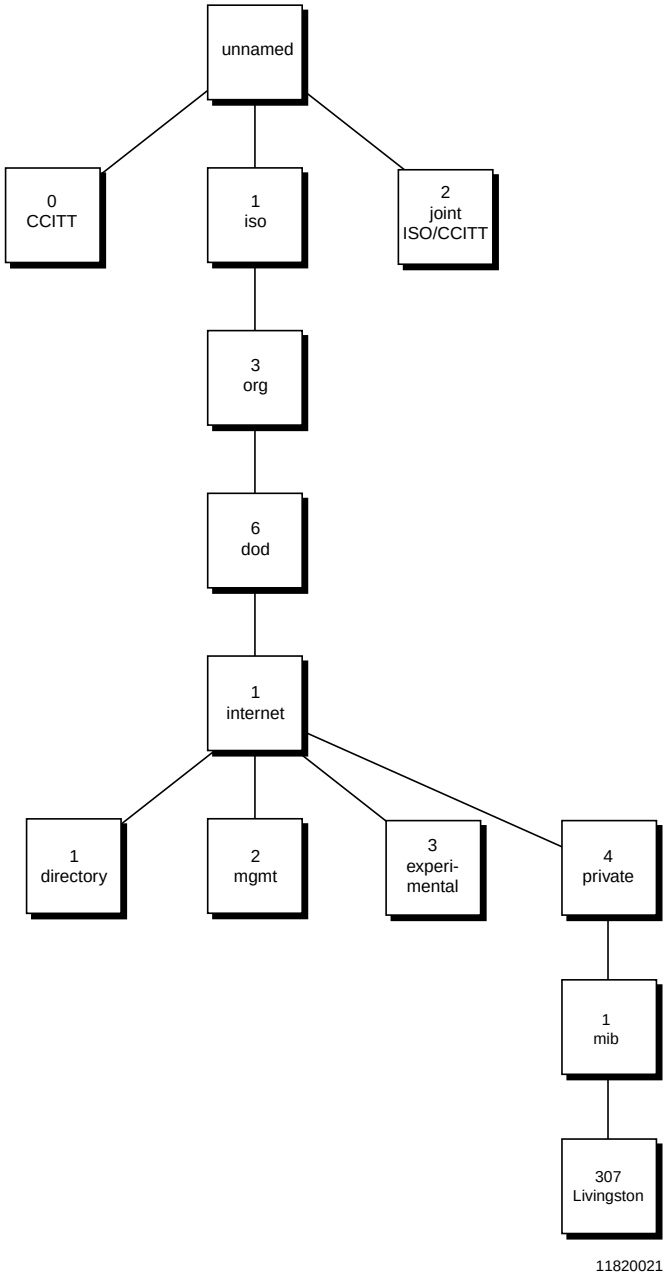
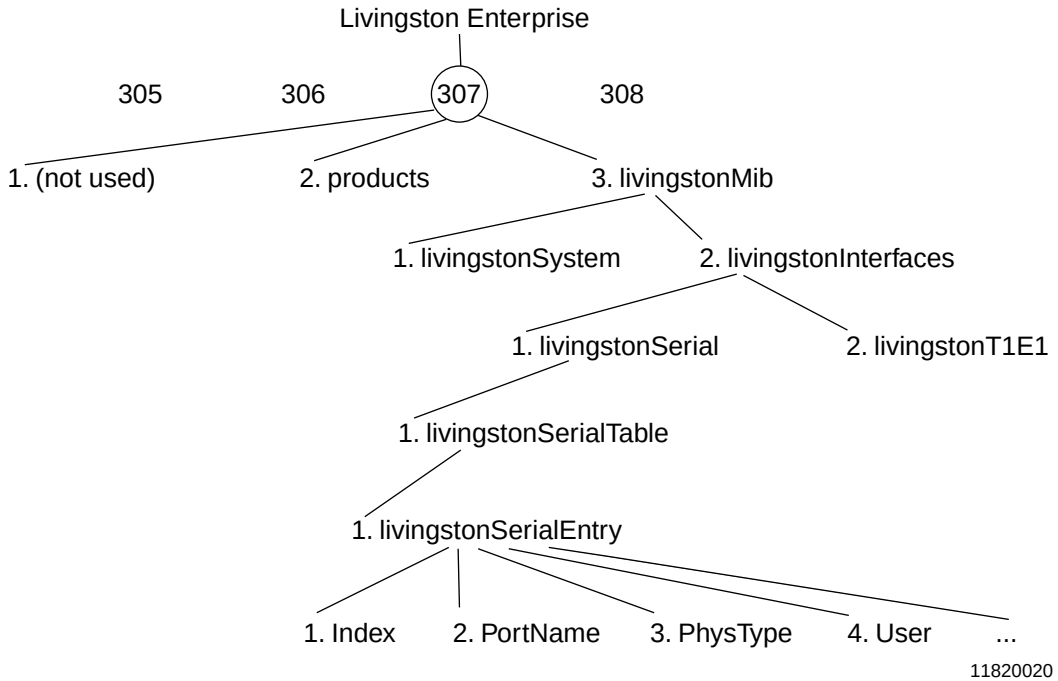


Figure 3-2 shows the tree structure of the private Livingston portion of the MIB.

Figure 3-2 Part of MIB Structure showing PortMaster Port S0.



Reading from the top down, the object identifier (OID) in Figure 3-2 (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 port name 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 Interfaces 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.
Direction	Direction in which the active session was initiated.

Table 3-6 Serial Interfaces Table *(Continued)*

Object	Definition
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 (Port Master 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: up (1) down (2) loopback (3)
Framing	Configured line framing. Line framing types include the following: 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
CarrierLoss	Total number of times the interface has lost the carrier signal

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

Object	Definition
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.

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
livingstonModemInByteCount	Total number of bytes received by the modem
livingstonModemOutByteCount	Total number of bytes transmitted by the modem

Table 3-8 Modem Table *(Continued)*

Object Type	Definition
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 alarms
```

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 alarms [Alarm-id]
```

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

```
Command> clear alarms 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 3-23 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 ipxroute Ipxnetwork Ipxaddress Metric Ticks
Command> save all
```

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

```
Command> delete ipxroute 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 workaround works only if all the products involved are 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 third-party routers can use them. Keep in mind that not all routers accept host routes.
- If the third-party 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 in "Example of Applying Static Netmasks" on page 3-24.

The next most common use for the static netmask table is to allow dial-in users to use specified IP addresses across multiple PortMaster products 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 the 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 a PortMaster IRX™ Router 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, see "Overview of Call-Check" on page 14-7 and refer to the *RADIUS for UNIX Administrator's Guide*.

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 10, "Using ISDN BRI," for details on BRI connections.

Configuring the Ethernet Interface 4

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

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 earlier than ComOS 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 12, "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 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.

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 enabled|disabled
```

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 can 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 enabled|disabled
```

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 c0000000000000an then view with the **show subinterface** command. Remove a subinterface from the subinterface table with the **delete subinterface** command.

2. **Associate the subinterface with a physical port.**

   Command> **set subinterface** *Name* **port** *Portlabel*

3. **Assign an IP address or an IP address and netmask to the subinterface.**

   Command> **set subinterface** *Name* **address** *Ipaddress* [*/NM*]|[*Netmask*]

   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.

Configuring an Asynchronous Port 5

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:

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 17, "Using Office-to-Office Connections," gives an example of a dial-up asynchronous office-to-office connection. Chapter 10, "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.

When connecting to the Internet, include packet filtering and security to ensure that access to the local network is restricted.

Chapter 18, "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 19, "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 access to central hosts from home, field offices, or on the road.

Chapter 19, "Providing User Dial-In Access," gives an example of an asynchronous dia-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 for access to programs via TCP/IP sockets, or by Telnet from the network.

Chapter 20, "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 must 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 affects only 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 message 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 12, "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 waits 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:

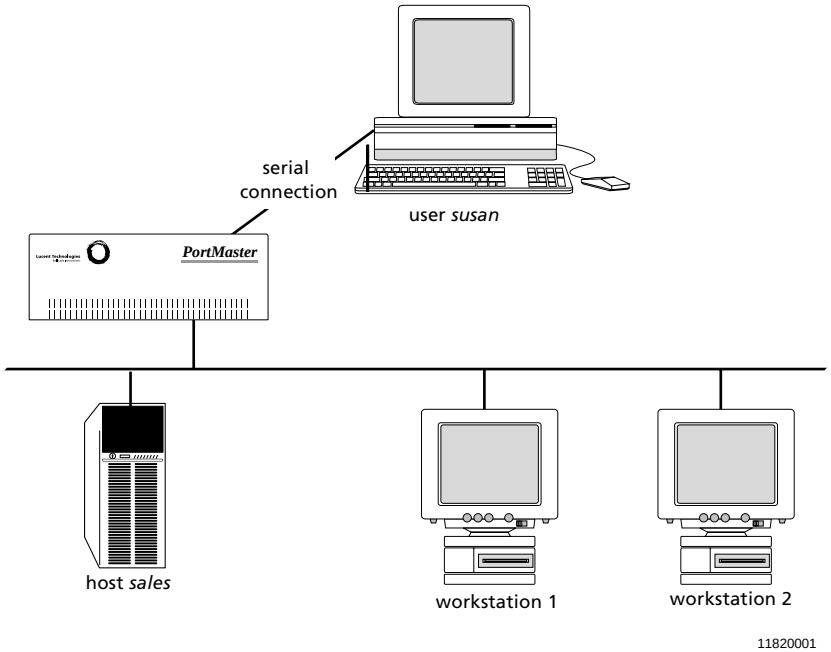
```
Command> set S0 |all idletime Number [minutes|seconds]
```

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.
Ipaddress	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 two-way 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 must 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 termtype** 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 you are 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

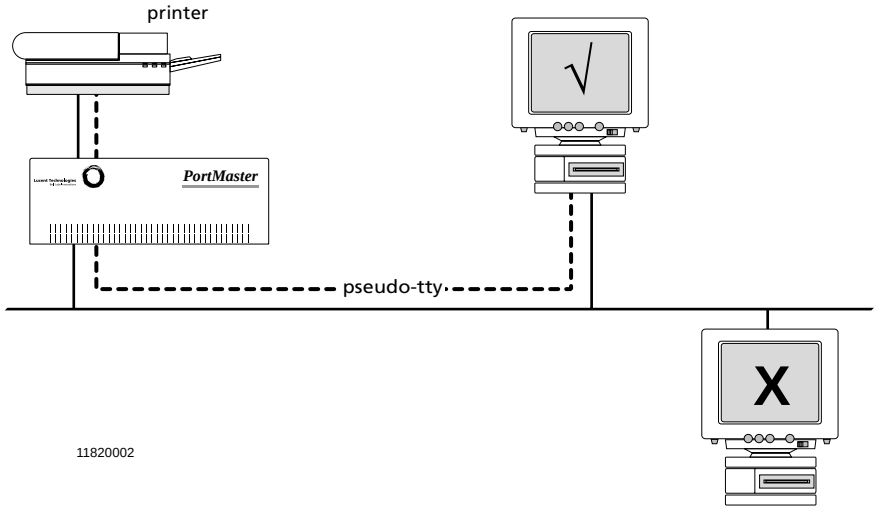
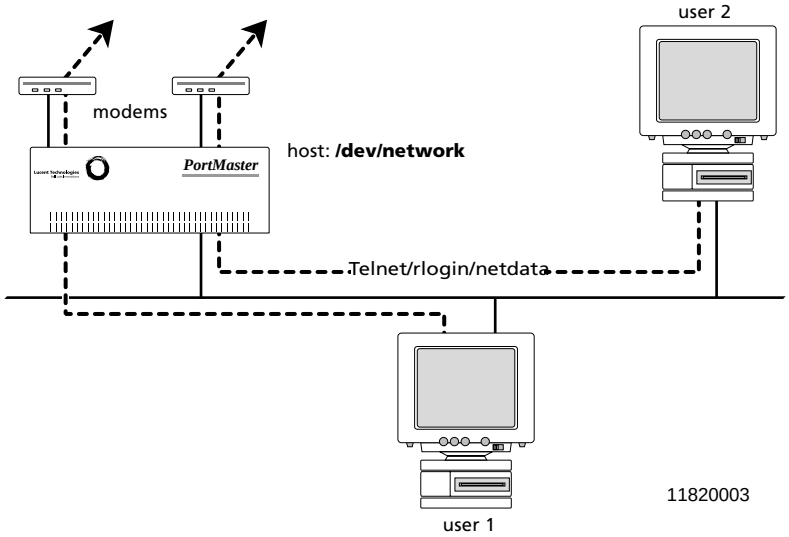


Figure 5-3 shows a host device configuration where the device service is set as **rlogin**, **telnet**, or **netdata**. In this configuration, the host device name is set as **/dev/network**. This configuration is used in cases where users want to log in remotely via **telnet** or **rlogin** to the shared 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. 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 that 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 S0 network dialin|dialout|twoway
   ```

2. **Save the configuration.**

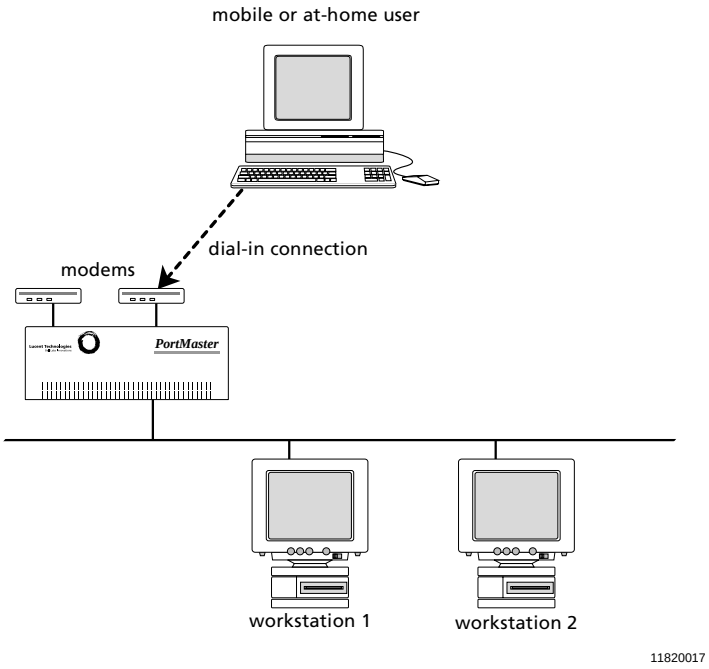
   ```
   Command> save all
   ```

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.

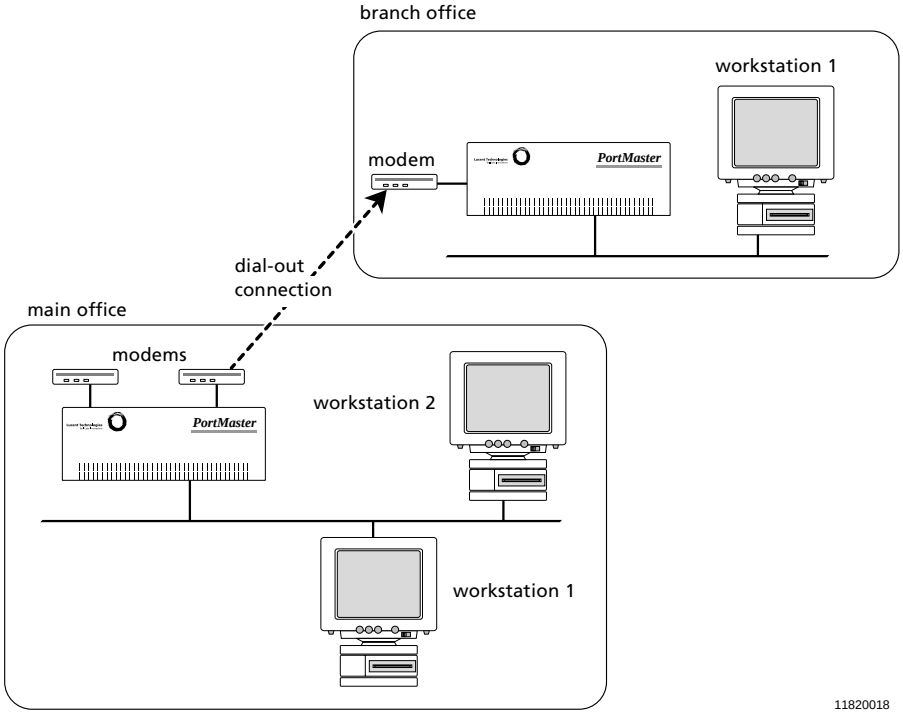
Figure 5-4 Dial-In-Only Port Access



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



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 on** 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
```

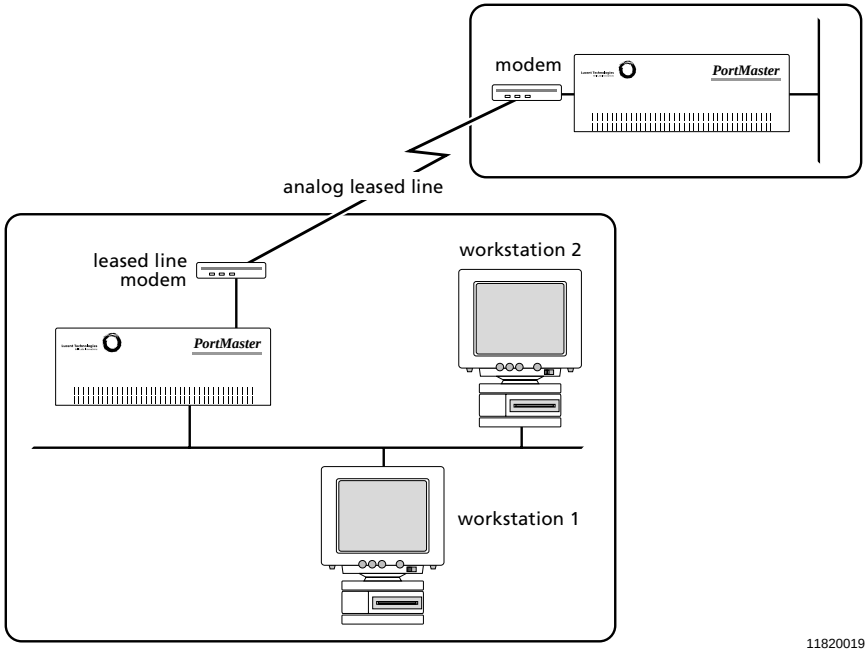
Configuring a Port for a Dedicated Connection

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



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 Ipaddress [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 *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

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 multiline load balancing.

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 – Releases earlier than ComOS 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 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. 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 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 data stream. 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 bit map of characters that are 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 12, "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.

Configuring a Synchronous WAN Port 6

This chapter describes the steps required to configure a PortMaster synchronous wide area network (WAN) port.

This chapter discusses the following topics:

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.

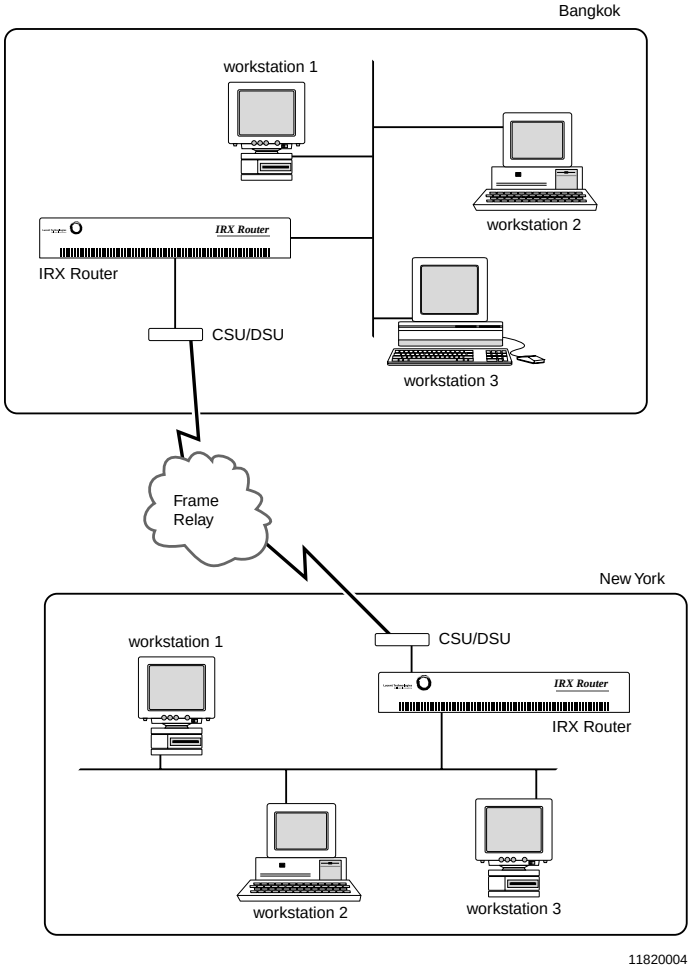
Routing over Leased Lines. A synchronous port can be used to connect to synchronous leased lines from 9600bps to T1 (1.544Mbps) or E1 (2.048Mbps) for continuous operation. A channel service unit/digital service unit (CSU/DSU) must be attached to the WAN port on the PortMaster. For more information, see Chapter 21, "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 twelve. For more information, see Chapter 15, "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 16, "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 appropriate for the amount and nature of the traffic. For more information about ISDN Basic Rate Interface (BRI) connections, see Chapter 10, "Using ISDN BRI." For information about ISDN Primary Rate Interface (PRI) connections, see Chapter 11, "Configuring the PortMaster 3."

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	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. 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.
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 deasserted 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 idletime 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 15, "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 15, "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 only network hardwired connections 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 – Releases earlier than ComOS 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 12, "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 W1 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.

Configuring Dial-In Users 7

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 for UNIX Administrator's Guide* for more information.

This chapter discusses the following topics:

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.

Note – 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.
Ipaddress	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 **0xffffffe** 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 – Releases earlier than ComOS 3.5 use 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 are replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. In most environments, the asynchronous map is 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 must 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 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 64.

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 does 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 12, "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 are 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|callback Locname|none
```

The **dialback** and **callback** keywords are synonyms. To disable callback connections for the user, use the **none** keyword.

For more information about configuring locations, refer to Chapter 8, "Configuring Dial-Out Connections."

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.

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 19-5.
prompt	This option allows the user to log in to a host by IP address or hostname at the time the login session is established.
Ipaddress	This option allows the user to connect only to the host specifically named. A valid hostname or IP address must be entered. 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 *carmela* to always be connected with the host *sales*.

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

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

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 12, "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	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 RS232 cable. However, some serial communications protocols, such as FAX, might have potential latency problems.

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|callback String|none
```

The **dialback** and **callback** keywords are synonyms. To disable callback connections for the user, use the **none** keyword.

Configuring Dial-Out Connections 8

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

This chapter discusses the following topics:

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 20, "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. PortMaster products have empty location 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.
automatic	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|automatic|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
```

Automatic

To establish an automatic dial-out connection, you must set the location type to **automatic**. 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 an automatic connection, use the following command:

```
Command> set location Locname automatic
```

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 an automatic 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. 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 15-12.

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 is a 32-bit hexadecimal value. 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 number.

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 – Releases earlier than ComOS 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 are used to dial the location *home*, while other ports are not used.

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 must 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 255. 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 10, "Using ISDN BRI."

Setting CHAP

When you enter a username and password into the location table, they are used as the system identifier and the RSA Data Security, Inc. MD5 Message-Digest Algorithm (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 are replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments 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 establish 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 must 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 is 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. Consider these activities 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 12, "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 automatic. 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 automatic or on-demand.

To test your configuration, use the following command:

```
Command> dial Locname [-x]
```

Using Modems 9

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:

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 data terminal equipment (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 a modem 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                                Wait for Reply
                -------------------------------------------  ------------------
                AT&F2&C1&D3S0=1S2=129s10=20&W                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 9-1 shows the current factory default settings for commonly used modems.

Table 9-1 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	115200	AT&F1&C1&D2&K3S0=1S2=129S10=20&W0&W1
card-v34-p	Cardinal MVP288CC PCMCIA	115200	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	115200	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	115200	AT&F&C1&D3S0=1S10=20&W0
hay-cent2	Hayes Century 2 Rack V.32bis	115200	AT&F&C1&D2&K3S0=1S10=20&W0
intel-v32-p	Intel V.32bis PCMCIA	115200	AT&F&C1&D3S0=1&W&W1^\rOK
megahz-v32-p	Megahertz XJ2288 V.34bis PCMCIA	115200	AT&F&C1&D3S0=1&W
megahz-v32-p	Megahertz XJ2288 V.34bis PCMCIA	115200	AT&F&C1&D3S0=1&W
micro-desk	Microcom 28.8	115200	AT&F&C1&D2$B115200\\Q3%U1&T5S0=1S10=20*W0&Y0
mot-uds	Motorola UDS V.34	115200	AT&F&C1&D2\\Q3S0=1S10=20S80=18&W
mot-bit	Motorola Bitsurfr	115200	AT&F&C1&D2%A4=1%A2=95&m0@P2=115200@P1=a&W
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

Table 9-1 Factory Default Modem Table Entries *(Continued)*

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
multizdx	MultiTech Z/DX fax/data v.32	115200	AT&F^ATM0&E1&C1&D3$SB115200S0=1S10=20%E0&W0
multi-v34	MultiTech MT2834 28.8k	115200	AT&F^AT&C1&D3S0=1&W0
multi-v34	MultiTech MT2834 28.8k	115200	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	115200	AT&F0M0S0=1V1&C1&D3&K3&W0&W1
para3811	Paradyne 3811+	115200	AT&FS0=1&W
ppi-v34-p	PPI ProClass V.34 PCMCIA	115200	AT&F&C1&D3&K3S0=1&W&W1
premax-v32-p	Premax V.32bis PCMCIA	115200	AT&F&C1&D3S0=1&W&W1
scout-v32-p	DSI Scout V.32bis PCMCIA	115200	AT&F&C1&D3S0=1&W
supra-288	Supra V.34	115200	AT&F2S0=1&W
supra-fax-288	SupraFax 28.8	115200	AT&F2&C1&D3S0=1S2=129s10=20&W
tdk-288-p	TDK DF2814 V.Fast PCMCIA	115200	AT&F&C1&D3S0=1&W
usr-v32-p	USR Courier/Sportster V.32bis PCMCIA	57600	AT&F1&W
usr-v34-p	USR Courier/Sportster V.34 PCMCIA	115200	AT&F1S0=1&W
usr-v32	USR Courier/Sportster V.32bis	57600	AT&F1S0=1&W

Table 9-1 Factory Default Modem Table Entries *(Continued)*

Modem Name (Short)	Modem Name (Long)	DTE Rate	Initialization String
usr-v34	USR Courier/Sportster V.34	115200	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	115200	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-type 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 9-6.

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 must 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 must 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:

```
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 9-2 describes the parity options.

Table 9-2 Parity Options

Option	Description
none	Assumes 8 databits, 1 stop bit, and no parity bit. This is the default.
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 data stream 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, 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.

Using ISDN BRI 10

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:

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 16, "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 service.

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 10-1 shows an example of an ISDN connection.

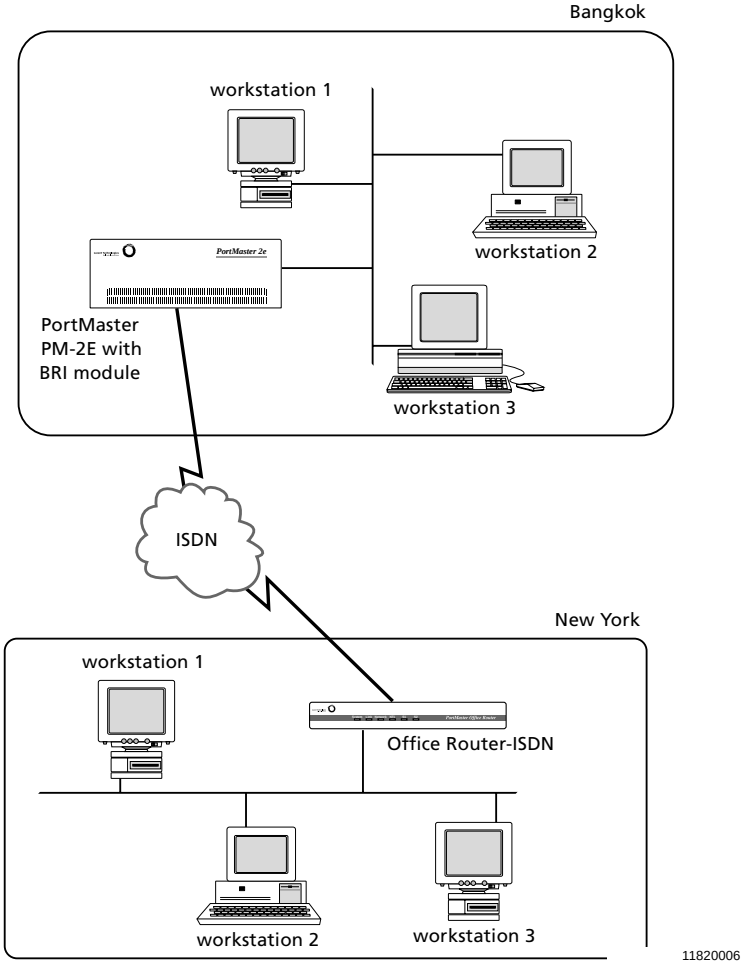
You can use PAP and CHAP for dial-in and dial-out authentication.

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 10-1 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 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 10-1.

Table 10-1 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 following international ISDN standards uses a different set of switch type settings, shown in Table 10-2.

Table 10-2 International ISDN BRI Switch Types

ISDN Switch Type	Used for
net3	EuroISDN standard (includes Swiss standards)
net5	Australia
vn2	France

Table 10-2 International ISDN BRI Switch Types *(Continued)*

ISDN Switch Type	Used for
vn4	France—current national switch type
1tr6	Germany—older switch type
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|net5|vn2|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 S10 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 S10 dn Number
Command> set S10 directory Number
```

Enter the following command to save the configuration to nonvolatile RAM:

```
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 telephone numbers within a setup message in ISDN. These values can vary among countries and telephone companies.

You can configure the PortMaster to automatically detect 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 recvcd 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 to place outbound calls successfully), 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 to place outbound calls successfully), 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 with Multilink PPP as defined in RFC 1717 or with 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 PortMaster 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:

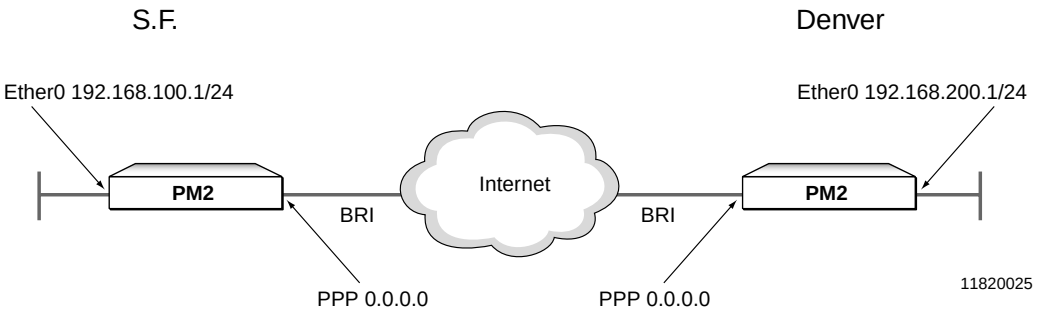
1. **Use a cable with RJ-45 connectors to connect the BRI port to the ISDN telephone line.**

Warning – 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 10-11).
   b. Configure Ethernet interface settings (page 10-12).
   c. Configure ISDN port settings (page 10-12).
   d. Configure dial-in users (page 10-13).
   e. Configure dial-out locations (page 10-14).
3. **Configure the following settings for the PortMaster in San Francisco:**
   a. Configure global settings (page 10-16).
   b. Configure Ethernet interface settings (page 10-16).
   c. Configure ISDN port settings (page 10-17).
   d. Configure dial-in users (page 10-18).
   e. Configure dial-out locations (page 10-19).
4. **Test the configuration (page 10-20).**
5. **Troubleshoot the configuration (page 10-21).**

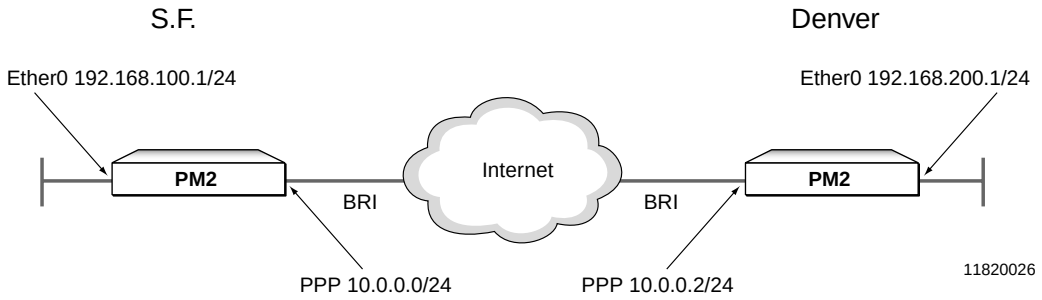
Figure 10-2 illustrates the ISDN BRI example in this section using unnumbered interfaces.

Figure 10-2 ISDN BRI Unnumbered



For comparison, Figure 10-3 shows a similar configuration using ISDN BRI with numbered interfaces.

Figure 10-3 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 10-3.

Table 10-3 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 10-3, 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 10-4.

Table 10-4 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 10-4, 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 10-5 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 10-5 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** *5551111*
Directory number S2	**set** *s2* **directory** *7005551112*
SPID S1	**set** *s1* **spid** *700555111100*
SPID S2	**set** *s2* **spid** *700555111201*

All the other parameters are left at their default values.

After you configure the ISDN BRI port as shown in Table 10-5, 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 10-6.

Table 10-6 User Table Values

Setting	Command
Username	**add netuser** *sf*
Password	**set user** *sf* **password** *anypasswd*
Protocol	**set user** *sf* **protocol** *ppp*

Table 10-6 User Table Values *(Continued)*

Setting	Command
User IP address	**set user** *sf* **address** *192.168.100.1*
Netmask	**set user** *sf* **netmask** *255.255.255.0*
IPX network	**set user** *sf* **ipxnet** *F3*
RIP routing	**set user** *sf* **rip on**
MTU	**set user** *sf* **mtu** *1500*
Compression	**set user** *sf* **compression on**

After you configure the user table as shown in Table 10-6, 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 10-7.

Table 10-7 Location Table Values

Setting	Command
Location name	**add location** *sf*
Type	**set location** *sf* **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** *sf* **protocol** *ppp*
IP destination	**set location** *sf* **destination** *192.168.100.1*
Netmask	**set location** *sf* **netmask** *255.255.255.0*

Table 10-7 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* **idletime** *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 10-7, 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 10-8.

Table 10-8 Global Values

Setting	Command
IP gateway	**set gateway** *192.168.1.2* (This is the address of the next upstream router.)
Default routing	**set default** *off*
System name	**set sysname** *sf*
ISDN switch	**set isdn-switch** *ni-1*

After you configure the global settings shown in Table 10-8, 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 10-9.

Table 10-9 Ethernet Values

Setting	Command
Protocol	**set ether0** *ipx* **enable**
IP address	**set** *ether0* **address** *192.168.100.1*
Netmask	**set** *ether0* **netmask** *255.255.255.0*
IPX network	**set** *ether0* **ipxnet** *F2*
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 10-9, 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 10-10 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 10-10 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** *5552222*
set directory number S2	**set** *s2* **directory** *5552223*
SPID S1	**set** *s1* **spid** *700555222200*
SPID S2	**set** *s2* **spid** *7005552222301*

All the other settings are left at their default values.

After you configure the synchronous WAN port as shown in Table 10-10, 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 10-11.

Table 10-11 User Table Values

Setting	Command
Username	**add netuser** *denver*
Password	**set user** *denver* **password** *anypasswd*
Protocol	**set user** *denver* **protocol** *ppp*
User IP address	**set user** *denver* **address** *192.168.200.1*
Netmask	**set user** *denver* **netmask** *255.255.255.0*
IPX network	**set user** *denver* **ipxnet** *F3*
RIP routing	**set user** *denver* **rip on**
MTU	**set user** *denver* **mtu** *1500*
Compression	**set user** *denver* **compression on**

After you configure the user table as shown in Table 10-11, 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 10-12.

Table 10-12 Location Table Values

Setting	Command
Location name	**add location** *denver*
Type	**set location** *denver* **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** *denver* **protocol** *ppp*
IP destination	**set location** *denver* **destination** *192.168.200.1*
Netmask	**set location** *denver* **netmask** *255.255.255.0*
IPX network	**set location** *denver* **ipxnet** *F3*
RIP routing	**set location** *denver* **rip on**
MTU	**set location** *denver* **mtu** *1500*
Idle timer	**set location** *denver* **idletime** *2*
Dial group	**set location** *denver* **group** *2*
Username	**set location** *denver* **username** *sf*
Telephone number	**set location** *denver* **telephone** *5551212*
Password	**set location** *denver* **password** *anypasswd*
High-water mark	**set location** *denver* **high_water** *0*
Maximum ports	**set location** *denver* **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 10-12, 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 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 are 0 except for a small number of abnormal termination errors resulting from plugging and unplugging cables. 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 solidly lit; otherwise, refer to the hardware installation 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 10-13 describes how to interpret the output of the **show** *S10* command for ISDN BRI ports.

Table 10-13 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.

Configuring the PortMaster 3 11

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:

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 or E1.

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
```

Table 11-1 Line Use Options

Options	Descriptions
isdn	Configures the line as ISDN B channels. This is the default.
t1	Configures the entire line as a T1 line.
e1	Configures the entire line as an E1 line.
fractional	Allows a channelized T1 or E1 line to be divided into groups.
isdn-fractional	Allows an ISDN PRI line to be divided into groups.
inband	Sets the channelized T1 or E1 line for inband signaling.

You use the **fractional** keyword in this command to break up a channelized T1 or E1 line into groups. The **isdn-fractional** keyword refers to PRI.

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 11-2 explains the channel group options.

```
Command> set Line0 group Cgroup channels Channel-list
```

Table 11-2 Channel Group Options

Option	Description
Line0	Line0 or Line1.
Cgroup	Group number from 1 to 63 that designates a port number on each T1 or E1 line or T1 card.
Channel-list	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.

Setting the Channel Rate

To set the channel rate to 56Kbps or 64Kbps for a channel group, use the following command. Table 11-3 explains the channel rate options.

```
Command> set Line0 group Cgroup 56k|64k
```

Table 11-3 Channel Rate Options

Option	Description
Line0	Line0 or Line1.
Cgroup	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 11-4 explains the inband signaling protocol options.

```
Command> set Line0 signaling wink|immediate|fxs
```

Table 11-4 T1 Inband Signaling Protocol Options

Option	Description
Line0	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 PortMaster products do not require dial digits (the calling number and caller ID) when establishing a connection, most telecommunications service providers (telcos) transmit this information by default. You can use the **r2gen** signaling option if you do not require dial digits, but you must first arrange for the telco not to transmit these signals.

The PortMaster defaults to **r2generic** 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 multifrequency robbed-bit signaling (MFR2), you must specify a profile with the **mfr2** option.

To set the inband signaling protocol and the inband call options used with channelized E1, use the following command:

```
Command> set Line0 signaling r2generic|mfr2 Profile
```

Table 11-5 explains the inband signaling protocol options and profiles.

Table 11-5 E1 Inband Signaling Protocol Options

Option	Profile	Description
Line0		Line0 or Line1.
mfr2		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 11-6 explains the ISDN switch options.

```
Command> set isdn-switch ni-2|dms-100|4ess
|att-5ess|net5|vn2|vn3|1tr6|ntt|kdd|ts014
```

Table 11-6 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.

Table 11-6 ISDN Switch Options *(Continued)*

ISDN Switch	Description
att-5ess	AT&T 5ESS.
net5	European ISDN PRI standard.
vn2	France—older switch.
vn3	France—older switch.
1tr6	Germany—older switch.
ntt	Japan.
kdd	Japan.
ts014	Australia. To use this switch type, set the port type to **network hardwired**, set the directory number for the port appropriately, and reset the port.

Setting the Framing Format

To set the framing format for the E1 or T1 line, use the following command. Table 11-7 explains the framing format options.

```
Command> set Line0 framing esf|d4|crc4|fas
```

Table 11-7 T1 Inband Signaling Protocol Options

Option	Description
Line0	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 11-8 explains the encoding method options.

```
Command> set Line0 encoding b8zs|ami|hdb3
```

Table 11-8 Encoding Method Options

Option	Description
Line0	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 method for compressing and expanding, or companding, digitized audio signals.

To set the pulse code modulation, use the following command. Table 11-9 explains the pulse code modulation options.

```
Command> set Line0 pcm u-law|a-law
```

Table 11-9 Pulse Code Modulation Options

Option	Description
Line0	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:

```
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.

You configure a directory number when a T1 line is configured for ISDN PRI. If local exchange numbers are used, however, do not set a directory number because the PortMaster 3 will not respond with the correct telephone number to a second channel request.

If a local exchange is used and no directory is configured, when a second channel is requested the PortMaster 3 uses the caller's Called-Station-ID.

When lines are configured for channelized T1, you must configure a PortMaster 3 directory number because the Called-Station- ID feature is not supported under this configuration.

To set a telephone number for an individual port when the line is configured as ISDN B channels, use the following command. Table 11-10 explains the directory number options.

```
Command> set S0 directory Number
```

Table 11-10 Directory Number Options

Options	Description
S0	One of the ISDN ports
Number	Access telephone number

Using Non-Facility Associated Signaling (NFAS)

Non-facility associated signaling (NFAS) is an ISDN PRI protocol that allows you to define two D channels to carry signaling messages for up to 20 T1 interfaces. This feature relieves telcos and Internet service providers (ISPs) of the need to provide D channel signaling for each T1 interface, and increases bandwidth by making those D channels available to carry data. NFAS is supported only on the PortMaster 3.

To enable NFAS, you configure one T1 line as the primary interface, another T1 line as the secondary interface, and the remaining T1 lines as "slave" interfaces.

The D channel on the primary T1 interface, in "in service" mode, carries signaling messages for the following B channels:

- B channels on its own interface
- B channels on the T1 interface configured as the secondary interface
- B channels on T1 interfaces configured exclusively as slave interfaces

The D channel on the secondary interface, held in standby mode, is referred to as the backup D channel.

Provisioning

Because NFAS requires additional control command exchanges, NFAS T1 interfaces are provisioned differently at the switch. To help you determine the kind of provisioning you require for ISDN setup, refer to the information in the hardware installation guide and on the Lucent website at **http://www.livingston.com**.

Understanding NFAS

After you reboot PortMaster 3s configured for NFAS, D channels on the primary and secondary interfaces initialize in "out of service" mode. The switch then puts the D channel on the primary interface in "in service" mode and the D channel on the secondary interface in standby mode. As call traffic commences on the T1 interfaces, the primary D channel handles signaling messages for all channels in the group, which typically includes the primary T1 interface, the secondary T1 interface, and other T1 interfaces configured as slave interfaces.

If the primary interface fails, the D channel on the secondary interface switches to "in service" mode and begins to carry signaling messages for channels on the secondary T1 interface and all other slave interfaces previously serviced by the primary T1 interface.

Meanwhile, the switch attempts repeatedly to activate the primary interface. When the primary interface comes up, the D channel on that interface goes into standby mode; it does not try to preempt the "in service" function from the secondary interface. Message signals for the reactivated primary T1 interface are carried by the D channel on the secondary T1 interface.

Note that when the primary interface fails, all calls in process are dropped on all interfaces serviced by that D channel. Call traffic does not resume until the D channel on the secondary interface switches to "in service" mode and begins carrying signaling messages.

Multichassis NFAS

The ComOS implementation of NFAS is designed for use across multiple PortMaster 3s configured as a group on the same Ethernet. A group is an arbitrary number between 1 and 99 that you assign to an interface. You can define multiple groups of PortMaster products on the same Ethernet segment, but each group must be supported by its own primary and secondary D channel pair.

NFAS message signaling travels over Ethernet using the User Datagram Protocol (UDP). A reliable, proprietary protocol provides packet sequencing, acknowledgment for packets, and retransmission of lost packets.

The two T1 interfaces of any single PortMaster 3 cannot belong to different groups. If only one interface exists, or if one interface is disabled, the single active interface can be part of a NFAS group by itself. Once you configure NFAS on one PortMaster 3 T1 interface, the other T1 interface cannot run in standard PRI mode.

NFAS without a Backup D Channel

Because the PortMaster 3 has two T1 interfaces, you can run full NFAS on a single PortMaster 3 by configuring one interface as the primary and the other as the secondary. You gain no bandwidth with this configuration, however, because the D channel on each interface is still required for signaling, even though one of the D channels remains in standby mode.

If you do not configure a backup D channel and use a single D channel marked primary, you gain one B channel; the drawback is that if the primary interface fails, you have no backup D channel and no calls are possible on the PortMaster 3 until the primary interface reactivates.

A single D channel can be an acceptable solution if you have only one PortMaster 3 available. If two or more PortMaster 3s are available, a backup D channel on a PortMaster other than the one configured with the primary interface is recommended.

Configuring NFAS

Use the following command to configure NFAS:

```
Command> set Line0 nfas pri|sec|sla|dis Identifier Group
```

You must reboot the PortMaster for the configuration to take effect. Configure each interface on each PortMaster.

Displaying Information About NFAS Configurations

Use the following command to display NFAS parameters on an interface:

```
Command> show Line0
```

Enter the following command to display a list of members, called neighbors, in an NFAS group:

```
Command> show nfas
```

Enter the following command to display the last 40 significant messages exchanged between a PortMaster and its neighbors:

```
Command> show nfas history
```

Enter the following command to display NFAS statistics:

```
Command> show nfas stat
```

Debugging NFAS

To turn on or off print debugging statements for NFAS, use the following command:

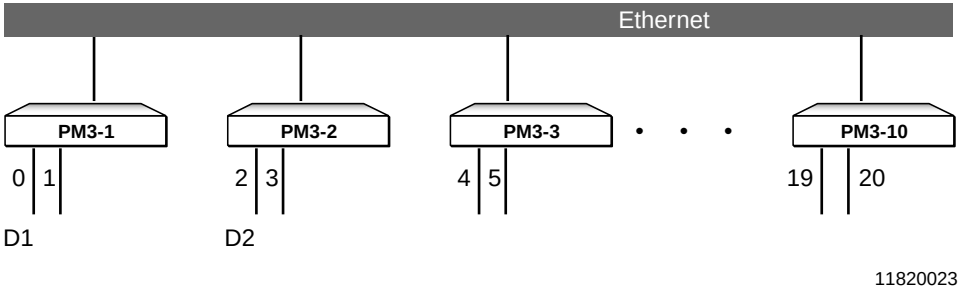
```
Command> set debug nfas on|off
```

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

Example NFAS Configuration

This section shows how to derive the maximum benefit from NFAS by "stacking" 10 PortMaster 3s in a single group (see Figure 11-1). Because two D channels carry message signaling for the entire group, you gain 18 D channels for data transfer.

Figure 11-1 Optimal NFAS Configuration



Sample Configuration

The convention, when configuring NFAS, is to set interface 0 as the primary.

To configure NFAS on the PortMaster 3s illustrated in Figure 11-1, enter the following commands:

```
Command> set line0 nfas pri 0 5
Command> set line0 nfas sla 1 5
Command> set line0 nfas sec 2 5
```

```
Command> set line0 nfas sla 3 5
Command> set line0 nfas sla 4 5
Command> set line0 nfas sla 5 5
Command> set line0 nfas sla 6 5
Command> set line0 nfas sla 7 5
...
```

Configure the remaining PortMaster 3s according to this scheme. Use the **save all** command to save the configuration, and reboot each PortMaster.

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 11-11 explains the digital modem options.

```
Command> set M0 on|off
```

Table 11-11 Digital Modem Options

Option	Description
M0	Any modem number from M0 to M59. Changes to the default setting must be made to individual modems.
on	Makes the modem available for use. This is the default.
off	Busies the modem so it is unavailable.

Note – Digital modems do not require any configuration or initialization string.

Hot-Swapping Digital Modem Cards

With the last call 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 M0 lastcall
```

When the last call 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 11-12 explains the analog modem options.

```
Command> set location Locname analog on|off
```

Table 11-12 Analog Modem Options

Option	Description
Locname	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 M0
```

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 digital 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 can 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|immediate
   ```

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 immediate
Command> set line1 framing esf
Command> set line1 encoding b8zs
Command> save all
Command> reboot
```

To display the line configuration for Line1, 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 channels 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 PortMaster products in a single telephone hunt group, and on the same Ethernet.

Setting Multichassis PPP

To enable Multichassis PPP, set the end point discriminator on all PortMaster products sharing a hunt group and Ethernet to the same 12-digit hexadecimal number. For convenience, you can use the Ethernet MAC address of one PortMaster as the end point discriminator for all the PortMaster porducts 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 end point discriminator to take effect.

Displaying Multichassis PPP Addresses

To display the addresses of the neighboring PortMaster products 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:

```
Command> set debug mdp-status|mdp-events|mcppp-event on|off
```

Table 11-13 explains the debug options for the PortMaster 3

Table 11-13 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.

Configuring Filters 12

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:

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.

In addition to configuring filters at the command line, you can use the Java-based FilterEditor, available at **http://www.livingston.com/forms/one-click-dnload.cgi**, to create, edit, and copy filters across PortMaster products and files. See the FilterEditor online help for more information.

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 12-1 shows different ways to use filters.

Table 12-1 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 12-1 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.

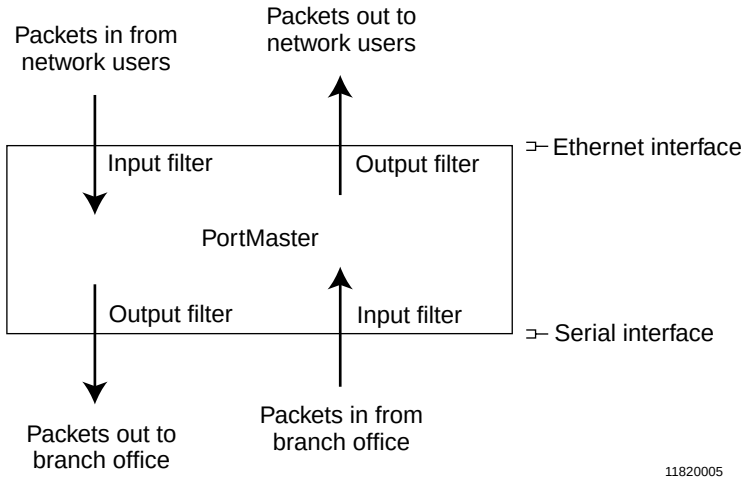
A maximum of 256 filter rules per filter is allowed for the PortMaster 3 and IRX. For other PortMaster products, the maximum number of filter rules allowed is 100. The PortMaster generates an error message when the number of filter rules exceeds the limit.

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 12-1, an input filter is used on packets entering the PortMaster and an output filter is used on packets exiting the PortMaster.

Figure 12-1 Input and Output Filters



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 must 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. 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 12-6
- "Filtering TCP and UDP Packets" on page 12-7
- "Creating IPX Filters" on page 12-7

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 Encapsulating 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) protocol. 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] [notify]
```

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] [notify]
```

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] [notify]
```

Note – ICMP and UDP packets generated by the PortMaster are not blocked by output filters. You must explicitly deny ICMP and UDP packets.

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, test a filter 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. 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 12-2 describes, line by line, each rule in the filter.

Table 12-2 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 12-3 describes, line by line, each rule in the filter.

Table 12-3 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.)
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 must 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 except 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 might 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.

```
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 12-4 describes, line by line, each rule in the filter.

Table 12-4 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 username 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
```

Configuring NAT 13

This chapter describes the ComOS implementation of network address translator (NAT) software. The chapter provides a brief introduction to the feature, followed by a discussion of NAT concepts and detailed configuration guidelines. The chapter concludes with examples of typical uses for the technology.

This chapter includes the following sections:

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

Note – NAT is not supported on the PortMaster Office Router.

Overview of NAT

The Lucent ComOS implementation of the Network Address Translator (NAT) protocol is based on RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*. A network address translator (NAT) is software that runs on a router and maps one IP address or group of IP addresses to another IP address or group of IP addresses. This mapping, or translation, is transparent to users and applications. NAT for ComOS includes the following:

- Basic NAT, or **one-to-one** translation of private IP address to global IP address, requires that one global IP address be available for each internal host with a private address concurrently connecting to an external host.
- Network address port translation (NAPT), or **many-to-one** translation, is an extension to basic NAT whereby multiple IP addresses and associated TCP/UDP ports are translated to a single IP address and its TCP/UDP ports.
- Outsource NAT is an implementation of the NAT protocol in which NAT processing is done on the "server-side" of a connection for external hosts. Outsource NAT can be used for external hosts that do not have the ability to translate private IP addresses to global IP addressees, or as a way to centralize management of external hosts.

The Lucent ComOS supports NAT, NAPT, and outsource NAT for outbound and inbound sessions.

NAT Concepts

This section explains NAT terminology and offers some hints to help you make the most effective use of the NAT software.

Private and Global Addressing

In general for NAT, the terms **private** and **global** refer to addresses in a network, while the terms **internal** and **external** apply to hosts. ComOS maintains NAT map tables of associations of private IP addresses and global IP address.

Private addresses are IP addresses assigned to hosts in a private network. Hosts in a private network are referred to as internal hosts. PortMaster routers running NAT software translate private addresses to global addresses when internal hosts communicate outside the local network.

Global addresses are standard IP addresses that are accessible from any point on the Internet. Global addresses are the addresses of hosts that are external to a private network. When PortMaster routers running NAT software receive IP packets destined for global IP addresses that they maintain in their NAT map tables, they translate the global address to the associated private IP address.

External hosts do not recognize the private IP addresses of internal hosts. Private IP addresses are usually contained within one of several ranges reserved for this purpose. Reserved IP address ranges currently include the following:

- 10.0.0.0 through 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 through 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 through 192.168.255.255 (192.168.0.0/16)

Lucent strongly recommends that you number your private IP networks with IP addresses from one of these ranges.

Note – The 192.168.0.0/16 address range is used in this chapter to represent global addresses in example configurations.

Address Mapping

In the context of NAT, the term **mapping** refers to the association of private IP addresses with global IP addresses. A NAT map is essentially a table where the ComOS stores these associated addresses. The NAT software refers to this table when translating addresses.

NAT maps can be **static** or **dynamic**. With a static address map, a particular private address is always translated to a particular global address; the same private-to-global translation is performed each time address translation is needed. In dynamic address mapping, a private address is translated to the next available global address.

Sessions—Inbound vs. Outbound

A NAT session is a communication that passes through NAT software. Sessions are deemed **inbound** or **outbound** with reference to the router doing the translation. A session originating on an external host is inbound to the NAT router. A session originating on an internal host is outbound to NAT router.

Basic NAT and NAPT

Basic NAT maps one private IP address to one global IP address. This is called **one-to-one** mapping and requires one global IP address for each internal host that attempts to connect concurrently to external hosts. Because basic NAT is capable of many one-to-one mappings of private to global addresses, basic NAT mapping is sometimes referred to as **many-to-many** translation.

For basic NAT, you can configure IP address pools from which IP addresses are allocated dynamically. If all your internal hosts do not usually require global addresses at the same time, you can potentially have an address pool with fewer addresses than you have internal hosts. The obvious danger in this approach is that you will have a shortage on those occasions when all internal hosts try to access the external network simultaneously.

Alternatively, you can guarantee external access for all internal hosts by creating a static map where each private address is permanently assigned to a global address. In this case, the IP address pool size matches the actual number of internal hosts requiring address translation.

The network address port translator (NAPT) differs from basic NAT because it provides external access for a number of internal hosts using a single global IP address. NAPT, referred to as **many-to-one** translation, translates internal addresses to one of the 64,000 available port numbers of a single global address.

NAT Restrictions

The Lucent ComOS implementation of NAT does not support the following:

- ComOS releases before ComOS 3.9
- SNMP applications across network address translation—an Abstract Syntax Notation One (ASN.1) payload might contain IP addresses and TCP/UDP ports of private network.
- DNS zone transfer across network address translation—NAT needs a distinct internal DNS server to maintain name mapping for internal hosts.
- Routing protocols across network address translation—NAT cannot advertise the local network to the backbone.
- NAPT for applications sensitive to client-side TCP/UDP ports, such as **rlogin**.

- End-to-end virtual private network (VPN) tunnels.
- Multicast applications.

NAT Configuration Tasks

This section lists the tasks you must perform to configure NAT on your PortMaster, with references to sections that provide detail and discussion to help you decide the best configuration for your situation.

You configure separate NAT address maps for inbound and for outbound traffic. NAT maps can use static or dynamic address pools. If your environment is a small office, home office (SOHO) with a simple Internet service provider (ISP) dial-up account, or you require no more than a default NAPT map for outbound sessions, refer to the section "Quick Setup of Outbound NAPT" on page 13-32. See also "NAT and NAPT Examples" on page 13-31.

To configure NAT, you must first create a NAT map. Although Lucent recommends the sequence in this section, the rest of the NAT configuration can be done in any order. Perform the following tasks to set up network address translation on your PortMaster:

1. **Create a NAT map.**

   Use the following command to create a NAT map:

   ```
   Command> add map Mapname
   ```

2. **Specify the address map as static or dynamic and enter an address range.**

   a. Use the following command to specify a map type and address range:

   ```
   Command> set map Mapname addressmap|staticaddressmap Ipaddrxfrom Ipaddrxto
   ```

   See "NAT Addressing" on page 13-6 and "NAT Maps" on page 13-9 for a discussion of these topics.

   b. For static address maps that use a TCU/UDP port or port range, use the following command:

   ```
   Command> set map Mapname static-tcp-udp-portmap
   ```

   c. See "Using TCP/UDP Maps" on page 13-18 for details.

   Refer to "Modifying and Deleting Maps" on page 13-14 as needed.

3. **Save the map.**

   Use the following command to save the map:

   ```
   Command> save map
   ```

4. **Specify the direction of an address map and associate it with an interface, user, or location.**

   Use the following command to define the map as inbound or outbound; associate it with an interface, user, or location; and optionally enable the NAT outsource function:

   ```
   Command> set Ether0|S0|W1|location Locname|user|Username nat inmap|outmap
   [outsource]
   ```

   See "Configuring Ports, Locations, and Users for NAT" on page 13-18 for information about associating a map with an interface, user, or location. If you are configuring a PortMaster to do outsource NAT for a client, see "Configuring Outsource NAT" on page 13-24.

5. **Reset active NAT sessions on all interfaces on the PortMaster.**

   Use the following command to reset active NAT sessions on an interface:

   ```
   Command> reset nat [Ether0|S0|W1]
   ```

Refer to "NAT Session Management" on page 13-28 for additional configuration tasks.

NAT Addressing

In network address translation, maps and addressing are closely linked. To distinguish addressing from mapping, this chapter uses the term **pool** to refer to groups or ranges of private and global IP addresses. The term **map** refers to the association of a private address or group of addresses with a global address or group of addresses.

This section discusses inbound and outbound NAT using static and dynamic addressing schemes. The emphasis here is on addressing. The section, "NAT Maps" on page 13-9 covers similar ground but with the emphasis on maps and mapping.

A NAT map is an association of private and global addresses that is stored in a table called a map table. You use the *IPaddrxfrom* and *IPaddrxto* parameters of the **set map** command to configure one-to-one mappings of a private IP address to a global IP

address. These parameters also allow for configuration of the IP address allocation pools from which global IP addresses can be dynamically or statically allocated for outbound sessions.

You can use static or dynamic address maps for outbound NAT; however, you can use only static address maps for inbound NAT.

Configuring Dynamic Address Pools for Outbound NAT

Dynamic address pools are useful when you have fewer global IP addresses than privately addressed internal hosts, provided that all internal hosts do not need a global address at the same time.

After you create a NAT map using the **add map** command, you use the **set map** *Mapname* **addressmap** *Ipaddrxfrom Ipaddrxto* command to set the map as dynamic and define the private address range and the pool of global addresses to which private addresses are translated as needed.

For example, to create an outbound address map called *dynamo.out* that gives the hosts on the private network 10.9.9.0/27 access to the global IP address block 192.168.9.0/28, use the following command:

```
Command> set map dynamo.out 1 addressmap 10.9.9.0/27 192.168.9.0/28
```

Although with dynamic address pools you can map private address blocks to relatively smaller global address blocks, the two-to-one ratio in this example (the netmask /27 provides 30 hosts, while the netmask /28 provides 14 hosts) might be extreme in most cases.

You must also configure a user, location, or port for this map. See "Configuring Ports, Locations, and Users for NAT" on page 13-18.

Configuring Static Address Pools for Outbound NAT

For outbound NAT, you can create an address map that statically maps the private addresses of hosts on an internal network to a pool of global IP addresses.

After you create a NAT map using the **add map** command, you use the **set map** *Mapname* **staticaddressmap** *Ipaddrxfrom Ipaddrxto* command to set the map as static and define the private address range and the pool of global addresses to which private addresses are translated.

For example, to create one-to-one mappings for hosts on a private network with IP addresses in the range 10.1.1.0/24 to global IP addresses in the range 192.168.65.0/24, enter the following command:

```
Command> set map Mapname 1 staticaddressmap 10.1.1.0/24 192.168.65.0/24
```

With this mapping, the host with private IP address 10.1.1.1 is translated to global IP address 192.168.65.1, 10.1.1.2 is translated to global IP address 192.168.65.2, and so on.

When configuring static address maps, make sure that the number of global IP addresses in the pool is equal to the number of private IP addresses.

Configuring Static Address Pools for Inbound NAT

If you want to allow inbound sessions to a group of internal hosts with private IP addresses, you can create an inbound map and apply it to the port.

After you create a NAT map using the **add map** command, you use the **set map** *Mapname* **staticaddressmap** *Ipaddrxfrom Ipaddrxto* command to set the map as static and define the pool of global addresses and the private addresses to which global addresses are translated.

For example, to create an inbound map called *isp.in* to allow inbound sessions from the external 192.168.65.0/24 network to the private 10.1.1.0/24 network, enter the following command:

```
Command> set map isp.in 1 staticaddressmap 192.168.65.0/24 10.1.1.0/24
```

With this address map, the public IP address 192.168.65.1 is always mapped to the private IP address 10.1.1.1, public IP address 192.168.65.2 is always mapped to private IP address 10.1.1.2, and so on.

Mixing IP Address Notations

Although private and global address ranges in a static address pool must be of equal size, they need not be represented in the same notation. You can use a hyphen (-) to separate the two addresses that define a range, use the classless interdomain routing (CIDR) notation, or mix hyphen-separated ranges with CIDR notation.

For example, you can create an inbound map that statically maps 14 private addresses (10.1.1.1-10.1.1.14) to 14 global addresses (192.168.65.1-192.168.65.14) by using the following command:

```
Command> set map Mapname 1 staticaddressmap 192.168.65.1-192.168.65.14
10.1.1.1-10.1.1.14
```

This example uses hyphen-separated address ranges of 14 addresses each. These same address ranges can be configured in CIDR notation as follows:

```
Command> set map Mapname 1 staticaddressmap 192.168.65.0/28 10.1.1.0/28
```

To mix a hyphen-separated address range with an address range of equal size in CIDR notation, enter the addresses as follows:

```
Command> set map Mapname 1 staticaddressmap 192.168.65.0/28 10.1.1.1-10.1.1.14
```

With the /28 netmask, and 192.168.65.0 reserved for the network, 192.168.65.1 through 192.168.65.14 are available for mapping. And because this is a static address map, 10.1.1.1 always maps to 192.168.65.1, 10.1.1.2 always maps to 192.168.65.2, and so on. Again, the only requirement is that the ranges span the same number of addresses.

NAT Maps

Address maps allow you to map the private IP addresses of internal hosts to individual addresses or pools of global addresses. NAT supports static and dynamic address maps. Static address maps establish links between private and global addresses that span multiple sessions. Dynamic address maps establish unique links between private and global addresses for each session.

Mirror image inbound and outbound static address maps are ideal for network renumbering (see "Using Basic NAT to Avoid Address Renumbering" on page 13-34), or in any situation where you require a permanent mapping of private to global addresses.

Dynamic address maps are well suited for all situations that do not require specific mappings of private to global addresses, and in situations where you have more internal hosts than available global addresses.

How NAT Maps Work

NAT maps define the translations between global IP addresses and private IP addresses. ComOS evaluates address mappings from left to right, with the address of the source (whether internal or external) appearing to the left of the address of the destination. When you are viewing a NAT map table or examining an address map you are creating at the PortMaster prompt, the source address—whether local (outbound) or remote (inbound)—always appears on the left.

For example, an outbound map called *isp.out* that translates the private IP address 10.5.3.6 of an internal host to the global IP address 192.168.5.3 is entered as follows:

```
Command> set map isp.out 1 addressmap 10.5.3.6 192.168.5.3
```

The private address (10.5.3.6), which is the address being translated, appears to the left of the global address (192.168.5.3).

In contrast, an inbound map called *isp.in* that translates global IP address 192.168.5.3 to private IP address 10.5.3.6 of an internal host is entered as follows:

```
Command> set map isp.in 1 addressmap 192.168.5.3 10.5.3.6
```

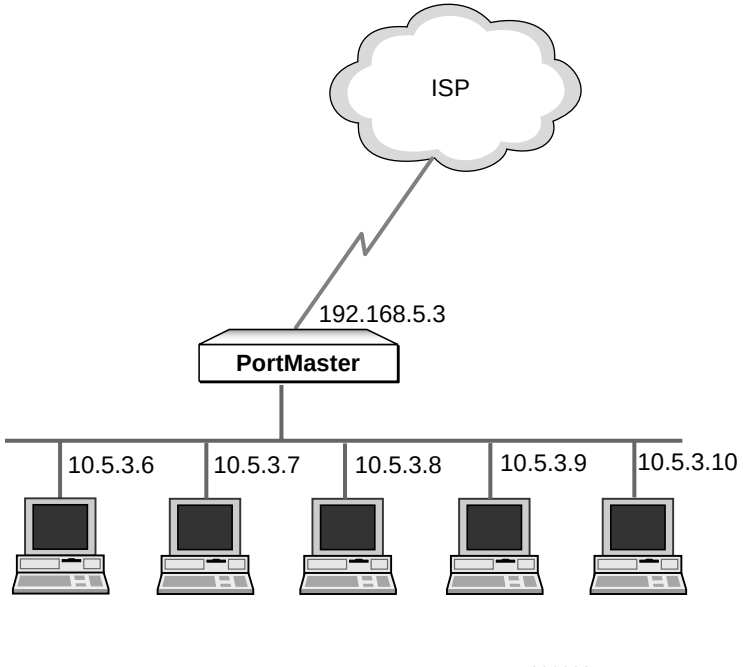
The global address (192.168.5.3), which is the address being translated, now appears to the left of the private address (10.5.3.6).

Creating Maps for Outbound Sessions

You use outbound maps to translate the private IP addresses of internal hosts when those hosts communicate with hosts external to the private network. Outbound maps can be static or dynamic, depending on whether you possess sufficient global addresses for all your internal hosts (see "NAT Addressing" on page 13-6). The two types of address maps (dynamic and static respectively) are equivalent, however, only when you are mapping single IP addresses. In practice, users in a small office, home office (SOHO) generally want to give several internal hosts access to the Internet or to some external host.

Figure 13-1 illustrates a typical use of outbound maps in a SOHO situation in which a PortMaster connects the SOHO to an ISP and does network address translation for one or more internal hosts with private IP addresses.

Figure 13-1 Outbound Map



To map the private address 10.5.3.6 to the global address 192.168.5.3, you can create an outbound map in either of the following ways:

```
Command> set map Mapname 1 addressmap 10.5.3.6 192.168.5.3
```

```
Command> set map Mapname 1 staticaddressmap 10.5.3.6 192.168.5.3
```

The difference between a dynamic address map and a static address map becomes clear when you create an address map to give all hosts in Figure 13-1 access to the Internet. Again, you can do this in either of the following ways:

```
Command> set map Mapname 1 addressmap 10.5.3.6-10.5.3.10
192.168.5.3-192.168.5.7
```

```
Command> set map Mapname 1 staticaddressmap 10.5.3.6-10.5.3.10
192.168.5.3-192.168.5.7
```

The first command uses a dynamic address map (see "Configuring Dynamic Address Pools for Outbound NAT" on page 13-7). With this kind of map, each time an internal host in the address range 10.5.3.6-10.5.3.10 initiates an outbound session, it receives the first available address from the global IP address range 192.168.5.3-192.168.5.7.

The second command uses a static address map (see "Configuring Static Address Pools for Outbound NAT" on page 13-7). In this case, whenever the internal host with private IP address 10.5.3.6 initiates an outbound session, it always maps to global address 192.168.5.3. The internal host with private address 10.5.3.7 always maps to global address 192.168.5.4, and so on.

You must also define a location, user, or port for this map (see "Configuring Ports, Locations, and Users for NAT" on page 13-18). For example, to associate this outbound map, which you name *myisp.outmap*, with location *isp*, enter the following command:

```
Command> set location isp nat outmap myisp.outmap
```

Creating Maps for Inbound Sessions

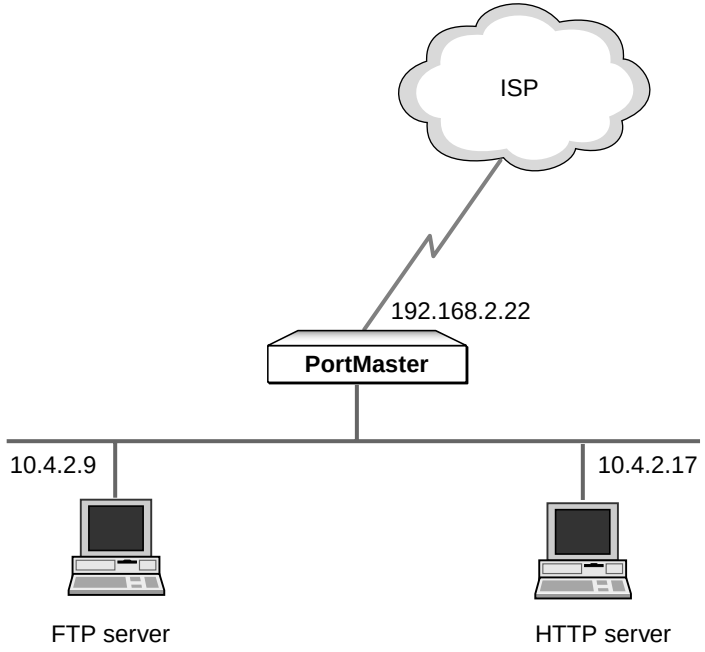
Note – Inbound maps are restricted to static address maps or static TCP or UDP port maps only. Outbound maps do not have this restriction.

Inbound maps are a convenient way to make internal servers accessible to Internet users. You can make an internal web site accessible to the Internet or an external network by mapping the location, which you have set up for dialing to your ISP, to the internal web server. For example, you might set up a web server with the private address 10.4.2.17 (see Figure 13-2). Assume that 192.168.2.22 is the global address assigned to you by your ISP and that this is the address of the PortMaster running NAT.

To configure this router using an inbound map called *isp.in* so that Internet users can connect to your web server, enter the following commands:

```
Command> add map isp.in
Command> set map isp.in 1 static-tcp-udp-portmap 192.168.2.22:http
10.4.2.17:http
```

Figure 13-2 Inbound Map



To make an internal FTP server accessible to Internet users, you can add a rule to *isp.in* that maps the global address of your router to the FTP server.

For example, to allow external access to your internal FTP server with private address 10.4.2.9, you can statically map the internal FTP site to the global address by entering the following commands:

```
Command> set map isp.in 2 static-tcp-udp-portmap 192.168.2.22:ftp 10.4.2.9:ftp
Command> set location isp nat inmap isp.in
```

By adding these two rules to *isp.in*, you ensure that all inbound FTP sessions to 192.168.2.22 are translated to the FTP port at 10.4.2.9, and all inbound HTTP sessions to 192.168.2.22 are translated to the HTTP port at 10.4.2.17. These examples statically map a global address to a specific port on a private address. See "Configuring Static Address Pools for Inbound NAT" on page 13-8 for a discussion of static address-to-address mapping for inbound sessions.

Note – Because ComOS interprets map rules in numerical order, for best performance assign the lowest numbers to the most commonly used rules. See "Modifying and Deleting Maps" on page 13-14 for a guidelines on working with rules.

Modifying and Deleting Maps

You can use the **set map** command to remove the contents of a map or to remove a rule you no longer want.

For example, to remove the contents of a NAT map, enter the following command:

```
Command> set map Mapname blank
```

You can then use the **set map** command to modify the map.

Suppose you have a map called *trustworthy* with the following two rules:

```
Command> show map trustworthy

1. addrmap          172.16.0.0/12 @ipaddr

2. addrmap          10.0.0.0/8 @ipaddr
```

To remove rule 1 from NAT map *trustworthy*, enter the following command:

```
Command> set map trustworthy 1
NAT Map trustworthy has rule 1 Removed.
```

You can enter the following command to verify that the rule has been removed:

```
Command> show map trustworthy

1. addrmap          10.0.0.0/8 @ipaddr
```

Note that rule 2 has now become rule 1.

To add the address map **172.16.0.0/12 @ipaddr** to *trustworthy*, enter the following command:

```
Command> set map trustworthy 2 172.16.0.0/12 @ipaddr
```

Note that what was originally rule 2 now becomes rule 1.

```
Command> show map trustworthy

1. addrmap          10.0.0.0/8 @ipaddr

2. addrmap          172.16.0.0/12 @ipaddr
```

Note – To more easily reassign rule numbers to maps and reorganize rule priority, use PMVision.

To delete a map, use the following command:

```
Command> delete map Mapname
```

Using the @ipaddr Macro

The **@ipaddr** macro causes ComOS to use the IP address assigned to the port for which the address map is being used.

If you want to use the address map for outbound sessions or outbound outsource sessions, you can set the *Ipaddrxto* argument for the **set map addressmap** command to the special macro **@ipaddr**.

For example, to use the special macro **@ipaddr**, enter the following command:

```
Command> set map addressmap 1 0.0.0.0/0 @ipaddr log
```

The resulting map is equivalent to the **defaultnapt** map. You can also use the **@ipaddr** macro to statically map a global address to a TCP or UDP port service—such as FTP or SMTP. With that usage you must specify an IP address.

For example, to use the special macro **@ipaddr** to add a rule to a map for FTP service at host address 10.1.1.1, enter the following command:

```
Command> set map Mapname 1 static-tcp-udp-portmap @ipaddr:ftp 10.1.1.1:ftp
```

You can specify the port number or the port service. See Appendix B, "TCP and UDP Ports and Services," for a complete list of services and their corresponding port numbers.

Using the Default NAPT Map

The reserved map name, **defaultnapt**, subjects all sessions on a port to network address port translation (NAPT) using the IP address assigned to the port. The **defaultnapt** map name is supported for outbound NAPT only.

When you assign **defaultnapt** to **outmap**, all outbound IP sessions from a given port are subject to NAPT using the IP address assigned to the port.

If you assign **defaultnapt** to **outmap** for the outsource port (the **outsource** option in the command), all inbound IP sessions on a given port are subject to outsource NAPT using the IP address assigned to the port.

To configure default NAPT outsource on your PortMaster, follow these steps:

1. **Set the map to defaultnapt, associate it with a user, location, or interface, identify it as inbound or outbound, and specify the outsource function.**

   ```
   Command> set user superfly nat outmap defaultnapt outsource
   ```

   In this example, user *superfly* is configured for default NAPT outsource.

2. **Set the destination IP address of the network user.**

   ```
   Command> set user superfly destination 192.168.200.112
   ```

   This command sets the IP address of the user (see Figure 13-3). In this example, user *superfly*, whose workstation has a private IP address, is assigned the destination address of the port on the local non-NAT router that connects to the PortMaster doing network address translation for it.

3. **Set the netmask for user** ***superfly*****.**

   ```
   Command> set user superfly netmask 255.255.255.255
   ```

4. **Set the IP address of the network user.**

   ```
   Command> set user superfly address|destination 192.168.200.112
   ```

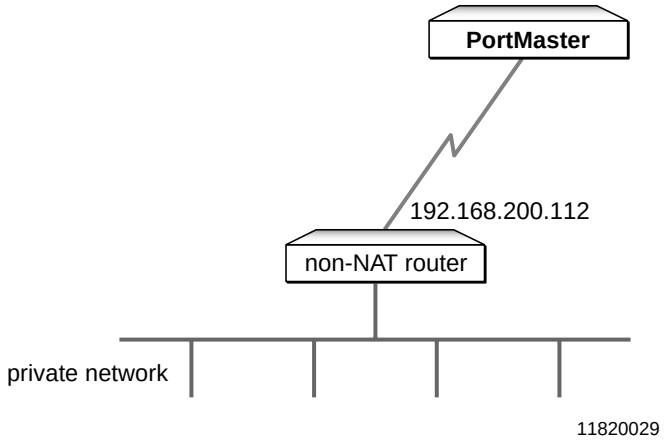
   The **set user address** and **set user destination** commands are synonyms for each other. Note that the IP address is the address of the local router.

5. Set the IP address of the PortMaster serial port to the IP address of the network user.

```
Command> set user superfly local-ip-address 192.168 24.65
```

This command creates a dial-out point-to-point network connection when both ends require an IP address. The IP address is the address of the PortMaster doing network address translation for this workstation (see Figure 13-3).

Figure 13-3 Default NAPT Outsource



Note – In this release of NAT, inbound maps are restricted and can contain static address maps and/or static TCP/UDP port maps only. Outbound maps do not have this limitation.

When configuring NAT for a specific port, user, or location, you need not translate all the hosts behind the NAT. By configuring address maps carefully, you can be highly selective about which hosts use NAT processing.

Using TCP/UDP Maps

The *Portname* variable in the **set map** command can be a port name or a decimal value between 1 and 65535. Table 13-1 lists common TCP/UDP port names and associated decimal values. See Appendix B, "TCP and UDP Ports and Services," for a complete list of well-known services

Table 13-1 TCP/UDP Ports

Port Name	Decimal Value
Telnet	TCP: 23
FTP	TCP: 20/21
TFTP	UDP: 69
HTTP	TCP: 80
DNS	TCP/UDP: 53
SMTP	TCP: 25
RADIUS	UDP: 1645

By using the *Ipaddrxfrom*:{*Tport1*|*Portname*} *Ipaddrxto*:{*Tport2*|*Portname*} syntax, you can define ports or a range of ports for a static map. This approach obviates the need to set up a number of map rules.

For example, you can statically map an internal web server with private IP address 10.1.1.10 to global IP address 192.168.1.10 in either of the following ways:

```
Command> set map Mapname static-tcp-udp-portmap 192.168.1.10:http
10.1.1.10:http

Command> set map Mapname static-tcp-udp-portmap 192.168.1.10:80 10.1.1.10:80
```

Configuring Ports, Locations, and Users for NAT

When you apply NAT to a port, location, or user, think of NAT as just another parameter to the **set** command.

NAT parameters that must be preceded with **set** *Ether0* | *S0* | *W1* **nat**, **set location** *Locname* **nat**, or **set user** *Username* **nat** include the following:

- **sessiontimeout** [**tcp** | **other**] *Number* [**minutes** | **seconds**]
- **log sessionfail** | **sessionsuccess** | **syslog** | **console** [**on** | **off**]
- **session-direction-fail-action drop** | **icmpreject** | **passthrough**
- **inmap** *Mapname* [**outsource**]
- **outmap** *Mapname* [**outsource**]

Configuring Ports for NAT

NAT port configuration varies according to the use you intend for the port. You can configure a port for inbound service, outbound service, or both. You can apply static address maps or dynamic address maps to the port. Or you can use the reserved map name **defaultnapt**, or the special macro **@ipaddr**.

This section offers general guidelines and discusses options for NAT port configuration.

See "defaultnapt Providing Inbound HTTP Service" on page 13-37 for an example of NAT port configuration. Refer to the *PortMaster Command Line Reference* for command details.

To configure a port for NAT service, follow these steps:

1. **Set the address of the port.**

   Use the following command to set the local IP address of the port:

   ```
   Command> set Ether0|S0|W1 Ipaddress
   ```

2. **Create a NAT map.**

   You must create a NAT map for address translation. If the port will be used for both inbound and outbound NAT, you must create two maps. Use the following command to add a map to the map table:

   ```
   Command> add map Mapname
   ```

3. **Define the map.**

   You must define the map as static or dynamic, enter an appropriate rule number, and specify the addresses or ranges of addresses. Use the following command to define the map:

   Command> **set map** *Mapname Rulenumber* **addressmap**|**staticaddressmap** *Ipaddrxfrom Ipaddrxto*

   If you want the map to provide inbound access to particular services such as FTP or HTTP, use the following command to define the map:

   Command> **set map** *Mapname* **static-tcp-udp-portmap** *Ipaddrxfrom*:{*Tport1*|*Portname*} *Ipaddrxto*:{*Tport2*|*Portname*}

4. **Associate the map to the port as inbound, outbound, or default NAPT.**

   Use the following command to apply an inbound or outbound map to a port:

   Command> **set** *Ether0*|*S0*|*W1* **nat inmap**|**outmap defaultnapt**|*Mapname*

   When you use **defaultnapt** as the map, you do not need to indicate whether the map is static or dynamic or specify addresses.

5. **Set the idle time for a NAT session.**

   Use the following command to set the maximum idle time for a NAT session:

   Command> **set nat** *Ether0*|*S0*|*W1* **sessiontimeout**

6. **Set the default action that the PortMaster takes in the event that a request for a NAT session is refused.**

   Use the following command to specify the action the PortMaster takes when a session is refused:

   Command> **set nat** *Ether0*|*S0*|*W1* **session-direction-fail-action drop**|**icmpreject**|**passthrough**

7. **Reset the port.**

   Use the following command to reset NAT on the port:

   Command> **reset nat** *Ether0*|*S0*|*W1*

Configuring Locations for NAT

You can set up to 20 parameters when configuring a NAT location. This section offers general guidelines and discusses some common options.

See "Setting Up a Dial-Out Location Using defaultnapt" on page 13-33 for an example of NAT location configuration. Refer to the *PortMaster Command Line Reference* for command details.

1. **Create a location.**

   Use the following command to add a location to the location table:

   ```
   Command> add location Locname
   ```

2. **Assign the location a telephone number.**

   Use the following command to assign a telephone number to the location:

   ```
   Command> set location Locname telephone 5551212
   ```

3. **Set the username for the dial-out location.**

   Use the following command to set a user to the location:

   ```
   Command> set location Locname user Username
   ```

4. **Set the user password for the location.**

   Use the following command to set the password:

   ```
   Command> set location Locname password Password
   ```

5. **Set the protocol for the location.**

   Use the following command to set the transport protocol:

   ```
   Command> set location Locname protocol slip|ppp|frame_relay|x75-sync
   ```

6. **Set the destination address.**

   Use the following command to set the destination IP address:

   ```
   Command> set location Locname destination Ipaddress|negotiated
   ```

7. **Set the maximum number of dial-out ports for this location.**

   Use the following command to set the maximum number of network dial-out ports that the PortMaster can use for this location:

   ```
   Command> set location Locname maxports Number
   ```

8. **Set the local IP address of the port.**

   Use the following command to set the local IP address of the port:

   ```
   Command> set location Locname local-ip-address Ipaddress|assigned
   ```

9. **Set the NAT map to use for this location.**

   Use the following command to associate a NAT map to the location:

   ```
   Command> set location Locname nat inmap|outmap defaultnapt|Mapname
   ```

10. **Set the idle time for a NAT session.**

    Use the following command to set the maximum idle time for a NAT session:

    ```
    Command> set nat Ether0|S0|W1 sessiontimeout
    ```

11. **Set the default action that the PortMaster takes in the event that a request for a NAT session is refused.**

    Use the following command to specify the action the PortMaster takes when a session is refused:

    ```
    Command> set nat Ether0|S0|W1 session-direction-fail-action
    drop|icmpreject|passthrough
    ```

Configuring NAT Users

By configuring NAT users, you can allow them to dial in to a PortMaster doing outsource network address translation.

1. **Add a NAT user.**

   Use the following command to add a user to the user table:

   ```
   Command> add netuser Username
   ```

2. **Set the user password.**

   Use the following command to set a password for the user:

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

3. **Set the maximum number of ports.**

   Use the following command to set the maximum number of network dial-out ports for this user:

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

4. **Set the protocol.**

   User the following command to set the transport protocol for this user:

   ```
   Command> set user Username protocol slip|ppp|x75-sync
   ```

5. **Set the destination address.**

   Use the following command to set the IP address of the user:

   ```
   Command> set user Username address Ipaddress
   ```

6. **Set the local IP address.**

   Use the following command to set the local IP address on the PortMaster that the user dials in to:

   ```
   Command> set user Username local-ip-address Ipaddress
   ```

7. **Associate the user with a NAT map.**

   Use the following command to associate the user with a NAT map:

   ```
   Command> set user Username nat inmap|outmap defaultnapt Mapname
   ```

8. **Set the idle time for a NAT session.**

   Use the following command to set the maximum idle time for a NAT session:

   ```
   Command> set nat Ether0|S0|W1 sessiontimeout
   ```

9. **Set the default action that the PortMaster takes in the event that a request for a NAT session is refused.**

   Use the following command to specify the action the PortMaster takes when a session is refused:

   ```
   Command> set nat Ether0|S0|W1 session-direction-fail-action
   drop|icmpreject|passthrough
   ```

Configuring Outsource NAT

In an outsource NAT configuration, address translation is done on a PortMaster (typically at an ISP) for clients who do not have the capability to run NAT on their local router. Outsource mode NAT allows a PortMaster to handle the NAT processing and management for one or more connected network interfaces. When a remote client dials in to a WAN port on a PortMaster configured to do network address translation for it, the PortMaster performs NAT service for that device.

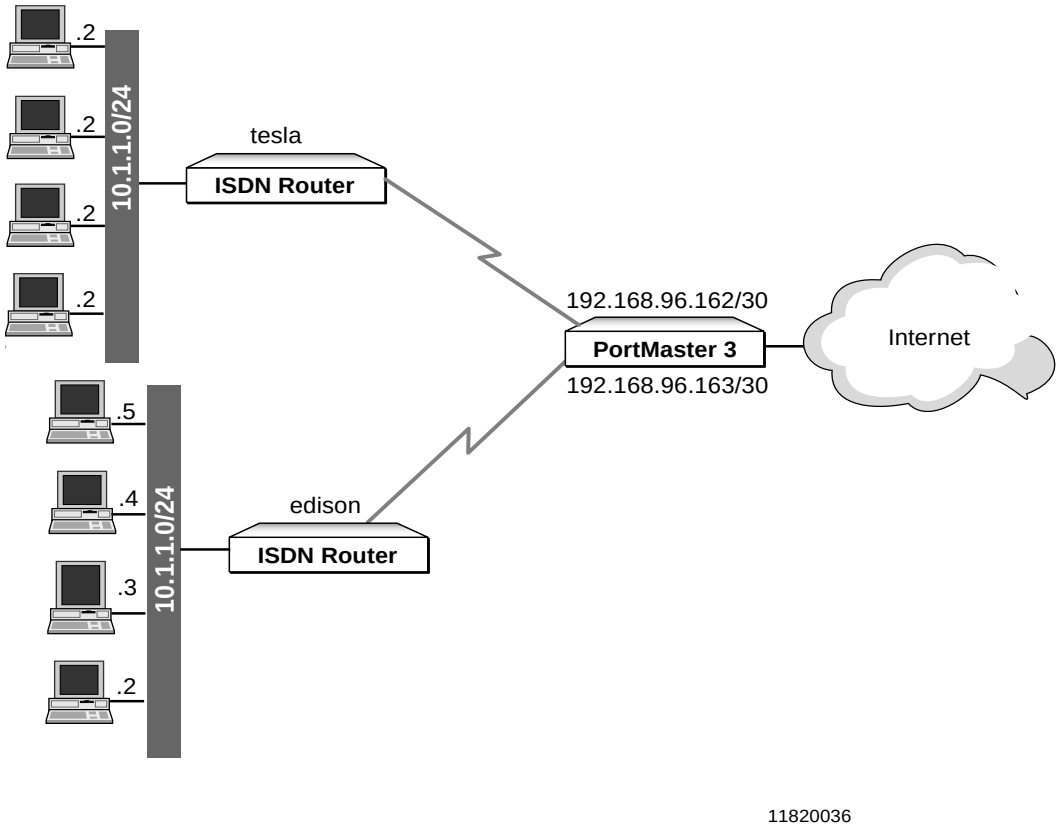
With outsource NAT, all NAT configuration is done on the PortMaster, where a central site administrator maintains NAT mappings for all sites connected to it. Central site administration avoids the complexity of managing a number of separate routers with different capabilities.

In Figure 13-4, a PortMaster at an ISP does network address translation for two sites that dial in via ISDN routers, which cannot do network address translation. Note that both sites, which are different clients of the ISP, use the same 10.1.1.0/24 network.

As long as the individual client networks connect to different interfaces on the PortMaster, there is no conflict of address space. In this example, network user **tesla** and network user **edison** have assigned identical IP addresses to their workstations, but the PortMaster running NAT does not confuse them.

This aspect of the NAT protocol is convenient for situations in which companies merge, or when large companies take over small companies. Rather than search through potentially thousands of private addresses for conflicts, or renumber entire networks (see "Using Basic NAT to Avoid Address Renumbering" on page 13-34), you can simply configure network address translation on strategically located PortMaster products.

Figure 13-4 Outsource NAT Scenario



Configuration for tesla

To configure outsource NAT for user **tesla** as illustrated in Figure 13-4, follow this procedure:

1. **Create user tesla.**

   ```
   Command> add netuser tesla
   ```

2. **Set a password for user tesla.**

   ```
   Command> set user tesla password ACpower
   ```

3. **Set the maximum network dial-out ports for this user.**

   ```
   Command> set user tesla maxports 2
   ```

4. **Set the protocol to ppp.**

   ```
   Command> set user tesla protocol ppp
   ```

5. **Set the destination address.**

   ```
   Command> set user tesla destination 192.168.129.130
   ```

6. **Set the local IP address of the port.**

   ```
   Command> set user tesla local-ip-address 192.168.96.162
   ```

7. **Set the map to defaultnapt outsource.**

   ```
   Command> set user tesla nat outmap defaultnapt outsource
   ```

No NAT configuration is needed on the dial-up router side.

FTP Configuration for tesla

If you want user **tesla** to be able to run an FTP server (with private IP address 10.1.1.1) on his network and have it accessible globally, you must complete the following additional steps:

1. **Create an inbound map called tesla.inmap.**

   ```
   Command> add map tesla.inmap
   ```

2. **Set the TCP/UDP port mapping, and set the port being configured as the destination address.**

   ```
   Command> set map tesla.inmap 1 static-tcp-udp-portmap @ipaddr:ftp 10.1.1.1:ftp
   ```

3. **Specify that the map be used in outsource mode.**

   ```
   Command> set user tesla nat inmap tesla.inmap outsource
   ```

Configuration for edison

To configure outsource NAT for user **edison** as illustrated in Figure 13-4, follow this procedure:

1. **Create user edison.**

   ```
   Command> add netuser edison
   ```

2. **Set a password for user edison.**

   ```
   Command> set user edison password DCpower
   ```

3. **Set the maximum network dial-out ports for this user.**

   ```
   Command> set user edison maxports 2
   ```

4. **Set the protocol to ppp.**

   ```
   Command> set user edison protocol ppp
   ```

5. **Set the destination address.**

   ```
   Command> set user edison destination 192.168.129.130
   ```

6. **Set the local IP address of the port.**

   ```
   Command> set user edison local-ip-address 192.168.96.163
   ```

7. **Set the map to default NAPT outsource.**

   ```
   Command> set user edison nat outmap defaultnapt outsource
   ```

No NAT configuration is needed on the dial-up router side.

FTP Configuration for edison

If you want user **edison** to be able to run an FTP server (with private IP address 10.1.1.1.) on his network and have it accessible globally, you must complete the following additional steps:

1. **Create an inbound map called edison.inmap.**

   ```
   Command> add map edison.inmap
   ```

2. **Set the TCP/UDP port mapping, and set the port being configured as the destination address.**

   ```
   Command> set map edison.inmap 1 static-tcp-udp-portmap @ipaddr:ftp
   10.1.1.1:ftp
   ```

3. **Specify that the map be used in outsource mode.**

   ```
   Command> set user edison nat inmap edison.inmap outsource
   ```

NAT Session Management

A NAT session is any active connection involving network address translation. You can view and manage NAT sessions in several ways. To display active NAT sessions, enter the following command:

```
Command> show nat sessions
```

To view statistics on NAT in real time, enter the following command:

```
Command> show nat statistics
```

This command displays statistics on a per port basis, including successful translations, failures, address shortages (when you are using IP pools), and unsuccessful translations and lookups due to timeouts.

To display a list of active IP address and port bindings, including a list of the remaining resources available for use (such as TCP/UDP ports or IP addresses), enter the following command:

```
Command> show nat mapusage
```

This command is useful for debugging and to monitor resource use.

Resetting NAT Sessions

When you modify a NAT configuration on an active port or interface, you must reset the interface or port for the changes to take effect. To reset a port or interface, use the following command:

```
Command> reset nat [Ether0|S0|W1]
```

To reset all existing NAT sessions, you can globally reset the entire NAT subsystem by entering the following command:

```
Command> reset nat
```

Caution – This command resets all existing NAT sessions on the PortMaster just as if it had been rebooted. When you reset NAT on a PortMaster with active sessions, some connections might be left open on clients and servers or not shut down properly. Because globally resetting NAT can leave connections between hosts in an unknown state, Lucent recommends that you avoid using this command while sessions are active.

You can delete individual sessions by specifying the session identification number. Use the **show nat sessions** command to display session identification numbers, then use the following command to delete NAT sessions by session ID:

```
Command> delete nat sessions Sessionid
```

Administration Considerations for NAT

A few special considerations must be taken when configuring your network in the presence of a NAT.

Advertising Routing Information

Because NAT maps private addresses to global addresses, you must disable network advertisements on the NAT router global interface.

For example, if you are running NAT on an PortMaster IRX-211 with Ether0 as your private interface and Ether1 (on which you have NAT enabled) as your global interface, you must disable RIP broadcasts. To disable RIP broadcasts on the global interface, enter the following command to set RIP to listen only:

```
Command> set ether1 rip listen
```

If you want no routing updates, enter the following command:

```
Command> set ether1 rip off
```

If you are using OSPF, specify the private IP address range as **quiet** by entering the following command:

```
Command> set ospf area 0.0.0.0 range 10.0.0.0/8 quiet
```

If you are using BGP, you must ensure that you do not advertise private IP address blocks to the Internet. Refer to the *PortMaster Routing Guide* for details.

Routing Global IP Addresses for NAT and Static Routing

Because NAT is not designed to advertise routing, the global IP addresses (or networks) used by NAT might require that you add static routes on the routers with which the PortMaster has an external peer relationship. In particular, when basic NAT assumes management of a pool of global addresses, you must add a static route for the pool of addresses on the next-hop router of the PortMaster.

For example, if a PortMaster 3 is providing outsource NAT service for dial-in networks and is using the 192.168.38.0/24 network (subnetted for the numbered IP links), the post-NAT packets have 192.168.38.*x* as the source address. Another router on the same segment as the PortMaster 3 must have a static route to return the response packets with a destination IP address of 192.168.38.*x* to the PortMaster 3 running outsource NAT.

Ethernet ARP

NAT does not provide Ethernet ARP services for the global IP addresses it uses. For this reason Lucent recommends that NAT be configured on WAN interfaces. If you choose to configure basic NAT on a LAN interface, however, be sure to select a global IP address block (for use in conjunction with NAT) that does not fall within the same network prefix of the LAN interface itself.

NAT Security

Security is viewed differently in different environments. Because NAT provides a one-way session traffic filter that restricts sessions from external hosts into your network, NAT provides a certain degree of security.

In addition, because address assignment in NAT is often done dynamically, an attacker has more difficulty pointing to a specific host in the NAT domain as a potential target. Partial privacy is gained because an individual connection is harder to trace to a particular user.

You can use firewalls in conjunction with NATs to provide additional filtering of unwanted traffic. However, NATs cannot by themselves transparently support all applications and often must coexist with application-level gateways (ALGs) such as

SOCKS. Customers looking to deploy NAT must determine their application requirements before they can assess any possible security that the extensions to NAT might add to their network.

In fact, the use of NATs can compromise security by allowing the end user traffic payload to be "sniffed" by the NAT routers and/or ALG extensions. NAT routers that are not within a trusted boundary can cause a security problem. Although you can encrypt NAT traffic, usually NAT must be the end point to such encryption and decryption. For example, you cannot configure end-to-end IPSec with NAT routers in between. The end point must be a NAT router.

In addition, NAT operation can have an unintended consequence. Placing your private network behind a NAT often makes the network appear inaccessible from the outside.

NAT is not an all-in-one security solution. You must evaluate your organization's particular configuration and network topology to determine whether NAT will eliminate any need for further security measures, such as a firewall.

DNS

When configuring DNS on hosts behind a NAT, you can add a map similar to the following *dns.inmap* example on the internal interface, which is usually Ether0 on a PortMaster. Alternatively, you can enter the IP address of your PortMaster as the DNS server. This type of map is useful if you do not always have the same DNS server (multiple providers) but do not want to reconfigure all your private hosts.

```
Command> set dns.inmap 1 static-tcp-udp-portmap @ipaddr:dns
Ipaddrxto:{Tport1|Portname}
Command> set ether0 nat inmap dns.inmap
```

NAT and NAPT Examples

This section includes the following NAT example configurations:

Quick Setup of Outbound NAPT

This section provides guidelines for quick setup of outbound NAPT. Outbound NAPT, or many-to-one, is most common in small office, home office (SOHO) situations where a user dials in to an Internet service provider (ISP) and is assigned a single dynamic IP address.

To configure outbound NAPT for a SOHO, follow this procedure:

1. **Enable NAPT on the router dialing out to a location.**

   For example, to enable NAPT on a PortMaster dialing out to location *myisp*, enter the following command:

   ```
   Command> set location myisp nat outmap defaultnapt
   ```

2. **Set the local IP address for the location to assigned.**

   To set the location address, use the following command:

   ```
   Command> set location myisp local-ip-address assigned
   ```

   This allows the location to receive an IP address dynamically.

3. **Reset the port (if currently connected).**

   To reset the port on which the NAT map has been configured, enter the following command:

   ```
   Command> reset S0|W1
   ```

Note – You must reset the port whenever you add, delete, or modify a map. You then connect as you would normally.

If *myisp* is a dial-on-demand location for which you are configuring NAT for the first time, you must also either reboot the router, or enter the following commands:

```
Command> set location myisp maxports 0
Command> set location myisp manual
Command> reset dialer
```

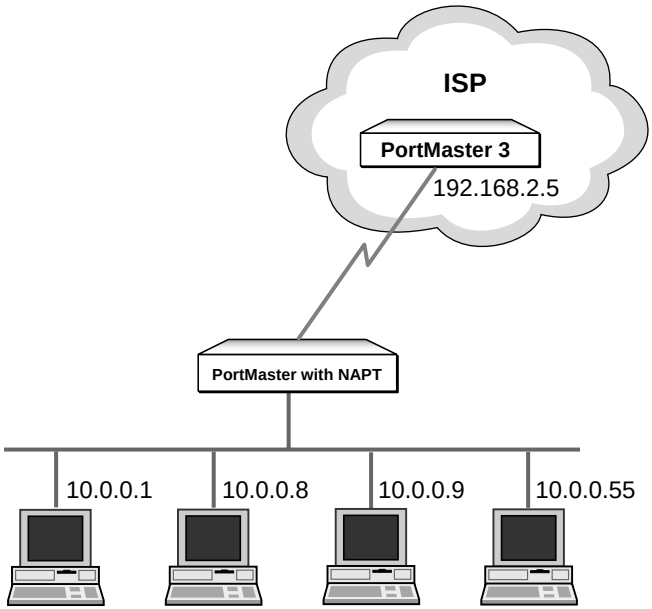
```
Command> set location myisp on-demand
Command> set location myisp maxports 1
Command> reset dialer
```

With the **defaultnapt** configuration, the addresses of all hosts behind the PortMaster are translated to the IP address of the interface that is assigned to the location (see "Using the Default NAPT Map" on page 13-16). If the hosts behind the PortMaster have not yet been configured with IP addresses, see "Private and Global Addressing" on page 13-2.

Setting Up a Dial-Out Location Using defaultnapt

In this example, (Figure 13-5), location *corporate-power* is configured on a PortMaster for user **tesla** to dial in to the corporate network's PortMaster 3 (192.168.2.5). The PortMaster 3 has one IP address dynamically assigned for the PortMaster of user **tesla** in a NAPT configuration. Everything behind this PortMaster is subject to NAPT.

Figure 13-5 Dial-Up Using NAPT



To configure location *corporate-power* as a dial-out location using **defaultnapt** for user **tesla**, as illustrated in Figure 13-5, enter the following commands on the PortMaster:

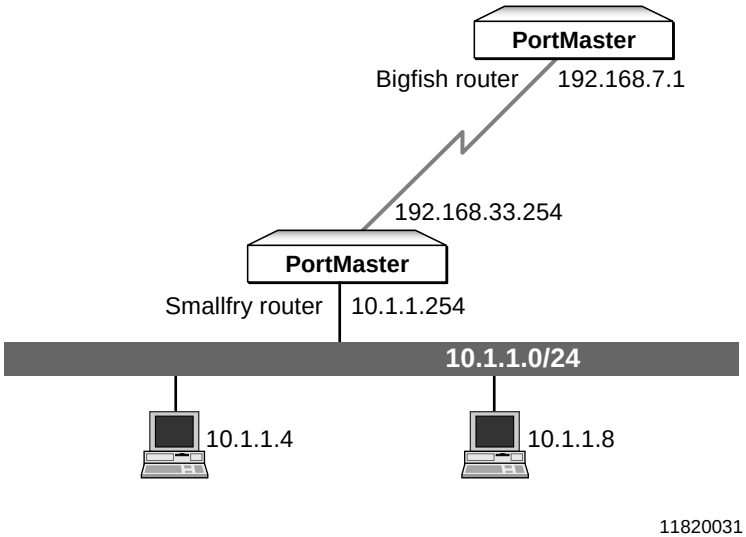
```
Command> add location corporate-power
Command> set location corporate-power telephone 5558583
Command> set location corporate-power username tesla
Command> set location corporate-power password ACrules
Command> set location corporate-power destination 192.168.2.5
Command> set location corporate-power maxports 2
Command> set location corporate-power idletime 15 minutes
Command> set location corporate-power on-demand
Command> set location corporate-power local-ip-address assigned
Command> set location corporate nat outmap defaultnapt
```

Using Basic NAT to Avoid Address Renumbering

This example shows how you can avoid the laborious process and potential errors of renumbering the IP addresses of hosts in an existing network when merging with a larger network.

In this example, (Figure 13-6), the company Smallfry (10.1.1.0/24), which has just merged with Bigfish Inc. (192.168.0.0/16), renumbers its hosts to access the Bigfish network. Smallfry has an ISDN connection from its PortMaster to the Bigfish network. Bigfish has assigned Smallfry the IP address range 192.168.33.0/24.

Figure 13-6 Address Renumbering



To use basic NAT to avoid address renumbering as illustrated in Figure 13-6, add the following commands to the Smallfry PortMaster:

```
Command> add map smallfry.outmap
Command> set map smallfry.outmap 1 addressmap 10.1.1.0/24 192.168.33.0/24
Command> add location bigfish
Command> set location bigfish telephone 5558583
Command> set location bigfish username smallfry
Command> set location bigfish password bigsecret
Command> set location bigfish destination 192.168.7.1
Command> set location bigfish maxports 2
Command> set location bigfish idletime 15 minutes
Command> set location bigfish on-demand
Command> set location bigfish local-ip-address 192.168.33.254
Command> set location bigfish nat outmap smallfry.outmap
```

The above **smallfry.outmap** NAT map dynamically assigns IP addresses on an as-needed basis. If you want to statically map IP address translations, change the **smallfry.outmap** as follows:

```
Command> set map smallfry.outmap 1 staticaddressmap 10.1.1.0/24
192.168.33.0/24
```

Redirecting Traffic to a Backup Server

It is periodically necessary to take a server offline for maintenance or to install or update software. This example shows how to use a NAT map to redirect traffic to a backup server.

In this example, the following two servers are connected on the Ether1 port of a PortMaster IRX-211, providing inbound FTP and Web service:

- **primary.web.com** (192.168.2.1)
- **backup.web.com** (192.168.2.2)

All routers and hosts in this example have global IP addresses.

To redirect inbound traffic to the backup server as illustrated in Figure 13-7, add the following lines to the IRX-211 configuration:

```
Command> add map ether0.inmap
Command> set map ether0.inmap 1 addressmap 192.168.2.1 192.168.2.2
Command> set ether0 nat inmap ether0.inmap
Command> reset nat
```

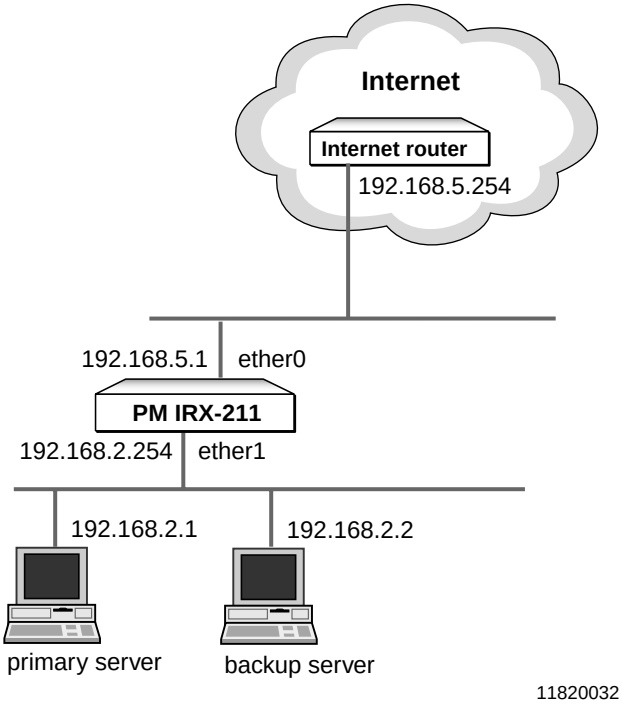
The backup server can now take over the services of the primary server.

You can optionally set the NAT **session-direction-fail-action** (**sdfa**) keyword to **passthrough**. This is useful if, after you bring up primary server, you want to run a Telnet or FTP session from the primary server after you enable it. Under the current configuration, NAT intercepts outbound packets from the remapped host.

To allow outbound sessions from the primary server, enter the following command:

```
Command> set ether0 nat sdfa passthrough
```

Figure 13-7 Redirect Traffic to a Backup Server

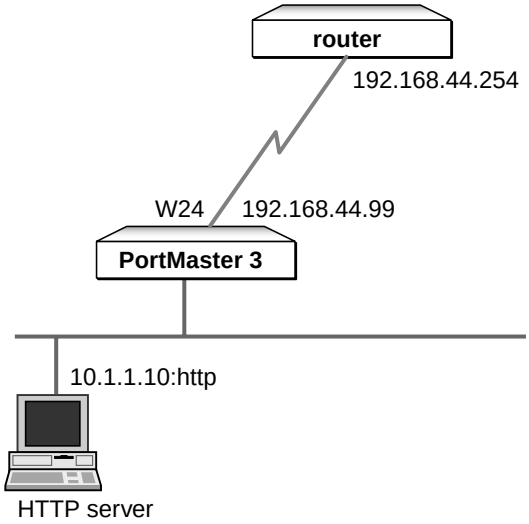


defaultnapt Providing Inbound HTTP Service

This example shows how to direct inbound HTTP packets to an internal HTTP server on a private network, while providing outbound access to the Internet using default NAPT for the other hosts on the private network.

In this example (Figure 13-8), Line1 on a PortMaster 3 is a T1 (WAN) link with the private network 10.0.0.0/8 behind it. The T1 PPP interfaces are numbered with global addresses (local: 192.168.44.99, destination: 192.168.44.254). The HTTP server, at 10.1.1.10, resides in the private network.

Figure 13-8 T1 Link Using **defaultnapt**



To configure a PortMaster to direct inbound HTTP packets to an internal web server and provide outbound access to internal hosts (as illustrated in Figure 13-8), add the following commands to the PortMaster configuration:

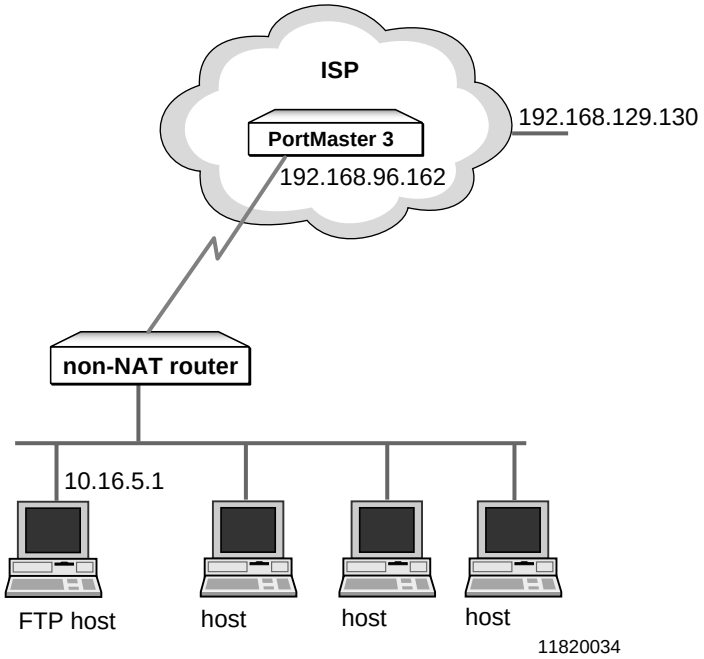
```
Command> set w24 address 192.168.44.99
Command> set w24 destination 192.168.44.254
Command> set w24 nat outmap defaultnapt
Command> add map w24.inmap
Command> set map w24.inmap 1 static-tcp-udp-portmap 192.168.44.99:http
10.1.1.10:http
Command> set w24 nat inmap w24.inmap
Command> reset w24
```

defaultnapt in Outsource Mode for a Dial-In User

This example (Figure 13-9) shows how to provide NAT service for user **tesla** connecting in an outsource mode NAPT configuration using the **defaultnapt** map on a PortMaster 3 at IP address 192.168.96.162.

The global IP address 192.168.129.130 is assigned to the dial-up router and will be used for NAT-translated packets. Because this configuration uses the **defaultnapt** map, the IP addresses in the internal client network are not important.

Figure 13-9 Dial-in User Using **defaultnapt**



To provide outsource mode NAPT service to dial-in user **tesla** as illustrated in Figure 13-9, add the following commands to the PortMaster 3 configuration:

```
Command> add netuser tesla
Command> set user tesla password ACpower
Command> set user tesla maxports 2
Command> set user tesla protocol ppp
Command> set user tesla destination 192.168.129.130
Command> set user tesla local-ip-address 192.168.96.162
Command> set user tesla nat outmap defaultnapt outsource
```

No NAT configuration is needed on the dial-up router side. If you want user **tesla** to run an FTP server (with private IP address 172.16.5.1) on his network and have it globally accessible, you must add the following additional commands to the PortMaster 3 configuration:

```
Command> add map tesla.inmap
Command> set map tesla.inmap 1 stupm 192.168.129.130:ftp 172.16.5.1:ftp
Command> set user tesla nat inmap tesla.inmap outsource
```

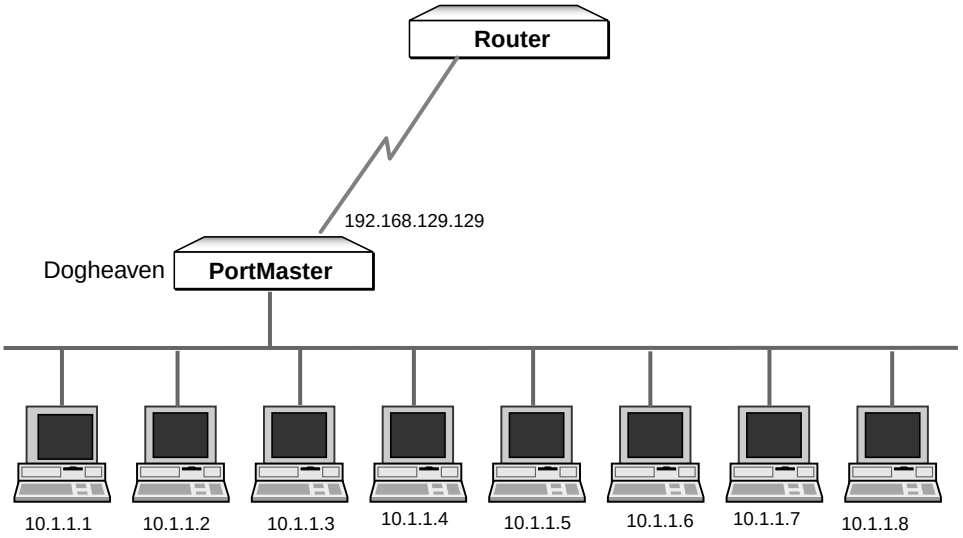
The **static-tcp-udp-portmap** keyword can be abbreviated to **stupm**.

Dial-Out Location Using a Dynamic Address Basic NAT Map

In this example, the company Dogheaven has outgrown the original address block of six IP addresses (192.168.129.128/29) it received from its ISP. The company can request more IP addresses, but they decide that the cost of additional IP addresses is not justifiable because all internal hosts on their company network do not need guaranteed access to external networks or to the Internet at all times.

Previously, the company statically mapped each internal host to a global IP address. To give the two new hosts access to a global IP address, they implement an IP address map that dynamically maps all hosts in the 10.1.1.0/24 network to the 192.168.129.128/29 address block.

Figure 13-10 Dial-Out Location Using a Dynamic Address Pool



To set up an address map that dynamically maps a group of private hosts to a smaller group of global IP addresses as illustrated in Figure 13-10, add the following commands to the PortMaster configuration:

```
Command> add map isp.outmap
Command> set map isp.outmap 1 addressmap 10.1.1.0/24 192.168.129.128/29
Command> add location isp
Command> set location isp telephone 5551234
Command> set location isp username dogheaven
Command> set location isp password k9
Command> set location isp destination negotiated
Command> set location isp maxports 2
Command> set location isp continuous
Command> set location isp local-ip-address assigned
Command> set location isp nat outmap isp.outmap
```

See "Configuring Dynamic Address Pools for Outbound NAT" on page 13-7 for more information.

Dial-Out Location Mixing Static and Dynamic Address Maps

In this example, a company Koolstuff receives the address block, 192.198.130.0/24, from its ISP. Because all workstations at Koolstuff do not need to access the Internet at the same time, Koolstuff can use a dynamic address pool. For security reasons, however, the company must give two of their trusted systems static IP addresses by adding rules to the address map.

In this configuration, trusted hosts with private addresses 10.1.1.1 and 10.1.1.2 always map to global IP addresses 192.168.130.1 and 192.168.130.2, respectively. This mapping is determined by rule 1 and rule 2 in the second and third lines of the configuration. The remaining internal hosts in the 10.1.0.0/16 network map to addresses in the address pool, 192.168.130.3-192.168.130.254, receiving any available address each time they need one.

To statically map two hosts to specific addresses and dynamically map the rest, configure the PortMaster as follows:

```
Command> add map isp.outmap
Command> set map isp.outmap 1 addressmap 10.1.1.1 192.168.130.1
Command> set map isp.outmap 2 addressmap 10.1.1.2 192.168.130.2
Command> set map isp.outmap 3 addressmap 10.1.0.0/16
192.168.130.3-192.168.130.254
Command> add location isp
Command> set location isp telephone 5558583
Command> set location isp username Koolstuff
Command> set location isp password 2cool
Command> set location isp destination negotiated
Command> set location bigcomp maxports 2
Command> set location bigcomp continuous
Command> set location bigcomp local-ip-address assigned
Command> set location bigcomp nat outmap isp.outmap
```

Network Application Compatibility

Because of the nature of the operation of NAT, some applications that work under basic NAT, might not work with NAPT. If you are using a particular application under NAPT and it is not working, try using basic NAT and see if the situation improves.

NAT-Friendly Applications

NAT-friendly applications supported include any TCP/UDP based applications that do not try to embed the IP source and/or IP destination address in their payload. Unless otherwise noted, the following applications have been tested and work for both inbound and outbound service:

- Telnet
- FTP
- TFTP
- HTTP
- Secure HTTP (HTTPS) and Secure Sockets Layer (SSL) protocol
- SMTP and **rlogin** (inbound only)
- X Windows, ping, **traceroute**, and DNS
- Secure Shell (SSH)

Unfriendly Applications

The following applications are considered NAT unfriendly either because they embed the IP source and/or destination address in the payload, are multicast or broadcast based, or rely on end-to-end node security:

- Multicast-based applications
- Routing protocols RIP and OSPF
- DNS zone transfers
- End-to-end VPN
- Any application that embeds the IP source and/or destination address(es) into the payload

Debugging and Troubleshooting NAT

When debugging and troubleshooting NAT, use the following points as guidelines:

- Verify that IP addresses are correct in map entries and that your maps match the flow of the session (inbound or outbound). Monitor the output of the **show nat sessions** command to verify that the correct translations are taking place. Make sure you entered a valid NAT map. Use **show nat mapusage** if no NAT maps are listed, in case you entered the map name incorrectly.
- Monitor the output of the **show nat statistics** command for failed translations, which can indicate incorrect session flow (direction) and possibly incomplete maps. (For more information about using the **show nat** commands, see "NAT Session Management" on page 13-28.)
- Monitor the source and destination IP addresses of packets passing through the PortMaster. (See the "Tracing Packets" section in the *PortMaster Troubleshooting Guide* for examples of simple **ptrace** debug filters.) If you are trying to run NAT on your WAN link, verify that private IP addresses are not going out the **ptp***nn* interface untranslated. If translation is not taking place, either your NAT maps are not configured correctly or NAT is not active on the port.
- You must reset an active port before a NAT configuration takes effect. On an Ethernet interface, you must globally reset the NAT subsystem. ("Resetting NAT Sessions" on page 13-28.)
- If a location is set to dial-on-demand, you must reboot the PortMaster for configuration changes to take effect. If a port loses network connectivity because, for example, the modem loses the carrier signal, NAT maintains the existing session state only if the IP address assigned to the port remains the same.

Logging Control

You can activate **syslog** and console logging on a per-port basis to help track configuration errors, and for auditing. To log to the PortMaster console all NAT sessions that fail for any reason, use the following command:

```
Command> set Ether0|S0|W1|location Locname|user Username nat log sessionfail
console
```

To log to **syslog**, substitute the **syslog** keyword for **console**.

syslog logging runs at the priority level displayed by the **show syslog** command. If you do not have a NAT **syslog** priority set, **syslog** logging does not take place.

Lucent recommends that you log NAT events at the **auth.notice** priority, the same priority as for packet filters. To set NAT logging at the recommended priority, enter the following command:

```
Command> set syslog nat auth.notice
```

You can log more selectively by appending the **log** keyword to the end of a map entry. For example, to have a **syslog** message sent to your log host whenever a session from 172.168.3.1 successfully translates (outbound) to the global IP address 192.198.247.6, enter the following command:

```
Command> set map Mapname 1 addressmap 172.16.3.1 192.168.247.6 log
```

The following example shows output from this command. The first four lines show translation errors, the remaining lines show successful translations.

```
Mar 24 17:28:11 nat-or NAT: ptp3: Out TCP (172.16.3.1:34172)->
(192.168.247.6:80) Xlation failed: Session may have prematurely timed out.

Mar 24 17:28:40 nat-or NAT: ptp3: Out TCP (172.16.3.1:34172)->
(192.168.247.6:80) Xlation failed: Session may have prematurely timed out.

Mar 24 17:28:57 nat-or NAT: ptp3: Out TCP (172.16.3.1:34177)->
(192.168.247.6:80) translated to (192.168.129.129:20001)->(192.168.247.6:80)

Mar 24 17:29:23 nat-or NAT: ptp3: Out TCP (172.16.3.1:34178)->
(192.168.247.6:80) translated to (192.168.129.129:20002)->(192.168.247.6:80)
```

Debugging NAT

NAT provides several ComOS debugging options. To turn off NAT logging, enter **set debug off** and then **reset console**.

- To view FTP payload processing, enter the following command:

  ```
  Command> set debug nat-ftp on
  ```

- To view ICMP ICMP error payload processing, enter the following command:

  ```
  Command> set debug nat-icmp-err on
  ```

- To view NAT parameter changes during interface binding, use the following command:

  ```
  Command> set debug nat-rt-interface on
  ```

- To enable full NAT debugging, use the following command.

  ```
  Command> set debug nat-max on
  ```

Network Diagnostic Tools for NAT

Because NAT includes ICMP and UDP translation, the two most common network diagnostic tools, ping and **traceroute**, can be used. However, the following restrictions apply:

- When using NAPT, **traceroute** or ping inbound is not available to the private hosts because you cannot reach these hosts directly from the outside. But any of the private hosts can use the tools in an outbound direction without any problems.
- You can use basic NAT inbound only if you have an inbound map active. The map must include an entry for the host you are trying to ping or trace a route to. As with NAPT, you can do all network diagnostics in outbound mode.

Configuring L2TP 14

This chapter describes how to set up a Layer 2 Tunneling Protocol (L2TP) tunnel between two PortMaster 3s or between a PortMaster 3 and another L2TP-compatible router.

This chapter includes the following topics:

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

Note – You must be running RADIUS 2.1 or later to configure L2TP.

Overview of L2TP

The Layer 2 Tunneling Protocol (L2TP) allows PPP frames to "tunnel" across the Internet. Tunneling is the encapsulation of one type of protocol within another protocol. In L2TP, PPP frames are encapsulated in IP/UDP packets. The ComOS implementation of L2TP currently has no built-in encryption capability.

L2TP Components

This section describes the fundamental components of L2TP and how they work together to tunnel data across the Internet.

L2TP allows PPP frames to be tunneled from a PortMaster answering dial-in calls to another PortMaster (or any L2TP-capable router) that processes the PPP frames. With L2TP, the functionality normally provided by one PortMaster is provided by two devices:

- **L2TP access concentrator** (**LAC**)—an L2TP-capable PPP access server that provides the physical connection (usually a modem or ISDN port) between the dial-in user and the outsourcer (an ISP or telephone company providing Internet service). You can configure a PortMaster 3 as a LAC.

  The primary function of a LAC is to transfer PPP frames from Layer 2 into Layer 3, and to forward those packets to a Layer 3 termination point. The LAC is responsible for setting up the tunnel with information learned from the RADIUS server. The LAC can also provide partial authentication through call-check.

- **L2TP network server** (**LNS**)—a PPP server with L2TP capabilities that is the end point of the L2TP session. The LNS terminates the L2TP tunnel and the L2TP PPP sessions. The LNS handles the actual authentication of the user (via a RADIUS server) and routes network traffic to and from the user.

  The LNS does not support dial-in/dial-out, analog, or ISDN connections. However, it can be configured for network hardwired and Ethernet connections. You can configure a PortMaster 3 as an LNS.

An outsourcer can use L2TP to provide dial-up access to a variety of clients (usually businesses or organizations) from a common physical dial-up pool. The dial-up pool resides on a shared access server (the LAC). The dial-up client maintains a home gateway (the LNS) and some type of IP connectivity to the outsourcer. IP connectivity can take place over point-to-point dedicated circuits, or over a network via Frame Relay, Asynchronous Transfer Mode (ATM), or any supported data transfer protocol.

In this configuration, L2TP provides virtual dial-up ports to the outsourcer clients. This setup is sometimes referred to as a virtual private dial-up network (VPDN). The service is transparent to client users—users still terminate PPP sessions on the client's network via the LNS, and clients do their own RADIUS authentication, accounting, and IP address assignment.

Locally stored profiles are not supported for L2TP. You must use RADIUS 2.1; in fact, most of the L2TP setup involves RADIUS configuration. See "Configuring L2TP on the RADIUS Server" on page 14-8 for more information.

Note – L2TP is not supported on the PortMaster 2, PortMaster 25, PortMaster IRX, or PortMaster Office Router platforms.

How L2TP Works

Basic L2TP service operates as follows. The LAC accepts a call and establishes a tunnel to the LNS for that PPP session. The LAC just accepts the call; it does not process PPP packets. If call-check is used, authentication can be done on the LAC; otherwise authentication takes place on the LNS, which terminates the call.

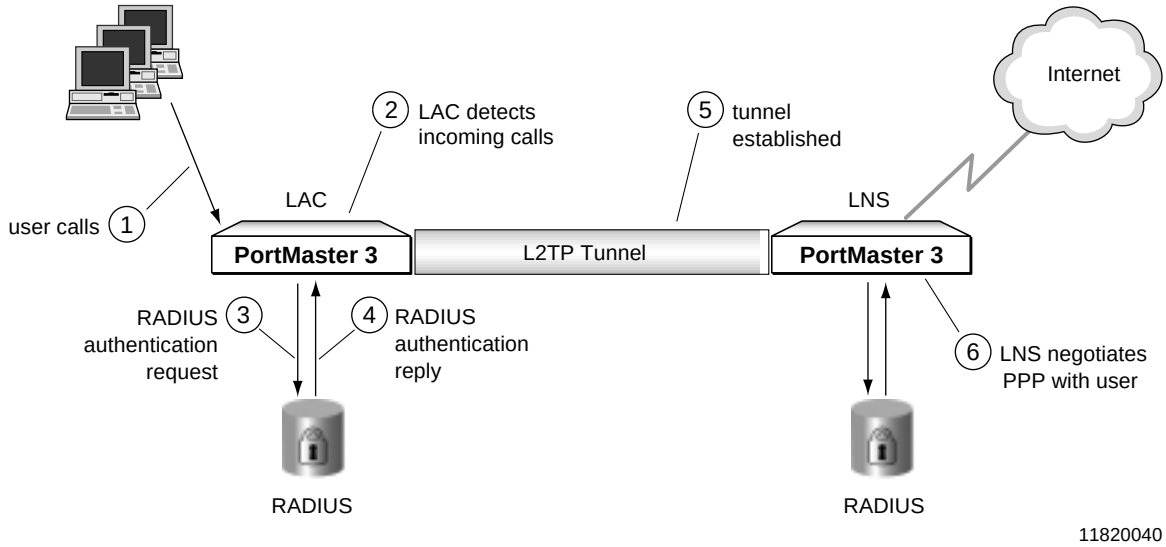
The tunnel can be established based upon the RADIUS check item Called-Station-Id or on the value of the User-Name attribute. If the call is based upon User-Name, partial authentication occurs on the LAC before the tunnel is established.

A session using Call-Check as a Service-Type and Called-Station-Id as a check item with L2TP proceeds as follows:

1. The dial-up user places a call.
2. The LAC detects the incoming call.
3. Using call-check, the LAC sends an authentication request to a RADIUS server containing the Called-Station-Id and Calling-Station-Id before answering the call. (See "Overview of Call-Check" on page 14-7.)
4. RADIUS accepts the user (if authentic) and sends an accept message to the LAC containing information about how to create the L2TP tunnel for this session.
5. The LAC creates a tunnel to the LNS by encapsulating the PPP frames into IP packets and forwarding those packets to the LNS.
6. The LNS negotiates PPP with the end user.

Figure 14-1 illustrates the basic operation of L2TP tunneling. Tunnel authentication can be set to either end of the tunnel, or to both ends for mutual authentication. See "Setting L2TP Tunnel Authentication (Optional)" on page 14-6.

Figure 14-1 L2TP Tunnel Operation



Configuring L2TP on the PortMaster 3

This section describes how to configure the PortMaster portion of an L2TP configuration. Because locally stored profiles are not supported for L2TP, you must use RADIUS. For information about configuring the RADIUS portion of L2TP, see "Configuring L2TP on the RADIUS Server" on page 14-8.

You use the following command to configure L2TP on a PortMaster 3:

```
Command> set l2tp disable|enable lac|lns
```

Setting Up a LAC

You designate a PortMaster 3 as a LAC by enabling the LAC feature in ComOS. The LAC feature is disabled by default. To designate a PortMaster 3 as a LAC, enter the following command:

```
Command> set l2tp enable lac
Command> save all
Command> reboot
```

To disable the LAC functionality on the PortMaster, enter the following commands:

```
Command> set l2tp lac disable
Command> save all
Command> reboot
```

Setting Up an LNS

The LNS feature is disabled by default. You designate a PortMaster 3 as the end point of an L2TP tunnel by enabling the LNS feature in ComOS. The PortMaster thereafter supports in-band channelized connections only. To designate a PortMaster 3 as an LNS, enter the following command:

```
Command> set l2tp enable lns
Command> save all
Command> reboot
```

To disable the LAC functionality on the PortMaster, enter the following command:

```
Command> set l2tp lns disable
Command> save all
Command> reboot
```

Refer to the *PortMaster Command Line Reference* for more details about L2TP commands.

Load Balancing among Tunnel Server End Points (Optional)

When you configure redundant tunnel server end points on the RADIUS server (see "Configuring Redundant Tunnel Server End Points" on page 14-11), the PortMaster selects tunnel end points serially, always beginning with the first.

To set the PortMaster to choose tunnel end points randomly, use the following commands:

```
Command> set l2tp choose-random-tunnel-endpoint on|off
Command> reset l2tp
Command> save all
```

Setting L2TP Tunnel Authentication (Optional)

You authenticate L2TP users by setting a password in the RADIUS user profile (see "Configuring a Shared Secret" on page 14-10). The user's session is then authenticated by the RADIUS server.

You can also authenticate the tunnel. You can set tunnel authentication in RADIUS, or you can set it on the LAC, the LNS, or both. If you want the RADIUS server to authenticate the tunnel, you must set a tunnel password in RADIUS (see "Configuring a Shared Secret" on page 14-10). RADIUS tunnel authentication takes priority over authentication by either the LAC or the LNS. If tunnel authentication is set on the LAC and/or the LNS **and** on the RADIUS server, the RADIUS server authenticates the tunnel.

To set tunnel authentication on the LAC or the LNS, you must first set an L2TP password locally on the PortMaster. To set a password on the PortMaster, use the following command:

```
Command> set l2tp secret Password|none
```

Use the **none** keyword to disable the password. This is the default.

After you set the L2TP password, use the following command to set remote tunnel authentication:

```
Command> set l2tp authenticate-remote on|off
```

Enter the **reset l2tp** command to make your changes take effect, then enter the **save all** command so the changes remain in effect after you reboot the PortMaster.

If you set remote authentication on the LAC, the LAC initiates authentication and the LNS authenticates. If you set remote authentication on the LNS, the LNS initiates authentication and the LAC authenticates. If you set tunnel authentication on both the LAC and the LNS, the LAC and the LNS authenticate each other.

If no tunnel exists, a tunnel is established for the first L2TP session, and tunnel authentication takes place before the session terminates.

Note – Because tunnels remain established until the PortMaster is rebooted, empty tunnels can exist.

Overview of Call-Check

The call-check feature allows an outsourcer (ISP or telephone company providing Internet service) to get the calling number of a dial-in user without accepting the call. A typical application for call-check is to hang up on a user attempting to dial in and then to call the user back, with no charge incurred for the initial call. Call-check can also be used to limit the number of active calls on a given number.

The call-check feature supports virtual points of presence (POPs) by allowing for redirection of calls. For example, you can set up two telephone numbers, one that is accepted and one that is redirected. If a customer calls the first number, the customer is authenticated normally; if a customer calls the second number, the call is accepted but forwarded through an L2TP session to an LNS for complete authentication of the user.

Call-check is available for the PortMaster 3 in ComOS 3.9 and later.

Enabling Call-Check on a PortMaster

The call-check feature is off by default. To enable or disable the call-check feature, use the following command:

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

How Call-Check Works

When call-check is enabled, the PortMaster sends a RADIUS access-request message for all incoming calls before accepting calls containing the Calling-Station-Id and Caller-Station-Id check items. The PortMaster expects to receive one of the following replies from the RADIUS server:

- RADIUS access-accept message with attributes, to accept the call and provide the indicated service—such as connecting the user via an L2TP session to a given LNS
- RADIUS access-accept message with no attributes to accept the call and perform the usual RADIUS authentication
- RADIUS access-reject message to reject the call

When you enable call-check, the **show global** command displays the words *call-check Enable* immediately after the ISDN switch type.

Note – If the call-check feature is enabled but no RADIUS support is configured, all dial-in users receive either a busy signal or dead air.

To use the call-check feature, you must modify the RADIUS dictionary on the RADIUS server. See "Configuring L2TP on the RADIUS Server" on page 14-8 for details.

Configuring L2TP on the RADIUS Server

This section describes how to configure the RADIUS portion of L2TP. "Configuring L2TP on the PortMaster 3" on page 14-4 describes the PortMaster portion of the configuration.

Note – You must be running RADIUS 2.1 or later to configure L2TP.

To define the tunnel configuration for L2TP, you must add some new attributes to the RADIUS dictionary and use them to configure user profiles. This section describes entries you make on the RADIUS server to support L2TP and includes the following topics:

- "Configuring Call-Check" on page 14-9
- "Configuring User Profiles" on page 14-9
- "Configuring Accounting" on page 14-11

For more information about RADIUS 2.1, see the *RADIUS for UNIX Administrator's Guide*.

You can use entirely separate RADIUS servers for the LAC and the LNS, or use the same one. The difference between a LAC and an LNS is that they authenticate at different stages in the tunneling process. Authentication is based on either a Called-Station-Id check item, a Calling-Station-Id check item, or both—information currently available only for ISDN PRI.

Configuring Call-Check

To use the call-check feature, you must add the following entries to the dictionary on the RADIUS server and then restart RADIUS so that it reads the new dictionary:

```
VALUE           Service-Type              Call-Check      10
VALUE           NAS-Port-Type             Virtual         5
ATTRIBUTE       Tunnel-Type               64              integer
ATTRIBUTE       Tunnel-Medium-Type        65              integer
ATTRIBUTE       Tunnel-Server-Endpoint    67              string
ATTRIBUTE       Tunnel-Password           69              string
VALUE           Tunnel-Type               L2TP            3
VALUE           Tunnel-Medium-Type        IP              1
```

Caution – The call-check Service-Type name and value have changed since ComOS 3.8b15, which used the name Call-Check-User and the value 129. This name and value are no longer valid. Make sure to remove any old entries in your dictionary and users file.

Configuring User Profiles

RADIUS user profiles on the LNS are the same as non-L2TP user profiles. On the LAC, however, some new user profiles are required. Exactly which additional user profiles you decide to add depends upon whether you use call-check or partial username-based tunneling on the LAC. The profiles in this section can be used on the RADIUS server serving the LAC for call-check or partial username-based tunneling.

The following sample user profile uses RADIUS check items Called-Station-Id and Call-Check to route callers that dial 555-1313 to the LNS at IP address 192.168.1.221:

```
DEFAULT Called-Station-Id = "5551313", Service-Type = Call-Check
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Tunnel-Type = L2TP,
          Tunnel-Medium-Type = IP,
          Tunnel-Server-Endpoint = "192.168.1.221"
```

Configuring a Shared Secret

The sample user profile in this section is the same as the profile in the previous section except that it uses a shared secret to authenticate the tunnel to the LNS.

```
DEFAULT Called-Station-Id = "5551313", Service-Type = Call-Check
        Service-Type = Framed-User,
        Framed-Protocol = PPP,
        Tunnel-Type = L2TP,
        Tunnel-Medium-Type = IP,
        Tunnel-Password = "mysecret",
        Tunnel-Server-Endpoint = "192.168.1.221"
```

In both sample user profiles, the first item is the RADIUS check item, the Called-Station-ID, which is used to match the entry before the call is answered. The L2TP parameters are pulled from matching entries.

The Tunnel-Type specifies the tunneling protocol. The Tunnel-Medium-Type, IP in these examples, specifies the transport medium over which the tunnel is created. Tunnel-Server-Endpoint indicates the other end of the tunnel, the LNS when L2TP is being used.

Configuring Partial Authentication on the LAC

If you do not use call-check but provider partial authentication based on the username, you can use the following user profile. In this sample, user *sara* dials into the LAC, which initiates an L2TP tunnel on the user's behalf to an LNS at IP address 192.168.1.55.

```
        sara Password = "apassword"
        Tunnel-Type = L2TP,
        Tunnel-Medium-Type = IP,
        Tunnel-Server-Endpoint = "192.168.1.55"
```

Configuring Redundant Tunnel Server End Points

To ensure continuous L2TP service in the event that the LNS fails, you can configure user profiles to contain redundant tunnel server end points. In this way, if the primary LNS goes down, inbound L2TP tunnels are redirected to alternative LNSs. You can configure up to three redundant tunnel server end points in a user profile.

The following sample RADIUS user profile uses redundant tunnel server end points. Each tunnel server end point is preceded by the Tunnel-Medium-Type for that tunnel.

```
DEFAULT Service-Type = Call-Check, Called-Station-Id = "5551234"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Tunnel-Type=L2TP,
          Tunnel-Medium-Type = IP,
          Tunnel-Server-Endpoint = "192.168.11.2",
          Tunnel-Medium-Type=IP,
          Tunnel-Server-Endpoint = "192.168.11.17",
          Tunnel-Medium-Type=IP,
          Tunnel-Server-Endpoint = "192.168.230.97"
```

Acceptance of a tunnel server end point is based on whether the host is running L2TP. However, if the machine designated as the tunnel server end point is configured as a LAC instead of an LNS, the session fails.

Note – This feature provides redundant backup, not load balancing. See "Load Balancing among Tunnel Server End Points (Optional)" on page 14-5.

Configuring Accounting

Both the LAC and the LNS can log user sessions to RADIUS accounting, but the data available to each depends upon whether you use call-check or partial authentication on the LNS.

- **Call-Check**—If you use call-check to establish the tunnel, the LAC accounting data includes only the calling line ID (CLID) information. The username is not present because that information has not yet been passed over the link. The LNS has both the CLID and username in its accounting data, along with the assigned IP address.
- **Partial Authentication**—If partial authentication instead of call-check is taking place on the LAC, the username might be available. If the username is available, it appears in the RADIUS accounting logs for both the LNS and the LAC.

In both cases, the LNS shows the NAS-Port-Type as **virtual**. In addition, the LAC has the NAS-Port-Type set to the connection type of the physical interfaces, which is the normal behavior of a network access server (NAS).

Administering L2TP on the PortMaster

This section describes administrative tasks you can perform to monitor or change L2TP settings on the PortMaster, and includes the following topics:

Manually Creating a Tunnel

To aid in troubleshooting and testing an L2TP tunnel configuration, you can manually bring up an L2TP tunnel with the following command:

```
Command> create l2tp tunnel udp Ipaddress [Password|none]
```

The *Ipaddress* is the end point of the L2TP tunnel. The password is optional; the default is **none**. If you specify a password, the PortMaster uses it when responding to a tunnel authentication request from the peer. If you do not specify a password, the PortMaster uses the L2TP secret if configured (see "Setting L2TP Tunnel Authentication (Optional)" on page 14-6). If no L2TP secret is configured, no authentication takes place.

For example, to create a tunnel to an L2TP-compatible device at IP address 192.168.10.19, enter the following command:

```
Command> create l2tp tunnel udp 192.168.10.19
```

Displaying L2TP Information

Use the following command to display information about the current L2TP operation:

```
Command> show l2tp global|sessions|stats|tunnels
```

You can see whether the PortMaster is configured to be an LNS or a LAC, monitor states of tunnel sessions, and view various internal statistics.

Resetting L2TP Tunnels

Use the following command to reset counters displayed by the **show l2tp stats** command, or to reset a particular tunnel. Tunnel numbers are displayed by the **show l2tp tunnels** command.

```
Command> reset l2tp [stats|tunnel Number]
```

When you specify the optional **stats** keyword, only the statistics are reset. Entering this command with no keyword closes all open PPP sessions and resets all L2TP tunnels.

Troubleshooting L2TP

Use the following command to display L2TP information.

```
Command> set debug l2tp max|packets [Bytes]|setup|stats on|off
```

PPP Tracing

Use the **set debug 0x51** command for PPP tracing on the LNS. If you are not using the call-check feature, this command also works normally on the LAC.

Modem Connections

You can view the Tx (transmit) speed of the connection on both the LAC and LNS and extended connection information, such as Rx (receive) speed, retrained (changed) speeds, and any changes due to modem renegotiations on the LAC only.

To view the connect speed on the LNS and display the speed and other information about the LAC, use the following command:

```
Command> show modems
```

Accounting for Firewalls between a LAC and an LNS

L2TP operates entirely over the User Datagram Protocol (UDP) on destination port 1701. The source port is determined by the PortMaster and is based on available ports with values greater than 1024. Keep this in mind when defining filter rules if you have a firewall between your LAC and LNS.

Using Frame Relay 15

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:

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 end point. 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 a 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

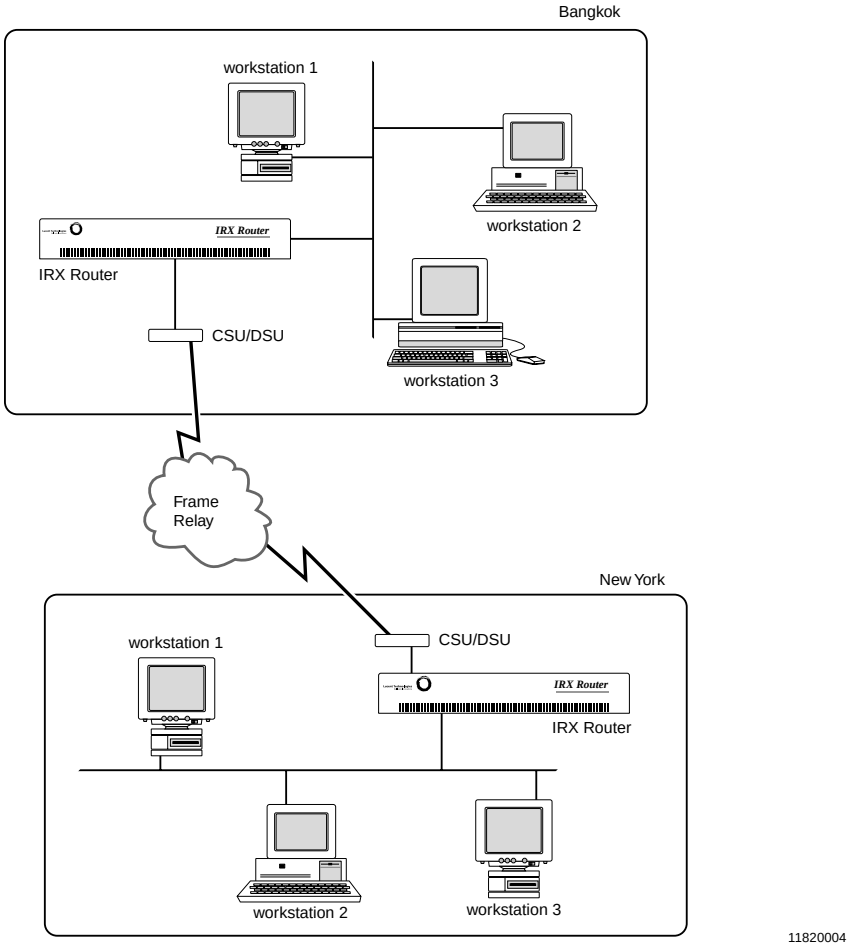
You configure Frame Relay by selecting the Frame Relay protocol, setting the IP address of the port, and specifying the DLCIs during the synchronous port configuration.

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 15-1 shows an example of a Frame Relay connection.

Note – All synchronous ports require an external clock signal to regulate the port speed.

Figure 15-1 Frame Relay Configuration



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 dlcilist Dlci_list
```

For information on Frame Relay subinterfaces see “Frame Relay Subinterfaces” on page 15-12.

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 15-8).
   b. Configure Ethernet interface settings (page 15-8).
   c. Configure synchronous port settings (page 15-9).
2. **Configure the following settings for the PortMaster in New York:**
   a. Configure Ethernet interface settings (page 15-10).
   b. Configure synchronous port settings (page 15-10).
3. **Troubleshoot the configuration (page 15-11).**

You can additionally configure Frame Relay subinterfaces. For information on Frame Relay subinterfaces see “Frame Relay Subinterfaces” on page 15-12.

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 15-1.

Table 15-1 Global Values

Parameter	Command
Gateway	**set gateway** *192.168.20.2*

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 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 15-2.

Table 15-2 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 15-2, 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 15-3.

Table 15-3 Synchronous WAN Port Values

Setting	Command
Port type	**set** *w1* **network** *hardwired*
Protocol	**set** *w1* **protocol** *frame*
Port IP address	**set** *w1* **address** *192.168.20.1*
Netmask	**set** *w1* **netmask** *255.255.255.0*
Modem control	**set** *w1* **cd on**
RIP routing	**set** *w1* **rip** *broadcast*
Annex-D	**set** *w1* **annex-d** *10*
	(LMI can be used instead of Annex-D.)
DLCI	**add dlci** *w1 16:192.168.20.2*
	(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 15-3, 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 15-4.

Table 15-4 Ethernet Values

Setting	Command
IP address	**set** *ether0* **address** *192.168.1.1*
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 15-4, 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 15-5.

Table 15-5 WAN Port Parameter Values

Setting	Command
Port type	**set** *w1* **network** *hardwired*
Protocol	**set** *w1* **protocol** *frame*
Port IP address	**set** *w1* **address** *192.168.*20.2
Netmask	**set** *w1* **netmask** *255.255.255.0*
Modem control	**set** *w1* **cd on**
RIP routing	**set** *w1* **rip** *listen*
Annex-D	**set** *w1* **annex-d** *10*
	(LMI can be used instead of Annex-D)

Table 15-5 WAN Port Parameter Values *(Continued)*

Setting	Command
DLCI	**add dlci** *w1 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 15-5, 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 W1 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 w1
  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 Relay 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_relay
Command> set location sub1 group 1
Command> set w1 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 w1
  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 W1 with DLCIs 16, 17, and 18. Port W1 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 w1 group 1

Command> add location sub1
Command> set location sub1 protocol frame_relay
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 ipdlci sub1 16
Command> add ipdlci sub1 17

Command> save all
Command> reset w1
```

Using Synchronous V.25bis Connections 16

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:

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.

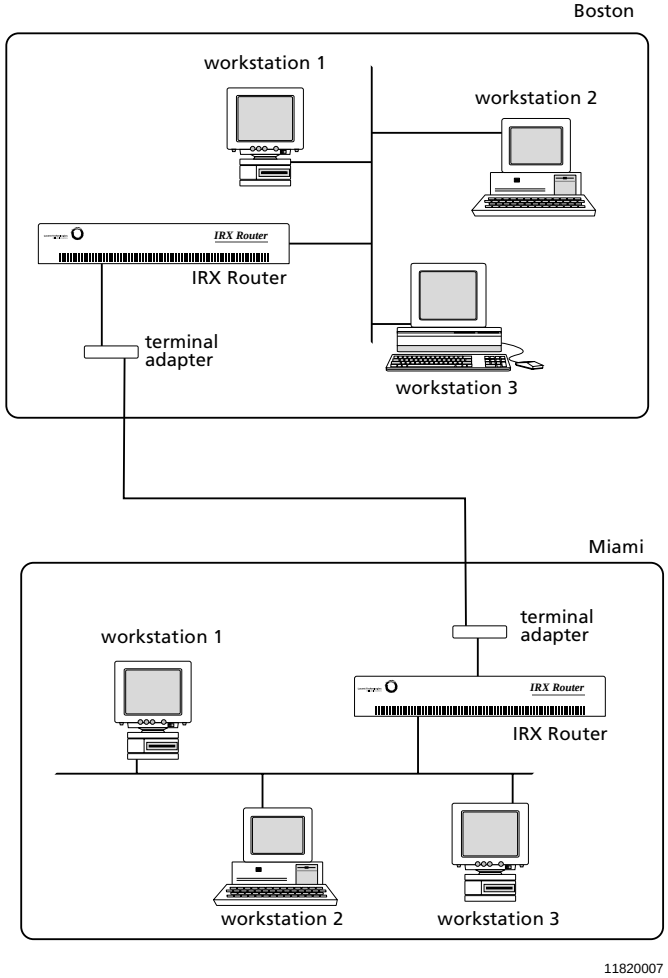
When connecting an asynchronous ISDN terminal adapter to an asynchronous port using AT commands to dial, configure the PortMaster just as you would for a modem. Refer to Chapter 17, "Using Office-to-Office Connections," and Chapter 18, "Using Internet Connections," for more information.

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 16-1 shows an example of an ISDN or switched 56Kbps connection.

Figure 16-1 Example of an ISDN or Switched 56Kbps Connection



11820007

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 16-4)
   b. Ethernet interface settings (page 16-4)
   c. Synchronous port settings (page 16-5)
   d. Dial-in users (page 16-5)
   e. Dial-out locations (page 16-6)
2. **Configure the following settings for the PortMaster in Miami:**
   a. Global settings (page 16-8)
   b. Ethernet interface settings (page 16-8)
   c. Synchronous port settings (page 16-9)
   d. Dial-in users (page 16-10)
   e. Dial-out locations (page 16-11)
3. **Test the configuration (page 16-12).**
4. **Troubleshoot the configuration (page 16-13).**

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 16-1.

Table 16-1 Global Values

Setting	Command
IP gateway	**set gateway** *192.168.1.1*
System name	**set sysname** *boston*

After you configure the global settings shown in Table 16-1, 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 16-2.

Table 16-2 Ethernet Values

Setting	Command
Protocol	**set ether0 ipx enabled**
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 16-2, 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 16-3.

Table 16-3 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 16-3, 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* must be configured on the PortMaster router in Boston with the values shown in Table 16-4.

Table 16-4 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 16-4 User Table Values *(Continued)*

Setting	Command
IPX network	**set user** *miami* **ipxnet** *F3*
RIP routing	**set user** *miami* **rip on**
MTU	**set user** *miami* **mtu** *1500*

After you configure user table settings as shown in Table 16-4, 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 16-5.

Table 16-5 Location Table Values

Setting	Command
Location name	**add location** *miami*
Type	**set location** *miami* **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** *miami* **protocol ppp**
IP destination	**set location** *miami* **destination** *192.168.1.1*
Netmask	**set location** *miami* **netmask** *255.255.255.0*
IPX network	**set location** *miami* **ipxnet** *F3*
RIP routing	**set location** *miami* **rip on**
MTU	**set location** *miami* **mtu** *1500*

Table 16-5 Location Table Values *(Continued)*

Setting	Command
Idle timer	**set location** *miami* **idletime** *5*
Dial group	**set location** *miami* **group** *1*
Username	**set location** *miami* **username** *miami*
Telephone number	**set location** *miami* **telephone** *5551212*
Password	**set location** *miami* **password** *anypasswd*
High-water mark	**set location** *miami* **high_water** *0*
Maximum ports	**set location** *miami* **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 16-5, 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 16-6.

Table 16-6 Global Value

Setting	Command
IP gateway	**set gateway** *192.168.1.2* (This is the address of the next upstream router.)
Default routing	**set default on**
System name	**set sysname** *miami*

After you configure the global settings shown in Table 16-6, 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 16-7.

Table 16-7 Ethernet Values

Setting	Command
Protocol	**set ether0 ipx enabled**
IP address	**set** *ether0* **address** *192.168.1.1*
Netmask	**set** *ether0* **netmask** *255.255.255.0*
IPX network	**set** *ether0* **ipxnet** *F2*
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 16-7, 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 16-8.

Table 16-8 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 16-8, 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* must be configured on the PortMaster in Miami with the values shown in Table 16-9.

Table 16-9 User Table Values for *Miami*

Setting	Command
Username	**add netuser** *boston*
Password	**set user** *boston* **password** *anypasswd*
Protocol	**set user** *boston* **protocol ppp**
User IP address	**set user** *boston* **destination** *192.168.200.1*
Netmask	**set user** *boston* **netmask** *255.255.255.0*
IPX network	**set user** *boston* **ipxnet** *F3*
RIP routing	**set user** *boston* **rip on**
MTU	**set user** *boston* **mtu** *1500*

No compression is used on synchronous lines.

After you configure user table settings as shown in Table 16-9, 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 16-10.

Table 16-10 Location Table Values

Parameter	Command
Location name	**add location** *boston*
Type	**set location** *boston* **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** *boston* **protocol ppp**
IP destination	**set location** *boston* **destination** *192.168.200.1*
Netmask	**set location** *boston* **netmask** *255.255.255.0*
IPX network	**set location** *boston* **ipxnet** *F3*
RIP routing	**set location** *boston* **rip on**
MTU	**set location** *boston* **mtu** *1500*
Idle timer	**set location** *boston* **idletime** *5*
Dial group	**set location** *boston* **group** *1*
Username	**set location** *boston* **username** *boston*
Telephone number	**set location** *boston* **telephone** *5551212*
Password	**set location** *boston* **password** *anypasswd*

Testing the Configuration

The configuration must 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 PortMaster 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 are 0 except for a small number of abnormal termination errors resulting from plugging and unplugging cables. 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 signal to the PortMaster. The CSU/DSU or terminal adapter can generate the clock signal 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.

Using Office-to-Office Connections 17

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:

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

Overview of Example Configuration

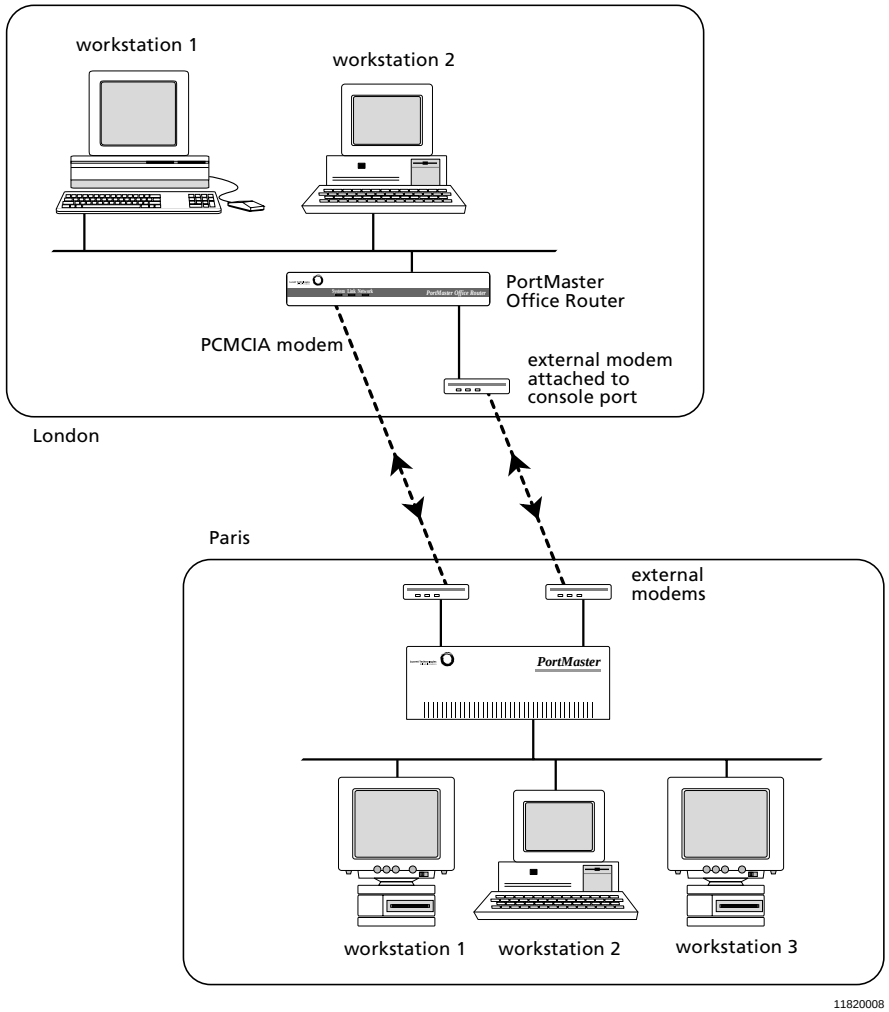
The example described in this chapter connects a PortMaster Office Router located in a branch office in London with a PortMaster 2 in the headquarters in Paris. These models are used as an example; you can use any PortMaster for this configuration.

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 17-1 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 17-1 Office-to-Office Dial-On-Demand Configuration



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 17-15.

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 examples in this chapter show variables in *italics*. 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 17-4).
   b. Ethernet interface settings (page 17-4).
   c. PCMCIA serial port settings (page 17-5).
   d. Dial-in users (page 17-6).
   e. Dial-out locations (page 17-7).
2. **Configure the following settings for the PortMaster 2 in the Paris office:**
   a. Ethernet interface settings (page 17-8).
   b. Dial-out port settings (page 17-9).
   c. Dial-in users (page 17-10).
   d. Dial-out locations (page 17-11).
3. **Test the configuration (page 17-12).**
4. **If necessary, configure the console port for multiline load balancing (page 17-13).**

Alternatively, you can configure a PortMaster Office Router for ISDN dial-on-demand connections. See page 17-15 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 17-1. The values shown in the table only apply to this example. When you are configuring your PortMaster, use values appropriate for your network.

Table 17-1 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 17-1, 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 17-2.

Table 17-2 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 17-2 Ethernet Values *(Continued)*

Setting	Command
Broadcast address	**set** *ether0* **broadcast high**

After you configure the Ethernet interface as shown in Table 17-2, 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 17-3. You must install the PCMCIA modem to configure port S1.

Table 17-3 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 idletime** *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 17-3, 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 9, "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* must be configured with the values shown in Table 17-4.

Table 17-4 User Table Values

Setting	Command
Username	**add netuser** *paris*
Password	**set user** *paris* **password** *anypasswd*
Protocol	**set user** *paris* **protocol ppp**
User IP address	**set user** *paris* **destination** *192.168.1.1*
Netmask	**set user** *paris* **netmask** *255.255.255.0*
IPX network number	**set user** *paris* **ipxnet** *F2*
RIP routing	**set user** *paris* **rip on**
MTU	**set user** *paris* **mtu** *1500*
Compression	**set user** *paris* **compression on**

After you configure the user table as shown in Table 17-4, 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* must be configured with the values shown in Table 17-5.

Table 17-5 Location Table Values

Setting	Command
Location name	**add location** *paris*
Type	**set location** *paris* **manual**
Protocol	**set location** *paris* **protocol ppp**
IP destination	**set location** *paris* **destination** *192.168.1.1*
Netmask	**set location** *paris* **netmask** *255.255.255.0*
IPX network	**set location** *paris* **ipxnet** *F2*
RIP routing	**set location** *paris* **rip on**
MTU	**set location** *paris* **mtu** *1500*
Compression	**set location** *paris* **compression on**
Idle timer	**set location** *paris* **idletime** *5*
High-water mark	**set location** *paris* **high_water** *0*
Dial group	**set location** *paris* **group** *1*
Telephone	**set location** *paris* **telephone** *5551212*
Username	**set location** *paris* **username** *London*
Password	**set location** *paris* **password** *anypasswd*
Maximum ports	**set location** *paris* **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 17-5, 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 2 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 17-6.

Table 17-6 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 17-6, 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 2 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 17-7.

Table 17-7 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 idletime 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 17-7, 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 2 in Paris so the Office Router in the London can dial in when traffic is queued. The new user **london** must be configured with the values shown in Table 17-8.

Table 17-8 User Table Values

Setting	Command
Username	**add netuser** *london*
Password	**set user** *london* **password** *anypasswd*
Protocol	**set user** *london* **protocol ppp**
User IP address	**set user** *london* **destination** *192.168.200.1*
Netmask	**set user** *london* **netmask** *255.255.255.0*
IPX network	**set user** *london* **ipxnet** *F2* (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** *london* **rip on**
MTU	**set user** *london* **mtu** *1500*
Compression	**set user** *london* **compression on**

After you configure the user table as shown in Table 17-8, 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 2 in Paris for the London office. This entry allows the PortMaster in Paris to call the Office Router in the London office when network traffic is queued. Configure a new location *london* with the values shown in Table 17-9.

Table 17-9 Location Table Values

Setting	Command
Location name	**add location** *london*
Type	**set location** *london* **manual**
Protocol	**set location** *london* **protocol ppp**
IP destination	**set location** *london* **destination** *192.168.200.1*
Netmask	**set location** *london* **netmask** *255.255.255.0*
IPX network	**set location** *london* **ipxnet** *F2* (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** *london* **rip on**
MTU	**set location** *london* **mtu** *1500*
Compression	**set location** *london* **compression on**
Idle timer	**set location** *london* **idletime** *5*
High-water mark	**set location** *london* **high_water** *0*
Dial group	**set location** *london* **group** *0*
Telephone number	**set location** *london* **telephone** *5551212*
Username	**set location** *london* **username** *paris*
Password	**set location** *london* **password** *anything*
Maximum ports	**set location** *london* **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 17-9, 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 must 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 PortMaster 2 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
   ```

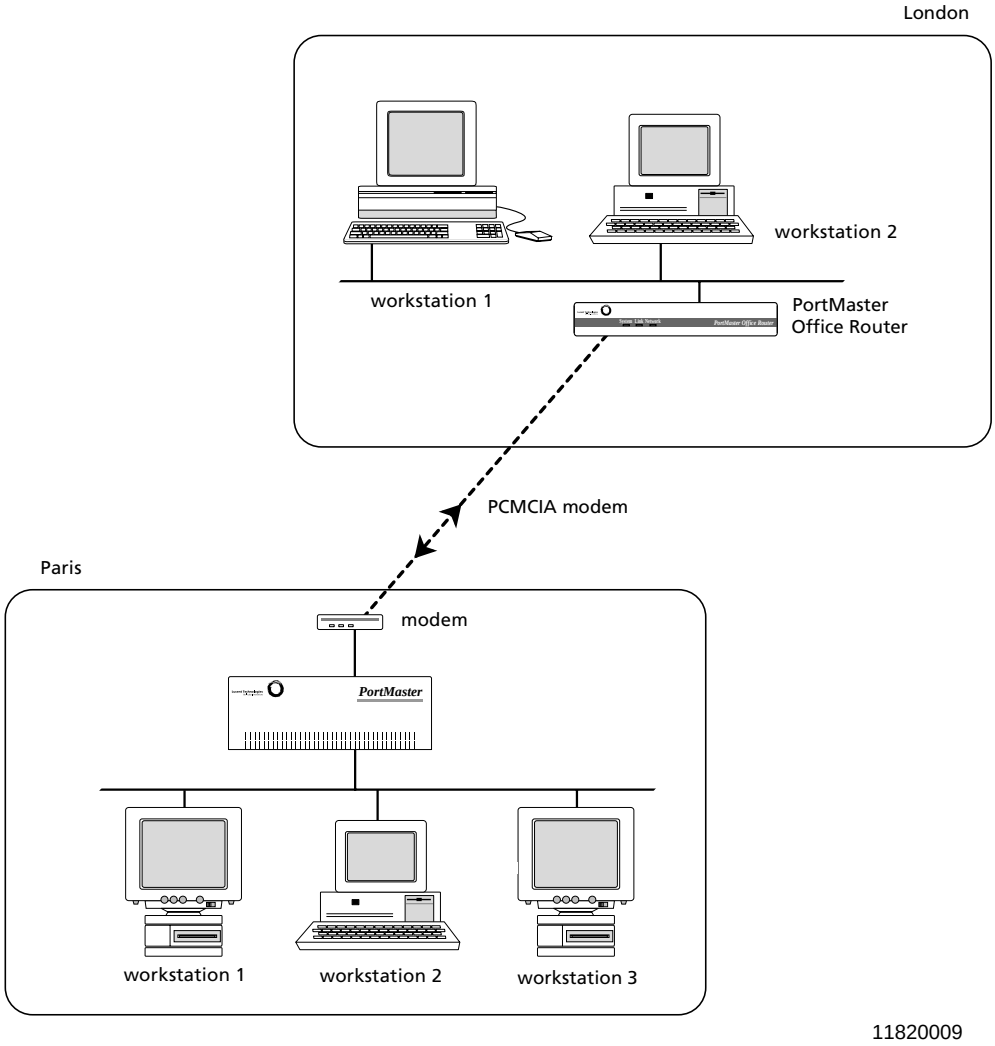
4. **If you notice a problem, do the following:**
   a. Reset the port on the PortMaster 2 in the Paris office.
   b. Change the settings you think are causing the problem.
   c. Dial the London office again.
   d. Repeat this procedure until the connection is made correctly.
5. **Repeat Steps 1 through 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 17-2 shows the multiline load balancing configuration.

Figure 17-2 Multiline Load Balancing



To enable multiline load balancing, you must configure the S0 port using the same settings shown for the PCMCIA port in Table 17-3. In addition, when you configure the location *paris* on the Office Router in the London office, use the values shown in Table 17-10 for the maximum number of ports and the high-water mark. See "Dial-Out Location Settings for London" on page 17-7 for the other values.

Table 17-10 Location Settings for Load Balancing

Setting	Command
Maximum ports	**set location** *paris* **maxports** *2*
High-water mark	**set location** *paris* **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 username with the **set location username** command.
- Set the password with the **set location password** command.

For more information about ISDN connections, see Chapter 10, "Using ISDN BRI." For information about locations, see Chapter 8, "Configuring Dial-Out Connections."

Using Internet Connections 18

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.

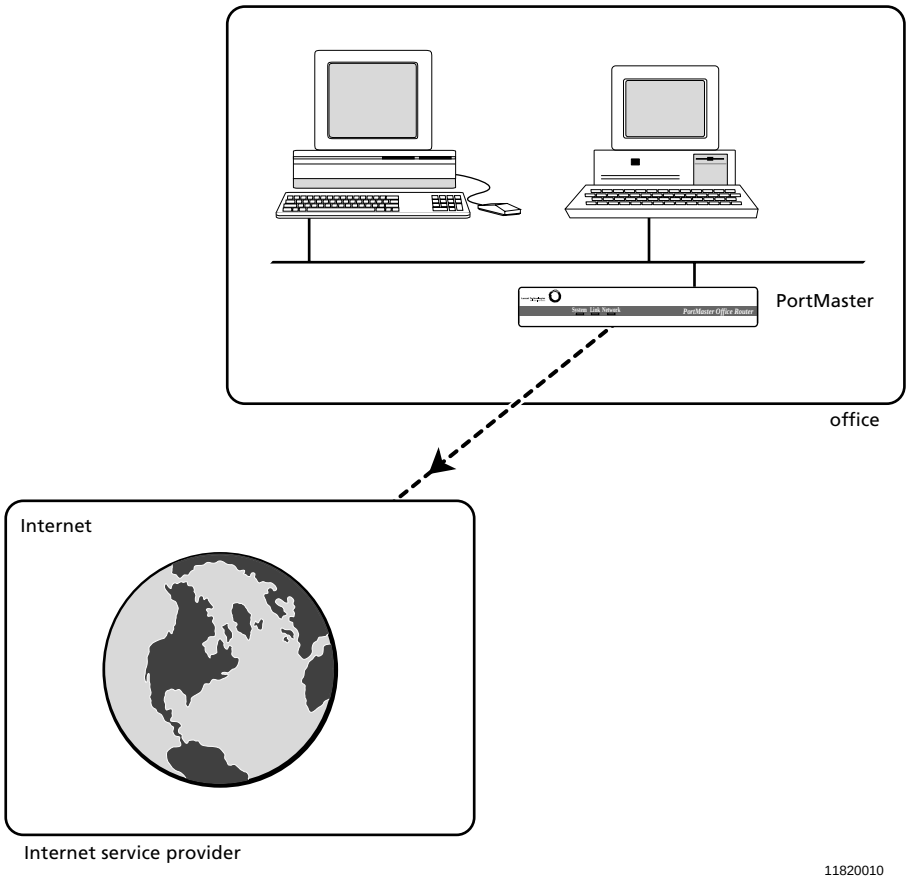
The following topics are discussed:

For information on related topics, refer to the following chapters:

Topic	**Chapter**
On-demand connections	Chapter 8, "Configuring Dial-Out Connections"
	Chapter 17, "Using Office-to-Office Connections"
Configuring a PortMaster for an ISDN connection	Chapter 11, "Configuring the PortMaster 3"
	Chapter 10, "Using ISDN BRI"
Frame Relay connections	Chapter 15, "Using Frame Relay
Synchronous leased lines	Chapter 21, "Using Synchronous Leased Lines

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

Figure 18-1 Continuous Internet Connection



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 17, "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 18-4).

   b. Ethernet interface settings (page 18-4).

c. Serial port settings (page 18-5 or page 18-6).

d. Dial-out location (page 18-7).

2. **Test the configuration (page 18-8 or page 18-9).**

3. **Set network filtering (page 18-10).**

Alternatively, you can configure a PortMaster with an ISDN port for an Internet connection. See "Using ISDN for Internet Connections" on page 18-11.

Configuring Global Settings

Configure the global settings to the values shown in Table 18-1.

Table 18-1 Global Settings Value

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 18-2.

Table 18-2 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 18-3.

Table 18-3 Serial Port Values for Continuous Dial-Out

Setting	Command
Port type	**set** *s1* **network dialout**
Protocol	**set** *s1* **protocol ppp**
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**
Dial group	**set** *s1* **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 configuring asynchronous ports, refer to Chapter 5, "Configuring an Asynchronous Port." Refer also to Chapter 9, "Using Modems."

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 18-4.

Table 18-4 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* must be configured with the values shown in Table 18-5, or as instructed by your ISP.

Table 18-5 Location Table Values

Setting	Command
Location name	**add location** *isp1*
Type	**set location** *isp1* **manual**
	(Change to **continuous** after testing the configuration.)
Protocol	**set location** *isp1* **protocol ppp**
IP destination	**set location** *isp1* **destination** *192.168.5.6*
Netmask	**set location** *isp1* **netmask** *255.255.255.0*
RIP routing	**set location** *isp1* **rip broadcast**
MTU	**set location** *isp1* **mtu** *1500*
Compression	**set location** *isp1* **compression on**
Input filter	**set location** *isp1* **ifilter** *internet.in*
Output filter	**set location** *isp1* **ofilter** *internet.out*
Idle timer	**set location** *isp1* **idletime** *0*
High-water mark	**set location** *isp1* **high_water** *0*
Dial group	**set location** *isp1* **group** *1*
Telephone number	**set location** *isp1* **telephone** *5551212*
Username	**set location** *isp1* **username** *office*
	(This value is provided by your ISP.)

Table 18-5 Location Table Values *(Continued)*

Setting	Command
Password	**set location** *isp1* **password** *passwd*
	(This value is provided by your ISP.)
Maximum ports	**set location** *isp1* **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.

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 must 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
Command> dial isp1 -x
```

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 is normally 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 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 12, "Configuring Filters." Refer to the *ChoiceNet Administrator's Guide* and *RADIUS for UNIX 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 18-6 provides a line-by-line description the filter.

Table 18-6 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 18-6 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 12-11.

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 10, "Using ISDN BRI," and Chapter 8, "Configuring Dial-Out Connections." See also Chapter 11, "Configuring the PortMaster 3."

Providing User Dial-In Access 19

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:

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

Overview of Dial-In Configuration

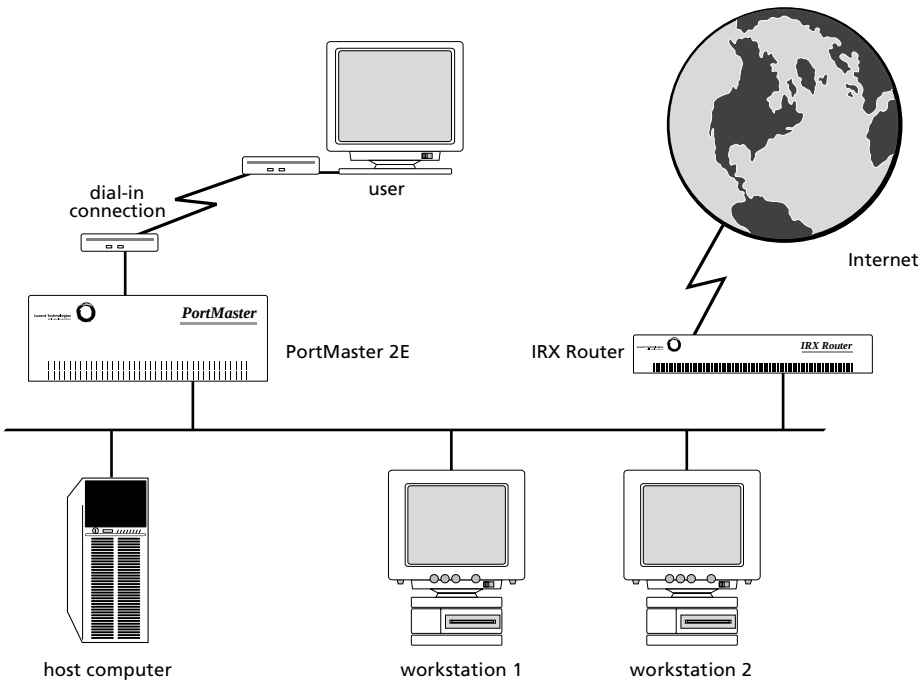
The PortMaster configuration described in this example (Figure 19-1) allows up to seven 30-port PortMaster Communications Servers to be connected together to provide up to 210 dial-in asynchronous ports. The PortMaster Communications Server allows dial-in users to access a host for shell accounts and/or 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 must be monitored closely to determine the need for additional ports. RADIUS accounting can help you to evaluate port usage. See the *RADIUS for UNIX 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 19-1 Dial-In User Configuration



Example Configuration

The example described in this chapter uses the values shown in Table 19-1. Change variable values to values that reflect your network.

Table 19-1 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 PortMaster products.	192.168.1.17 through 192.168.1.22 (**pm2.edu.com** through **pm7.edu.com**)
Reserved pool of assigned addresses for the first PortMaster.	192.168.1.33 through 192.168.1.62
Reserved pool of assigned addresses for the second PortMaster.	192.168.1.65 through 192.168.1.94

Table 19-1 Example Configuration Variables *(Continued)*

Variable Description	Value
Reserved pool of assigned addresses for the third PortMaster. Continue until the seventh PortMaster.	192.168.1.97 through 192.168.1.126
Reserved pool of assigned addresses for the seventh PortMaster.	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 19-5).**
2. **Configure global settings (page 19-5).**
3. **Configure Ethernet interface settings (page 19-6).**
4. **Configure asynchronous port settings (page 19-6).**
5. **Configure modems for the asynchronous ports (page 19-6).**
6. **Configure users via RADIUS settings if you have more than one hundred users (page 19-8).**
7. **Configure login users if you are not using RADIUS (page 19-9).**

8. **Configure network users if you are not using RADIUS (page 19-9).**
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 19-2.

Table 19-2 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_address** *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 19-2, 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 19-3.

Table 19-3 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 19-3, 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 19-4 can be set on all asynchronous ports on the first PortMaster. Use the modem

table described in Chapter 9, "Using Modems," to configure the attached modems, or set each port as a host device as described in Chapter 20, "Accessing Shared Devices," and configure each modem individually.

Note – On V.34 modems, lock the DTE rate at 115200bps unless your modem manual instructs otherwise. On V.32bis modems, 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 9, "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, connect to each 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 19-4 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** *usr-v34*
Speed 1	**set all speed 1** *115200*
Speed 2	**set all speed 2** *115200*
Speed 3	**set all speed 3** *115200*
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 19-4, 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 19-5 lists the RADIUS setting for the first PortMaster. For information about RADIUS parameters, refer to the *RADIUS for UNIX Administrator's Guide* or access the information via FTP from **ftp://ftp.livingston.com/pub/le/radius/radius.install**.

Table 19-5 RADIUS Values

Setting	Command
Secret	**set secret** *anyvalue*
Authentication server	**set authentication_server** *192.168.1.2*
Alternate authentication server	**set alternate_auth_server** *198.168.1.3* (This setting is optional. This secondary server must have a RADIUS database identical to that on the primary authentication server.)
Accounting server	**set accounting** *192.168.1.2*
Alternate accounting server	**set accounting 2** *192.168.1.3* (This setting is optional.)

After configuring RADIUS settings as shown in Table 19-5, 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 passthrough logins.

A user account must be set up on the PortMaster for each authorized user. Configure each new user *user1*, *user2*, and so on, with the values shown in Table 19-6.

Table 19-6 User Table Values for *user1*

Setting	Command
Username	**add user** *user1*
Password	**set user** *user1* **password** *passwd*
Login service	**set user** *user1* **service** *portmaster* (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 19-6, 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. Configure each new user *usera*, *userb*, and so on with the values shown in Table 19-7.

Table 19-7 User Table Values for *usera*

Parameter	Command
Username	**add netuser** *usera*
Password	**set user** *usera* **password** *passwd*
Protocol	**set user** *usera* **protocol** *ppp*
Address type	**set user** *usera* **destination** *assigned*
Compression	**set user** *usera* **compression** *on*
RIP routing	**set user** *usera* **rip** *off*

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 19-7, 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
   ```

Accessing Shared Devices 20

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:

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**).

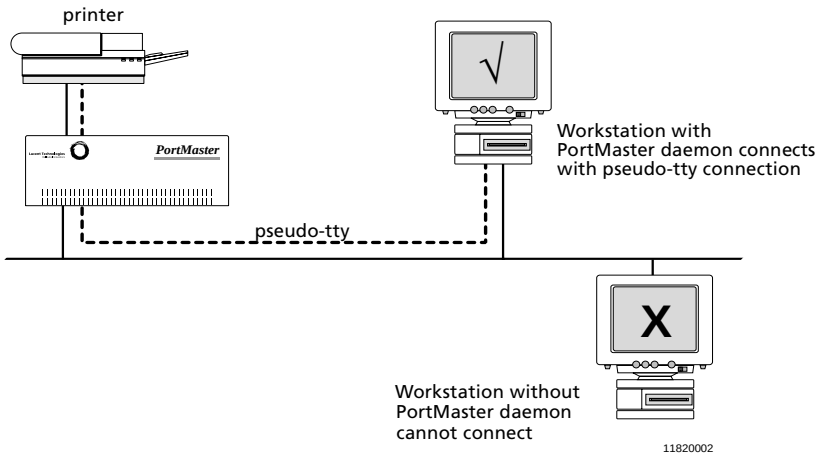
Host Device Configuration

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 20-1 shows a diagram of the host device configuration using the PortMaster device service and a pseudo-tty connection.

Figure 20-1 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**.

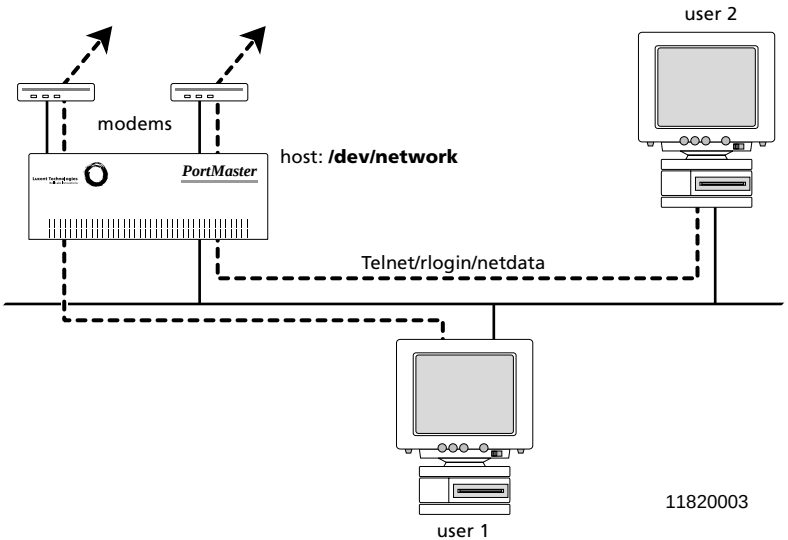
Figure 20-2 shows an example of the network device configuration.

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 20-2 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 20-4).**
4. **Configure Ethernet port settings (page 20-5).**
5. **Configure two-way serial port (S2) settings (page 20-5).**
6. **Configure serial printer port (S9) settings (page 20-7).**
7. **Configure parallel port (P0) settings (page 20-8).**
8. **If necessary, configure network devices for Telnet access (page 20-8).**

Configuring Global Settings

Configure the global settings to the value shown in Table 20-1.

Table 20-1 Global Value

Setting	Command
Default host	**set host** *192.168.200.2* (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 192.168.200.2.

After you configure global settings as shown in Table 20-1, 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 20-2.

Table 20-2 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 20-2, 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 20-3.

Table 20-3 Serial Port Values (S2)

Setting	Command
Port type	**set** *s2* **twoway /dev/ttyrf**

Table 20-3 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 20-3, 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 20-4. If the printer is a DTE, use a null modem cable to connect to the port.

Table 20-4 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 20-4, 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 20-5.

Table 20-5 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 20-5, 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 20-6. This example is for port S1.

Table 20-6 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 9, "Using Modems."

Using Synchronous Leased Lines 21

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:

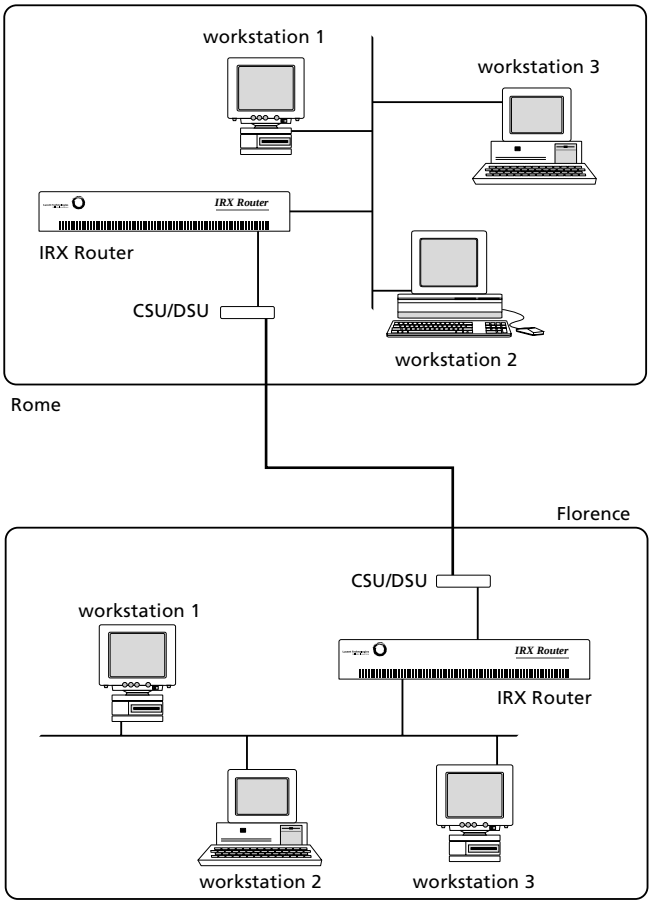
See the *PortMaster Command Line Reference* for more detailed command descriptions and instructions.

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 21-1 shows an example of the leased line connection.

Figure 21-1 Leased Line Configuration



If you are connecting two networks together for the first time, 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 recommended 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 21-4)
    b. Ethernet interface settings (page 21-4)
    c. Synchronous WAN port settings (page 21-5)
2. **Configure the following settings for the PortMaster in Florence:**
    a. Global settings (page 21-6)
    b. Ethernet interface settings (page 21-6)
    c. Synchronous WAN port settings (page 21-7)
3. **Troubleshoot the configuration, if necessary (page 21-8).**

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 21-1.

Table 21-1 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 21-1, 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 21-2.

Table 21-2 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 21-2, 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 21-3. 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 21-3 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 21-3, 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."

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 21-4.

Table 21-4 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 21-4, 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 21-5.

Table 21-5 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 21-5, 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 21-6. The IP address for the port is left unconfigured, accepting the default IP address value of 0.0.0.0.

Table 21-6 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 21-6, 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 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.
- 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.

Networking Concepts A

This chapter describes general network concepts that you must understand before you configure your PortMaster.

This chapter discusses the following topics:

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.

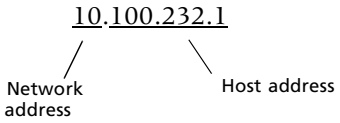
For example, 192.168.42.*x* describes a Class C network with addresses ranging from 192.168.42.0 through 192.168.42.255. CIDR uses 192.168.42.0/24 to describe the same range of addresses.

RIP-1 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

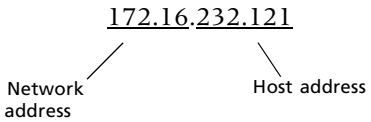
The class A IP address format allocates the highest 8 bits to the network field and sets the highest-priority bit to 0 (zero). The remaining 24 bits form the host field. Only 126 class A networks can exist (0 is reserved, and 127 is used for loopback networks), but each class A network can have almost 17 million hosts. No new class A networks can be assigned at this time.

For example:



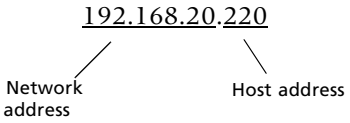
Class B Addresses

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 PortMaster products, 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:

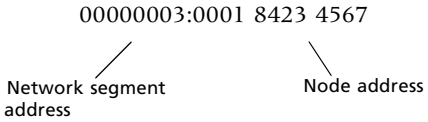
- Network segment address, expressed as 8 hexadecimal digits

  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 supernetwork (supernet) or a subnetwork (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	0xffffff00	255.255.255.0
25	2	126	0xffffff80	255.255.255.128
26	4	62	0xffffffc0	255.255.255.192
27	8	30	0xffffffe0	255.255.255.224
28	16	14	0xfffffff0	255.255.255.240
29	32	6	0xfffffff8	255.255.255.248
30	64	2	0xfffffffc	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 must 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 – Use the internal host table 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
- L2TP tunnels

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 for UNIX 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 for UNIX Administrator's Guide*.

Or, for a more fully featured RADIUS server, use the Lucent NavisRadius™ product, which supports vendor-specific attributes.

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 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)
nicname	43	TCP	**whois** Internet directory service
nicname	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
l2tp	1701	UDP	Layer 2 Tunneling Protocol (L2TP)

Glossary

Numerics

3DES

Triple data encryption standard. A strengthened version of the data encryption standard (DES) documented in RFC 1851. Also known as *triple DES*, this standard is based on the existing DES, but has a key three times as long.

10Base2

Physical specification for a type of Ethernet that transmits 10Mbps signals over thin 50-ohm baseband coaxial cable and has a cable length limit of 607 feet (185m) per segment. A 10Base2 Ethernet network is the least expensive Ethernet. This version of Ethernet is also known as *thin Ethernet* or *Cheapernet*.

10Base5

Physical specification for a type of Ethernet that transmits 10Mbps signals over standard (thick) 50-ohm baseband coaxial cable and has a cable length limit of 1640 feet (500m) per segment. A 10Base5 Ethernet network provides a low-cost alternative to fiber optic cable for use as a backbone within one building. This version of Ethernet is also known as *thick Ethernet*.

10BaseF

Physical specification for a type of Ethernet that transmits 10Mbps signals over fiber optic cable and has a cable length limit of from 1640 feet to 6560 feet (500m to 2000m) per segment. Use a 10BaseF Ethernet network to link users in different buildings.

10BaseT

Physical specification for a type of Ethernet that transmits 10Mbps signals over unshielded twisted-pair cable and has a cable length limit of 330 feet (100m) per segment. A 10BaseT Ethernet network is the most flexible topology for LANs and is generally the best choice for most network installations.

A

AAA

Authentication, authorization, and accounting. A remote access security approach that controls network access by requiring user identification and restricting access to only particular resources. AAA, also known as *triple A*, maintains records of use for billing and network audit.

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**.

access concentrator

See **remote access server**.

access-request

A packet sent by a network access server to a RADIUS server when a user logs in to the network access server. The access-request packet includes the user's login name and password and information about the connection made by the user to the network access server. RADIUS uses the access-request to authenticate the user and authorize services to the authenticated user.

access router

A type of router used to link a LAN across a WAN. An access router uses an Ethernet port to connect to a LAN and one or more asynchronous and/or synchronous ports to provide the LAN with a long-distance connection to another router on another network. PortMaster Office Routers and PortMaster IRX products are access routers.

access server

See **remote access server**.

accounting

See **RADIUS accounting**.

accounting server

The RADIUS server component responsible for handling RADIUS accounting.

ActivCard

An authentication system available from ActivCard, Inc. ActivCard uses tokens and a software server to generate and confirm one-time passwords to identify users and grant or deny them network access.

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.

ADSL

Asymmetric digital subscriber line. A modem and compression technology that can transmit multiple channels of multimedia data over regular telephone lines. An ADSL circuit is much faster than a regular telephone connection even though the customer connection is the same copper wires used for regular telephone service. Because an ADSL circuit must be configured to connect two specific locations, it is similar to a leased line.

advertisement policy

A set of rules that determines 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 American National Standards Institute (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**.

API

Application program interface or application programming interface. An interface between an operating system and application programs that includes the calling convention used for their communication and the services that the operating system makes available to the programs. An API provides a set of routines, protocols, and tools for building software applications, and specifies the standard software interrupts, calls, functions, and data formats that an application must use to initiate contact with hardware or network services. Programmers can use the API to write applications consistent with the operating environment without having to know all about it. In contrast to an API, a graphical user interface (GUI) and command interface are direct user interfaces to either the application or the operating system.

applet

1) A small application, such as a utility or other small program, that does not run on its own but is embedded and run from within another application. Applets often cannot access certain resources on the local computer, such as files and serial devices, and cannot communicate with most other computers across a network. 2) A small distributed application created with the Sun Microsystems Java programming language. Java applets are often embedded in HTML pages and can be downloaded and used by any computer equipped with a Java-capable browser. See also **HTML**; **Java**.

AppleTalk Remote Access

See **ARA**.

application program interface

See **API**.

application programming interface

See **API**.

ARA

AppleTalk Remote Access. A protocol that provides Macintosh users with direct access to information and resources at a remote AppleTalk site.

Archie

ARCHIvE. An Internet utility for finding files stored on anonymous FTP sites. To find a file with Archie, you must know the exact filename or a substring of it. See also **FTP**.

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.

asymmetric digital subscriber line

See **ADSL**.

asynchronous

Not synchronized by a shared signal and therefore proceeding independently; not occurring at predetermined or regular intervals.In asynchronous communication, data is transmitted character by character, intermittently rather than in a steady stream. Transmission can start and stop at any time. The beginning of a character of asynchronous data is indicated by a start bit, and the end is indicated by a stop bit.

Asynchronous communication is slower and less efficient than synchronous communication, but usually simpler and cheaper. All PortMaster products have at least one asynchronous port for connection to a console, or to connect an external modem, mainframe computer, or other peripheral device to the local network. Compare **synchronous**.

Asynchronous Transfer Mode

See **ATM**.

ATM

Asynchronous Transfer Mode. A packet switching network technology that organizes digital data into 53-byte cells, or packets, and transmits them via digital signal technology. ATM creates a fixed channel, or route, between two points whenever data transfer begins. The short, standardized ATM cells can be processed through a digital ATM switch and transmitted at speeds of 600Mbps or more. ATM supports multiple services, including voice, graphics, data, and video, and allows telephone and cable TV companies to dynamically assign bandwidth to individual customers.

ATM Forum

An international nonprofit organization formed to accelerate the use of Asynchronous Transfer Mode (ATM) products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

attribute

1) A named characteristic of something. 2) In RADIUS, one-half of an attribute-value pair used to identify (authenticate) a user or to configure (authorize) a user's session.

attribute-value pair

In RADIUS, the name of a characteristic that identifies (authenticates) a user or configures (authorizes) a user's session, and its value. Attribute-value pairs, also known as *AV pairs*, define the RADIUS protocol. Packets that are sent between a RADIUS server and a network access server consist of attribute-value pairs—for example, **password = "s64bigE&rt"**.

authentication

See **RADIUS authentication**.

authentication, authorization, and accounting

See **AAA**.

authorization

See **RADIUS authorization**.

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 high-speed line or series of connections that forms a major pathway within a network.

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.

bandwidth

1) The amount of data, usually measured in bits per second, that can be sent through a connection. 2) The range of frequencies available for network transmission.

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.

BBS

Bulletin board system. A computer service reached via modem or Telnet that allows users to conduct discussions, upload or download files, and post announcements. Some BBSs are devoted to specific interests; others offer a more general service. The World Wide Web is superseding most BBSs because it provides wider, cheaper access to information.

B channel

Bearer channel. The ISDN channel that is the primary carrier of data, voice, and other services. An ISDN Basic Rate Interface (BRI) has a single 64Kbps B channel, and an ISDN Primary Rate Interface (PRI) has either 23 B channels (in the United States) or 30 B channels (in Europe).

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**.

bit

Binary digit. 1) The basic unit of information. 2) The amount of information obtained as the answer to a yes-or-no question. (3) A computational quantity that can take on one of two values, such as *true* and *false*, or 0 and 1. (4) The smallest unit of storage that is sufficient to hold one bit. See also **bps**; **byte**.

bits per second

See **bps**.

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

Internet Bootstrap Protocol. Protocol used by a network node to determine the IP address of its Ethernet interfaces for network booting. When dumb hosts send a broadcast packet out on the network, UNIX hosts running BOOTP reply with an IP address, the address of a boot server, and the path of a configuration file to be loaded at boot time.

Border Gateway Protocol

See **BGP**.

bps

Bits per second. A unit for measuring the data rate.

BRI

Basic Rate Interface. An ISDN interface for homes and small businesses 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.

browser

A client software program used to locate and display World Wide Web pages. Examples of some well-known browsers are Netscape Navigator and Microsoft Explorer.

bulletin board system

See **BBS**.

byte

A set of bits (usually 8) that represent a single character. See also **bit**.

C

callback

A remote access server configuration that disconnects a dial-in user and then calls the user back at a pre-established telephone number before providing access. Callback provides an extra layer of security and can simplify telephone charges. Callback is sometimes known as *dialback*.

CAP

Competitive access provider. A company that provides network links between the customer and the interexchange carrier (IEC) or even directly to the Internet service provider (ISP). CAPs operate private networks independent of local exchange carriers. See also **CLEC**.

Carrier Detect

See **CD**.

CCITT

Consultative Committee for International Telegraph and Telephone. International organization formerly responsible for the development of communications standards and now called the *ITU-T*. See also **ITU-T**.

CD

Carrier Detect. A signal that indicates whether an interface is active. Also, a data communications equipment (DCE) signal—Data Carrier Detect (DCD)—generated by a modem indicating that a call has been connected.

central office

See **CO**.

CGI

Common gateway interface. A standard set of rules for transferring information between a World Wide Web server and a CGI program—any program designed to accept and return data that conforms to the CGI specification. For example, a CGI program can put the content of a form into an email message, or transform data into a database query. The program can be written in any programming language, including C, Perl, Java, or Visual Basic.

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. The user is given an unpredictable number and challenged to respond with an encrypted version. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. See also **PAP**.

chat

Real-time communication between two users on the Internet via computer. See also **IRC**.

check item

A component of a RADIUS user profile one or more of which must be matched in an access-request for the access to succeed. See also **address**; **reply item**.

ChoiceNet®

A packet-filtering application that enables central server storage of filters, dynamic filter downloading, and the control of user access based on lists of sites rather than individual sites. Developed by Lucent Technologies, the ChoiceNet server is shipped with all PortMaster remote access servers and routers.

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*.

class

In object-oriented programming, a category of objects. The class defines the common properties, operations, and behaviors of different objects that belong to it. For example, a class called *shape* might contain objects that are circles, rectangles, and triangles. A class can be regarded as a template definition of the methods and variables in a particular kind of object. A class with subclasses, which inherit all or some of its characteristics, is also known as a *superclass*. The structure of a class and its subclasses is called a *class hierarchy*. See also **class library**; **object**; **subclass**.

class library

A collection of related classes that solve specific programming problems. See also **class**.

classless interdomain routing

See **CIDR**.

clearing house server

A forwarding server in a proxy confederation that stores the addresses of all remote servers so that the other forwarding servers need to store only its address. The clearing house server forwards requests from forwarding servers to remote servers, and passes information back from the remote servers to the forwarding servers.

CLEC

Competitive local exchange carrier. A company that provides local dial-tone services as well as long-distance, data, and Internet services, usually to corporate markets in metropolitan areas. Many CLECs can compete with established regional Bell operating companies (RBOCs) because they use more current technology. See also **CAP**.

client

A software program on one computer that contacts and obtains data from a server software program running on another computer. Each client program is designed to work with one or more specific kinds of server programs, and each server requires a specific kind of client—a World Wide Web browser, for example.

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. The ChoiceNet product, for example, runs in a client-server environment.

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. 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.

CO

Central office. A local telephone company office where customer lines in a given area terminate and where subscriber lines are circuit-switched.

command line interface

The visual appearance and command input conventions that enable system administrators and system operators to configure, monitor, and manage the connected nodes in a data network. This type of direct command-entry screen interface is distinguishable from graphical user interfaces (GUIs). Compare **GUI**.

committed information rate

See **CIR**.

common gateway interface

See **CGI**.

communications server

A remote access device with one or more asynchronous ports that provides dial-up network access to users and devices without network interfaces. A communications server allows remote users, nonnetwork printers, mainframe computers, and other peripherals to connect to a network through its asynchronous port(s). PortMaster 2 products are communications servers. Compare **remote access server**.

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 products.

competitive access provider

See **CAP**.

competitive local exchange carrier

See **CLEC**.

compression protocol

A protocol that can improve Internet transmission speeds by as much as 400 percent by compressing data at the sending modem and decompressing it at the receiving modem. For PortMaster products, ComOS version 3.7 or later implements the PPP Compression Control Protocol (RFC 1962) and Stac LZS Compression Protocol (RFC 1974). Stac LZS data compression is available only on the PortMaster 3 and PortMaster Office Routers.

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.

Consultative Committee for International Telegraph and Telephone

See **CCITT**.

cookie

A small data file written to your hard drive by some websites when you view them in your browser. These data files contain information the site can use to track such things as passwords, lists of pages you have visited, and the date when you last looked at a certain page. Cookies maintain continuity in a series of requests and responses to the website.

cost

An arbitrary value assigned by a network administrator and used to compare paths through an internetwork environment. Cost is normally based on hop count, media bandwidth, or other measures. Routing protocols use cost values to determine the best—lowest-cost—path to a particular destination.

CPE

Customer premises equipment. Any hardware or software installed at a customer's site—such as routers, access servers, communications servers, terminal adapters, or modems—to enable communications with the public switched telephone network (PSTN). Maintenance of this equipment is primarily the responsibility of the customer rather than the responsibility of the local and/or long-distance carrier.

CRC

Cyclic redundancy check. An error-detection technique that derives a binary number by reading an incoming block of data and comparing it with a number transmitted with the data. If the numbers do not match, an error exists. See also **CRC error**.

CRC error

Cyclic redundancy check error. An error that indicates problems with source station hardware, receivers, retiming modules and/or repeaters, bridges, cables, or transceivers.

CSU

Channel service unit. An ancillary device needed to adapt the V.35 interface to a port on a telephone carrier switch. The CSU is placed between the data terminal equipment (DTE) and the switch.

customer premises equipment

See **CPE**.

cyclic redundancy check

See **CRC**.

D

database

A large collection of data organized for rapid search and retrieval, relatively simple management, and ease of updating. Traditional databases are organized by fields, records, and files. A field is a single piece of information, a record is one complete set of fields, and a file is a collection of records. The most prevalent type of database is the relational database. A database management system (DBMS) is required to access information from a database. See also **DBMS**; **distributed database**; **object-oriented database**; **RDBMS; relational database**.

database management system

See **DBMS**.

database table

A set of data arranged in rows and columns; a collection of records in a database.

data circuit-terminating equipment

See **DCE**.

data communications equipment

See **DCE**.

data encryption standard

See **DES**.

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**.

DBMS

Database management system. A collection of programs that enables you to store, modify, and extract information—organized in fields, records, and files—from a database. The DBMS accepts requests for data from the application program and instructs the operating system to transfer the appropriate data. Requests for information from a database are made in the form of a query—a stylized question. The terms *relational*, *network*, *flat*, and *hierarchical* refer to the way a DBMS organizes information internally. The internal organization can affect how quickly and flexibly information is extracted. New categories of data can be added to the database without disruption to the existing system. A DBMS also controls the security and integrity of the database. See also **RDBMS**.

DCE

Data communications equipment or data circuit-terminating 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 data terminal equipment (DTE) devices. Modems and interface cards are DCEs.

D channel

Data channel or delta channel. A full-duplex, 16Kbps Basic Rate Interface (BRI) or 64Kbps Primary Rate Interface (PRI) ISDN channel for performing call signaling and setup to establish a connection. The D channel is sometimes also used to carry user data.

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**.

DES

Data encryption standard. A popular block encryption method based on a 56-bit key. DES has been adopted by the U.S. Department of Defense and standardized as American National Standards Institute (ANSI) standards X3.92 and X3.106.

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**.

device

Any machine or hardware component that attaches to a computer or network. Examples of devices include printers, modems, routers, and network access servers.

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**.

dialed number identification service

See **DNIS**.

dial group

A number that is used to associate dial-out locations with ports on a PortMaster.

dictionary

See **RADIUS dictionary**.

digital service unit

See **DSU**.

digital signal processor

See **DSP**.

digital subscriber line

See **DSL**.

direct memory access

See **DMA**.

distributed database

A database that can be dispersed or replicated among different points in a network. See also **database**.

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.

DLL

Dynamic link library. A file containing executable routines—generally performing a specific function or set of functions—that is stored separately, loaded into memory only when required, and unloaded when space is needed for other applications. A DLL conserves memory, can be shared by other programs, and can be modified without changes to the calling program or other DLLs.

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.

DNIS

Dialed number identification service. A caller identification service that provides you with the number that the caller dialed. DNIS is typically a feature of 800 and 900 lines and is useful when calls from multiple 800 or 900 numbers are routed to the same destination. This service is most often provided on T1 lines by passing touch-tone dual-tone multifrequency (DTMF) or multifrequency (MF) digits and requires a T1 voice board.

DNS

Domain Name System. The system used on the Internet for translating between network hostnames (such as **bigcompany.com**) and IP addresses (such as 192.168.224.20).

domain name

A name that identifies one or more IP addresses. Domain names are used in uniform resource locators (URLs) to identify particular World Wide Web pages. Domain names always have two or more parts: the part to the left is the most specific, and the part to the right is the most general (as, for example, *Lucent.com*). A given machine can have more than one domain name, but a given domain name points only to one machine. Because the Internet is based on IP addresses, not domain names, every Web server requires a Domain Name System (DNS) server to translate domain names into IP addresses.

Domain Name System

See **DNS**.

dotted decimal notation

Common *n.n.n.n* notation for IP addresses. Each number *n* represents, in decimal, 1 byte of the 4-byte IP address. Dotted decimal notation is also known as *dot address*, *dotted notation*, *dotted quad notation*, or *four-part notation*.

DRAM

Dynamic random access memory. A type of semiconductor random access memory (RAM) that stores information in integrated circuits containing capacitors.

DS-0

Digital signal level 0. A single 64Kbps digital telephone channel.

DS-1

Digital signal level 1. See **T1**.

DSL

Digital subscriber line. A technology that uses sophisticated modulation schemes to pack data onto copper wires for connections from a telephone switching station to a home or office. DSL is similar to ISDN because both operate over existing copper telephone lines and require runs of usually less than 20,000 feet to a central telephone office. However, DSL offers much higher speeds than ISDN. Types of DSL include asymmetric DSL (ADSL), symmetric DSL (SDSL), high-data-rate DSL (HDSL) and single-line DSL (SDSL). See also **ADSL**.

DSP

Digital signal processor. A specialized digital microprocessor that performs calculations on digital signals that were originally analog to improve their accuracy and reliability. Most DSPs are programmable and can manipulate different types of information, including sound, images, and video.

DSR

Data Set Ready. The circuit that is activated when data communications equipment (DCE) is started 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 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**.

dual homing

A network topology in which a device is connected to the network through two independent access points, or points of attachment.

dynamic data exchange

See **DDE**.

dynamic filter download

A feature of ChoiceNet that downloads filters from the server to a network access server upon request.

Dynamic Host Configuration Protocol

See **DHCP**.

dynamic link library

See **DLL**.

dynamic random access memory

See **DRAM**.

E

E1

A 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 and can be connected with T1 lines for international use. 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.

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.

email

Electronic mail. Electronic messages, usually text, sent from one person's computer to another's. Email can also be broadcast automatically to a large number of addresses, or mail list.

Encapsulating Security Payload

See **ESP**.

endpoint discriminator

A 12-digit identifier used to associate multiple chassis in a Multichassis PPP domain.

ESP

Encapsulating Security Payload. A mechanism, documented in RFC 1827, for providing integrity and confidentiality to IP datagrams by means of encryption. See also **IPSec**.

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 (UTP).

Exterior BGP

See **EBGP**.

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.

extranet

An intranet that is accessible to authorized outsiders. You can access an extranet only if you have a valid username and password, and your identity determines which parts of the extranet you can view. Extranets are a popular means for business partners to exchange information. Compare **intranet**.

F

FAQ

Frequently asked questions. Documents that list and answer the questions most often asked about a particular subject. The World Wide Web contains thousands of FAQs on subjects as diverse as pet grooming and cryptography.

FDDI

Fiber Distributed Data Interface. A standard for transmitting data on fiber optic cable at rates of up to 100 million bits per second—10 times as fast as Ethernet, and about twice as fast as T3. FDDI networks are typically used as backbones for WANs.

Fiber Distributed Data Interface

See **FDDI**.

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.

finger

A command used to gather information about a network user—such as name, login name, office location, telephone number, email address, and account activity.

firewall

A way to restrict access between the Internet and an internal network. Most often, a firewall is a set of hardware components with appropriate filtering software that can guard an internal network against known problems or intruders, or isolate less secure parts of the internal network from other parts.

FireWall IRX™

A PortMaster IRX router with two Ethernet ports that provides two networks: a public network accessible to the Internet via World Wide Web and File Transfer Protocol (FTP) servers, and a private internal network protected from Internet traffic and potential intruders.

Flash RAM

See **NVRAM**.

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.

forwarding server

A server running a version of RADIUS that supports proxy service. The forwarding server passes a request for service from a proxy user to a remote server—or another forwarding server—for authentication.

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 an opening flag, address, control protocol, data, padding, frame check sequence, and closing flag. 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**.

frequently asked questions

See **FAQ**.

FTP

File Transfer Protocol. A TCP/IP protocol used to transfer files between network hosts or two Internet sites. Many Internet sites can be publicly accessed through the use of FTP. Users can log in with the account name *anonymous*. These sites are called *anonymous FTP servers*.

G

gateway

A combination of hardware and software linking two or more networks that use different protocols. Gateways between email systems, for example, allow users on different email systems to exchange messages. Gateways provide address translation services, but do not translate data.

Generic Routing Encapsulation

See **GRE**.

GIF

Graphics interchange format. A common format for image files on the World Wide Web and elsewhere on the Internet, especially suitable for images containing large areas of the same color. GIF is a bit-mapped format that also includes data compression. See also **JPEG**.

gigabyte

A data measurement unit equal to 1,073,741,824 bytes or 1,024 megabytes.

graphical user interface

See **GUI**.

graphics interchange format

See **GIF**.

GRE

Generic Routing Encapsulation. A protocol documented in RFC 1701 that allows one network protocol to be transmitted over another by encapsulating its packets—called *payload packets*—within GRE packets, which in turn are contained within packets of the outer or delivery protocol. RFC 1702 describes the use of GRE when the delivery protocol is IP.

GUI

Graphical user interface. A software interface based on pictorial representations and menus of operations and files. Compare **command line interface**.

H

H.324

The ITU-T recommendation describing terminals that send video, audio, and computer (multimedia) data over low bit-rate networks such as the public switched telephone network (PSTN). H.324 terminals can be integrated into PCs or implemented in stand-alone devices such as videotelephones.

hardwired

Pertaining to 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.

H channel

High-speed channel. A full-duplex ISDN Primary Rate Interface (PRI) channel operating at 384Kbps.

hello

A 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.

HMAC

Keyed-hashing message authentication code. A message authentication mechanism that uses cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function—for example, MD5 or SHA-1—in combination with a secret shared key. The effectiveness of HMAC depends on the properties of the underlying hash function. See also **MD5**; **SHA-1**.

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 that is a repository for services made available to other computers on a network. Computers, networked printers, and routers are examples of hosts.

HotJava

A World Wide Web browser from Sun Microsystems that can run Java applets.

hot-swappable

Able to be removed and replaced while the power is on and the system is operating. Hot-swapping components might disrupt service, however. For example, the line boards on a PortMaster 4 are hot-swappable because they can be replaced while ComOS is operating in a unit that is plugged in and turned on. Although you must turn off the line board and thereby terminate any services it is actively providing, the PortMaster 4 retains the board's settings so that the new board requires no reconfiguration after the swap. Compare **redundant**.

HTML

HyperText Markup Language. The authoring language used to create hypertext documents for the World Wide Web. Like the Standard Generalized Markup Language (SGML), on which it is based, HTML identifies the types of information in a document rather than the exact way it is to be presented. The presentation is left to the software that converts the contents to a suitable format for viewing. HTML also provides a way to link a word or block of text on a website to another file on the same or another website. See also **HTTP**.

HTTP

HyperText Transfer Protocol. The application protocol for moving hypertext files across the Internet. This protocol requires an HTTP client program on one end of a connection and an HTTP server program on the other.

hunt group

A group of multiple telephone circuits that allows telephone calls to find an idle circuit to establish a link.

hunt order

The order in which connections are made to a port. For example, if two ports are open, a connection is made to the port with the lower hunt order.

HyperText Markup Language

See **HTML**.

HyperText Transfer Protocol

See **HTTP**.

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.

IETF

Internet Engineering Task Force. International community of network designers, operators, vendors, and researchers working in groups to develop new Internet standards and specifications.

in-band signaling

The transmission of signaling information over the same path as data and/or voice information. Compare **out-of-band signaling**.

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**.

integrated access server

See **remote access server**.

Integrated Services Digital Network

See **ISDN**.

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.

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**.

International Telecommunication Union Telecommunication Standardization Sector

See **ITU-T**.

Internet

The total collection of interconnected networks and attached devices that use TCP/IP protocols. World-wide the Internet currently consists of several large national backbone networks and several regional and campus networks.

Internet Control Message Protocol

See **ICMP**.

Internet Engineering Task Force

See **IETF**.

Internet Network Information Center

See **InterNIC**.

Internet Packet Exchange protocol

See **IPX**.

Internet Protocol

See **IP**.

Internet Protocol Security

See **IPSec**.

Internet Relay Chat

See **IRC**.

Internet service provider

See **ISP**.

Internet telephony

See **VoIP**.

internetwork

A network of networks.

InterNIC

Internet Network Information Center. An organization that provides information and services related to networking technologies. The InterNIC is where new domain names are registered.

interoperability

The ability to exchange information among devices that have dissimilar operating systems or protocols.

intranet

A private internetwork inside a company or agency that uses the same kind of software running on the Internet, but only for internal purposes. A corporate intranet uses the Internet as its backbone, but the firewall surrounding the intranet prevents unauthorized access. Like the Internet, intranets are used to share information. See also **Internet**; **extranet**.

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, 192.168.200.1. 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 10.0.0.0/8 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.

IPSec

Internet Protocol Security. A set of protocols being developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the network layer. IPSec is useful for virtual private networks (VPNs) and for remote user access through dial-up connection to private networks. IPSec provides two choices of security service: Authentication Header (AH), which allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both sender authentication and data encryption.

IPVPN

IP-based virtual private network. See **VPN**.

IPX

Internet Packet Exchange. An 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**.

IRC

Internet Relay Chat. A protocol that provides real-time communication over the Internet via a series of linked, Internet-connected IRC servers. IRC allows anyone with Internet access and IRC client software to chat with others who have similar access. Unlike older chat systems, IRC is not limited to just two participants. See also **chat**.

IRX™ Routers

A series of PortMaster products that provide wide-area interconnectivity between Novell IPX, TCP/IP, and mixed network environments.

ISDN

Integrated Services Digital Network. A digital communications standard that enables the transmission of information over existing twisted pair telephone lines at higher speeds than standard analog telephone service. ISDN is available at two levels of service: Basic Rate Interface (BRI) for home and small business use and Primary Rate Interface (PRI) for larger users. Both levels provide multiple B (bearer) channels for data, voice, and other services, and one D channel for control and signaling information. See also **BRI**; **PRI**.

ISO

International Organization for Standards. The international organization that sets standards for network communication protocols.

ISP

Internet service provider. A company that provides individuals and other companies with access to the Internet and other related services. An ISP has the equipment and the telecommunication line access required to provide points-of-presence (POPs) on the Internet for the geographic area served. Larger ISPs who have their own high-speed leased lines are less dependent on the telecommunication providers and can provide better service to their customers.

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**.

J

jabber

1) A device that provides improper electrical signals on a network. On an Ethernet network, which uses electrical signal levels to determine whether the network is available for transmission, a jabber can cause the network to halt because it indicates to all other devices that the Ethernet is busy. 2) To transmit meaningless data via networks.

Java

A cross-platform, object-oriented programming language invented by Sun Microsystems. Java programs can be easily downloaded to a computer from the Internet. Small Java programs called *applets* add special features to World Wide Web pages including animation and interactive tools like calculators. See also **applet**.

Java database connectivity

See **JDBC**.

Java development kit

See **JDK**.

Java Runtime Environment

See **JRE**.

Java Virtual Machine

See **JVM**.

JDBC

Sometimes known as Java database connectivity. A Java application programming interface (API) for carrying out structured query language (SQL) statements. JDBC consists of a set of classes and interfaces written in the Java programming language. It provides a standard API for tool and database developers to write database applications in pure Java.

JDK

Java development kit. A suite of software than enables programmers to write applets and applications conforming to the Java 1.1 core application programming interface (API). Applets written with the JDK can be run by browsers supporting Java.

JRE

Java Runtime Environment. The smallest set of executable programs and files that constitute the standard Java platform. The JRE consists of the Java Virtual Machine (JVM), the Java platform core classes, and supporting files. Because it is the runtime part of the Java development kit (JDK), the JRE includes no compiler, debugger, or tools.

Joint Photographic Experts Group

See **JPEG**.

JPEG

Joint Photographic Experts Group. A bitmapped format for image files. JPEG provides lossy compression by segmenting the picture into small blocks, which are divided to get the desired ratio; the process is reversed to decompress the image. JPEG format is preferred over GIF files for the storage and transmission of color and grayscale photographs. See also **GIF**.

JVM

Java Virtual Machine. Software that acts like a mini-PC, interpreting the Java code so that the PC itself does not have to. A single Java applet or application can run unmodified on any operating system that has a virtual machine, or VM. Sun Microsystems writes a virtual machine that it licences to other companies, but operating system vendors generally write their own.

K

K56flex

A technology developed by Lucent Technologies and Rockwell International for delivering data rates up to 56Kpbs over standard telephone lines. K56flex sends digital data *downstream*—to a modem at a home or business but not from it. Data transmission in the upstream direction takes place at speeds of up to only 33Kbps. K56flex technology conforms to the ITU-T-approved V.90 standard for 56Kbps modems.

Kb

Kilobit(s). 1024 bits.

KB

Kilobyte(s). 1024 bytes.

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. See also **notification message**; **open message**; **update message**.

key

In a database management system (DBMS), a field used to sort data and thereby identify information.

keyed-hashing message authentication code

See **HMAC**.

kilobit

See **Kb**.

kilobits per second

See **Kbps**.

kilobyte

See **KB**.

L

L2F

Layer 2 Forwarding. A protocol developed by Cisco Systems and similar to the Point-to-Point Tunneling Protocol (PPTP) developed by Microsoft Corporation. L2F supports the creation of secure virtual private networks (VPNs) over the Internet. Cisco and Microsoft recently agreed to merge their protocols into a single standard called *Layer Two Tunneling Protocol (L2TP)*. See also **L2TP**.

L2TP

Layer 2 Tunneling Protocol. An extension to the Point-to-Point Protocol (PPP) that enables Internet service providers (ISPs) and others to operate virtual private networks (VPNs) over the Internet. L2TP interoperates with such existing standard security protocols as RADIUS. See also **L2F**.

L2TP access concentrator

See **LAC**.

L2TP network server

See **LNS**.

LAC

L2TP access concentrator. A Point-to-Point Protocol (PPP) access server with Layer 2 Tunneling Protocol (L2TP) capabilities that provides the physical connection (usually a modem or ISDN port) between the dial-in user and the outsourcer. On a PortMaster 4, a LAC can be a single line board or the entire device. See also LNS; outsourcer.

LAN

Local area network. A local collection, usually within a single building or several buildings, of PCs and other devices connected by cable 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.

Layer 2 Forwarding

See **L2F**.

Layer 2 Tunneling Protocol

See **L2TP**.

LCP

Link Control Protocol. The protocol used by the Point-to-Point Protocol (PPP) for establishing, configuring, and testing the data link connection.

LDAP

Lightweight Directory Access Protocol. A proposed open standard for directory services that enables anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. Endorsed by more than 40 companies, LDAP allows corporate directory entries to be arranged in a hierarchical structure that reflects geographical and organizational boundaries rather than according to arbitrary codes. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler and supports TCP/IP.

leased line

A permanent telephone connection between two points that is rented for exclusive use from a telecommunications common carrier. In contrast to a normal dial-up connection, a leased line is always active. Typically, the highest-speed data connections require a leased line connection. For example, a T1 channel is a type of leased line that provides a maximum transmission speed of 1.544Mbps

LEC

Local exchange carrier. An organization that provides telephone exchange service or exchange access. An LEC is a U.S. local telephone company, which can be either a regional Bell operating company (RBOC) or an independent. See also **RBOC**.

LED

Light-emitting diode.

Lightweight Directory Access Protocol

See **LDAP**.

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 Systems/Stratacom LMI, and the American National Standards Institute (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**.

LNS

L2TP network server. A Point-to-Point Protocol (PPP) server with Layer 2 Tunneling Protocol (L2TP) capabilities that is the end point of a session.The LNS handles the authentication of the user via a RADIUS server and routes network traffic to and from the user. The LNS has no physical ports, only virtual interfaces. On a PortMaster 4, an LNS can be an LNS board, a Quad T1 or Tri E1 board, or the entire device. See also LAC.

local area network

See **LAN**.

local exchange carrier

See **LEC**.

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 on a PortMaster.

location table

A database on the PortMaster where location settings are stored. See also **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**.

login status

RADIUS accounting data for an individual RADIUS user. Login status includes such information as username, start and stop times, connection times, IP address of the network access server, network access server port, and IP address of the user (framed IP address).

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.

Lucent

Marked by clarity; shining; glowing with light; resplendent.

M

MAC

1) Media access control. See **MAC address**. 2) Message authentication code. A mechanism used between two parties that share a secret key to verify the contents, origin, author, and other attributes of information exchanged by the parties. See also **HMAC**.

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

Megabit(s). 1,048,576 bits or 1,024 kilobits.

MB

Megabyte(s). 1,048,576 bytes.

MBone

Multicast backbone. An experimental framework for developing and refining multicast protocols and applications on the Internet. The MBone network within the Internet supports IP multicasting—the two-way transmission of data between multiple sites. Multicasting sends files, usually audio and video streams, to multiple users at roughly the same time somewhat as radio and TV programs are broadcast over the airwaves.

Mbps

Megabits per second. A unit for measuring data rates.

MD5

Message digest algorithm 5. An iterative cryptographic hash function for message authentication. Used in Simple Network Management Protocol (SNMP) v.2, for example, MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The PortMaster ComOS uses the RSA Data Security, Inc. MD5 Message-Digest Algorithm. See also **SHA-1**.

mean time to recovery

See **MTTR**.

mean time to repair

See **MTTR**.

media access control address

See **MAC address**.

megabit

See **Mb**.

megabits per second

See **Mbps**.

megabyte

See **MB**.

menu

A list of options displayed on a user's computer screen from which the user can choose. For example, a menu might provide a list of servers.

message authentication code

See **MAC**.

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.

MIME

Multipurpose Internet Mail Extensions. The standard, documented in RFC 1522 and RFC 1523, for attaching non-ASCII files to standard Internet mail messages. These files include graphics, spreadsheets, formatted word-processor documents, audio files, and other binary data.

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.

MTTR

1) Mean time to recovery. The average amount of time a device will spend in corrective maintenance over a given period of time. 2) Mean time to repair. The average amount of time needed to repair a failed unit.

MTU

Maximum transmission unit. The largest frame or packet that can be sent through a port on a PortMaster without fragmentation.

multicast backbone

See **MBone**.

Multichassis PPP

Multichassis Point-to-Point Protocol. Multilink PPP over two or more chassis.

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. Multiline load balancing is a proprietary PortMaster technique distinct from **Multilink PPP**.

Multilink PPP

Multilink Point-to-Point Protocol. A protocol defined in RFC 1990 that allows a PortMaster to automatically build up additional ISDN B channels as bandwidth needs increase. See also **Multichassis PPP**.

Multipurpose Internet Mail Extensions

See **MIME**.

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.

NAS

See **remote access server**.

NAT

Network address translator. Software that runs on a router and maps one IP address or group of IP addresses to another IP address or group of IP addresses. The mapping, or translation, is transparent to users and applications. The Lucent ComOS implementation of the Network Address Translator (NAT) protocol is based on the latest Internet Engineering Task Force (IETF) draft entitled *The IP Network Address Translator (NAT)*.

NCP

1) NetWare Core Protocol. A Novell protocol for accessing Novell NetWare file and print service functions via an underlying IPX or IP transport protocol. 2) Network Control Protocol. A series of protocols for establishing and configuring different network layer protocols over the Point-to-Point Protocol (PPP).

neighbor

In OSPF, two routers that have interfaces to a common network. On multiaccess networks, neighbors are dynamically discovered by the OSPF hello protocol.

netboot

To boot from a network server—usually a Trivial File Transfer Protocol (TFTP) server—or the process of doing so.

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 10.0.0.0/8 describe all networks whose IP addresses begin with 128. See also **IP address prefix**.

NetWare Core Protocol

See **NCP**.

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 access server

See **remote access server**.

network address translator

See **NAT**.

Network Control Protocol

See **NCP**.

network handle

A number assigned to an active socket on a PortMaster that can be used to close the socket manually rather than by request from the client.

network information center

See **NIC**.

Network Information Service

See **NIS**.

Network Information Service Plus

See **NIS+**.

network interface card

See **NIC**.

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.

NFAS

Non-facility associated signaling. Signaling that allows a D channel on one ISDN Primary Rate Interface (PRI) to control B channels located on other PRIs.

NIC

1) Network information center. Any office that handles information for a network. The famous of these on the Internet is the InterNIC. See also **InterNIC**. 2) Network interface card. A computer circuit board that provides network communication to and from a computer system. A NIC is also known as an *adapter*.

NIS

Network Information Service. A UNIX-based client-server protocol developed by Sun Microsystems for network naming and administration on LANs. On a network using NIS, each host client or server has information about the entire system. A user at a host can access files or applications on any host in the network with a single username and password. NIS is similar to the Domain Name System (DNS) used on the Internet, only simpler. See also **DNS**; **NIS+**.

NIS+

A later version of the Network Information Service (NIS) that provides additional security, hierarchical name spaces, and other improvements. See also **NIS**.

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 also **host**.

non-facility associated signaling

See **NFAS**.

nonvolatile RAM

See **NVRAM**.

nonvolatile random access memory

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.

null modem cable

A cable that joins computing devices directly to each other instead of over a network. You use a null modem cable to connect the console port or any asynchronous data terminal equipment (DTE) port on a PortMaster device to a terminal or other DTE.

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

object

In a database management system (DBMS), a specific instance of a class. An object contains real values instead of variables. Compare **class**.

object-oriented database

A database in which data is stored as objects in an object-oriented programming environment. See also **database**.

ODBC

Open database connectivity. A standard database access method developed by Microsoft Corporation to enable any application to access data handled by any database management system (DBMS). ODBC inserts a middle layer called a *database driver* between the application and the DBMS to translate the application's data queries into commands that the DBMS can recognize. Both application and DBMS must be ODBC-compliant—the application must be able to issue ODBC commands, and the DBMS must be able to respond to them.

ODI

Open Datalink Interface. A Novell specification that isolates the protocol stack from the network adapter drivers to provide hardware independence for network connectivity.

one-time password

A password that provides additional security for network access because it is used only once. Also known as a *dynamic password*, a one-time password is generated in encrypted form—via multiple iterations of a secure hash function—by software running on a user's computer or by a hardware device. The password is often based on a "seed" value sent by the server that provides access to the network, plus the user's secret pass phrase. The server runs software that calculates the same encrypted password. The passwords produced by the generator and the server must match before the user is granted access to the network. Users who do not have the algorithm of the device for generating the encrypted response cannot access the network. See also **ActivCard**; **CHAP**; **SecurID**; **token**.

open database connectivity

See **ODBC**.

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**.

Open Systems Interconnection

See **OSI**.

OSI

Open Systems Interconnection. An ISO standard for worldwide communications that defines a framework for the common functions in a telecommunications system. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom (physical) layer, over the channel to the next station and back up the hierarchy. Instead of serving as the universal standard as originally intended, the OSI standard serves as the model for designing and understanding networking products and protocols.

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.

out-of-band signaling

The transmission of signaling information over a different path from data and/or voice information. Compare **in-band signaling**.

outsourcer

A company that purchases goods and/or services for its customers and/or employees from an outside or third-party company known as a *wholesaler*. For example, an Internet service provider (ISP) or enterprise can purchase remote access services from another ISP or a telephone company. See also RAO.

P

packet

A unit of data sent across a network, usually containing a header that has an address and other identifying information.

packet switching

A technology for sending data over a network—the Internet, for example. The data that comes out of a connected device is broken into chunks called *packets*. Each packet contains the address of its origin (source) and the address of its destination. Data packets from many different sources can travel along the same lines and be sorted and directed through different routes by routers along the way. When all the packets forming a message arrive at the destination, they are recompiled into the original message. Most modern WAN protocols are based on packet switching technology. In contrast, normal telephone service is based on circuit switching, which allocates a dedicated line for transmission between two parties.

PAP

Password Authentication Protocol. An authentication protocol that allows the network access server to authenticate the user. 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 it identifies the remote end of the connection. 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).

parse

To divide character strings into components based on punctuation and other characteristics for further analysis.

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 **autonomous system path list**; **destination; route**.

PCMCIA

Personal Computer Memory Card International Association. An international body and trade association that establishes standards for integrated circuit cards called *PCMCIA cards*—or *PC cards*. These are credit-card-sized devices that expand the capability of a portable computer or other device to include more memory, modems, or a portable disk drive. For example, the PortMaster PCMCIA Office Router features a slot for a PCMCIA card that allows the use of V.34 or V.32bis PCMCIA modems.

peer

A router running BGP that the PortMaster running BGP communicates with via open messages, notification messages, update messages, and keepalive messages. A PortMaster can have both internal and external peers. See also **external peer**; **internal peer**.

Perl

Practical extraction and report language. An interpreted language developed by Larry Wall and distributed free over USENET. Perl version 5 (Perl5) includes object-oriented programming facilities and is a useful programming tool for the World Wide Web, UNIX system administration, and many other applications. Perl5 provides a more concise and readable way to do many system management tasks that were formerly accomplished by C programs or shell programs. Perl uses sophisticated pattern matching techniques to quickly scan large text files, extract information, and print reports. Although optimized for scanning text, Perl also handles binary data and can make **dbm** files look like associative arrays.

Perl5 regular expression

The most obvious very high-level feature of Perl. A single simple pattern match in Perl can perform the work of many lines in a different language. Regular expressions identify strings and help parse their contents using regular expression memory, most often with the regular expression memory variables $1, $2, $3, and so on. These variables are associated with parentheses inside a regular expression that can identify what its contents matched. Perl5 regular expressions are constructed and parsed by means of grammatical rules and operators that are similar to those used for arithmetic expressions. See also **regular expression**.

permanent virtual circuit

See **PVC**.

Personal Computer Memory Card International Association

See **PCMCIA**.

physical circuit

A physical connection between two devices.

ping

Packet Internet Groper. A program used to test and debug networks. Ping sends an Internet Control Message Protocol (ICMP) echo request packet to the specified host and waits for an echo reply packet. Ping reports success or failure and sometimes statistics about its operation.

PKIX

Public key infrastructure using X.509. A set of standards for an Internet public key infrastructure (PKI) that uses the ISO X.509 authentication standard. A PKI defines data formats and procedures for distributing and managing cryptographic keys via certificates digitally signed by certification authorities.

plain old telephone service

See **POTS**.

PMVision™

A Java-based graphical user interface (GUI) for monitoring, managing, debugging, and configuring PortMaster products.

point of presence

See **POP**.

Point-to-Point Protocol

See **PPP**.

Point-to-Point Tunneling Protocol

See **PPTP**.

policy

In BGP, the rule or set of rules a PortMaster product 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**.

POP

1) Point of presence. The location of a switching dial-in facility, usually for a long-distance telecommunications provider or an Internet service provider (ISP). Also, a local telephone number through which you can access your ISP. 2) Post Office Protocol. An extensible protocol for retrieving email from a remote server.

port

1) On a computer, the physical channel or connection through which data flows. 2) In a TCP/IP or UDP network, a numbered end point to a logical connection that determines the way a client application program specifies a particular server application on the network. Higher-level applications have ports with numbers preassigned by the Internet Assigned Numbers Authority (IANA)—for example, HTTP is assigned port 80, and RADIUS is assigned port 1645. These "well-known" ports are listed in RFC 1700, *Assigned Numbers*.

port limit

The number of ports to which a RADIUS user is permitted to be concurrently connected.

PortMaster®

The name of a family of remote access server and router products designed and manufactured by Lucent Technologies.

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.

Post Office Protocol

See **POP**.

POTS

Plain old telephone service. The analog dial-tone-type telephone networks and services in place worldwide, with transmission rates up to 52Kbps. In contrast, telephone services based on digital communications lines, such as ISDN and Fiber Distributed Data Interface (FDDI), have higher speeds and bandwidths. The POTS network is also called the *public switched telephone network (PSTN).*

PPP

Point-to-Point Protocol. A protocol that provides connections between routers and between hosts and networks over synchronous and asynchronous circuits. PPP was designed to work with network layer protocols like IP, IPX, and AppleTalk Remote Access (ARA) protocol, and relies on the Link Control Protocol (LCP) and Network Control Protocol (NCP). PPP also has built-in security mechanisms such as the Challenge Handshake Authentication Protocol (CHAP) and Password Handshake Authentication Protocol (PAP). See also **SLIP**.

PPTP

Point-to-Point Tunneling Protocol. A protocol developed by Microsoft Corporation and similar to the Layer 2 Forwarding (L2F) protocol developed by Cisco Systems. PPTP supports the creation of secure virtual private networks (VPNs) over the Internet. Cisco and Microsoft recently agreed to merge their protocols into a single standard called *Layer Two Tunneling Protocol (L2TP)*. See **L2TP**.

PRI

Primary Rate Interface. The ISDN interface to primary rate access. Primary rate access consists of a single 64Kbps D channel—plus 23 64Kbps B channels on a T1 line, or 30 64Kbps B channels on an E1 line—for voice, data, and other services. 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 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.

Proxy Address Resolution Protocol

See **Proxy ARP**.

Proxy ARP

A variation of the Address Resolution Protocol (ARP) 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**.

proxy service

A service that enables access requests to be forwarded to other servers—either directly or through intermediary servers—for authentication and, optionally, authorization.

PSTN

Public switched telephone network. See **POTS**.

public key infrastructure

See **PKIX**.

public switched telephone network

See **POTS**.

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.

Q

QoS

Quality of service. An indicator of the performance of a transmission system on the Internet and other networks. QoS is measured in transmission rate, error rates, latency, and other characteristics, and can to some extent be guaranteed to a customer in advance. Asynchronous Transfer Mode (ATM) technology supports QoS levels.

quality of service

See **QoS**.

query language

A set of rules for constructing queries to a database.

R

RADIUS

Remote Authentication Dial-In User Service. A client-server security protocol invented by the business unit of Lucent Technologies formerly known as Livingston Enterprises, Inc.

RADIUS accounting

The server component of RADIUS that monitors and records attempted and successful user connections. RADIUS accounting data includes RADIUS usernames, start and stop times, connection status, IP address of the network access server, network access server port, and IP address of the user (framed IP address).

RADIUS authentication

The process by which the server determines whether a user requesting access is legitimate. If a user is authenticated, his access request is forwarded for authorization.

RADIUS authorization

The process by which the RADIUS server handles an access request made by an authenticated user. RADIUS determines whether the user is authorized to receive the service(s) requested.

RADIUS dictionary

A RADIUS file used to parse access requests and generate responses. The dictionary lists all valid attribute-value pairs and specifies the data type required for the values.

RADIUS user

A person to whom a RADIUS service is provided after his or her identity is authenticated and session is authorized by RADIUS.

RAO

Remote access outsourcing. The practice whereby one service provider or enterprise, known as an *outsourcer*, purchases remote access services from another service provider, or *wholesaler*. The wholesaler physically terminates the dial-up access lines---telephone, ISDN, digital subscriber line (DSL), or other circuits---of one or more outsourcers and provides each outsourcer with a private dial-up network. The outsourcer is the end point for a session. The wholesaler can maintain the remote access equipment on the outsourcer's premises or can integrate the equipment into its own network, and often provides the outsourcer with tools for viewing resources. The wholesaler's equipment can be statically partitioned among outsourcers, or can dynamically allocate its ports to outsourcers as needed. RAO is also known as *wholesaling*.

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**.

RAS

See **remote access server**.

RBHC

See **RBOC**.

RBOC

Regional Bell operating company. One of the seven regional telephone companies created by the breakup of AT&T in 1984. Each owns two or more local telephone companies called *Bell operating companies (BOCs)*. RBOCs are also known as *Baby Bells* or *regional Bell holding companies (RBHCs)*, and more generally as *local exchange carriers (LECs)*. See also **LEC**.

RDBMS

Relational database management system. A DBMS that stores data in the form of related tables. Relational databases require few assumptions about how data is related or how it is extracted from the database, enabling the database to be viewed in many different ways. In contrast to flat-file databases, which consist of a single table, a relational system can spread the database over several tables. Most full-scale database systems are structured as an RDBMS. Small database systems often use other designs that provide less flexibility in posing queries.

record

In a database management system (DBMS), a complete set of information that constitutes a single entry in a database table. Records are composed of fields, each of which contains one item of information. In a typical database, a set of records constitutes a file. For example, a personnel file might contain records that have three fields: a name field, an address field, and a telephone number field.

redundant

Serving as a duplicate component to prevent failure of a system. When one component fails, the redundant one takes over its functions without interrupting service. For example, the optional third AC power supply on a PortMaster 4 is redundant because it is not required for normal operation unless one of the two required AC power supplies fails. Redundancy generally improves reliability. Compare **hot-swappable**.

regional Bell holding company

See **RBOC**.

regional Bell operating company

See **RBOC**.

regular expression

A powerful tool for matching patterns to manipulate text and data. Regular expressions are generally included as part of a larger utility—for example, **grep**—and are found in scripting languages (including Perl, Tcl, awk, and Python), editors (including Emacs, **vi**, and Nisus Writer), programming environments (including Delphi and Visual C++), and specialized tools (including **lex**, Expect, and **sed**). See also **Perl5 regular expression**.

relational database

A tabular database in which data is defined so that it can be reorganized and accessed in a number of different ways. See also **database**; **RDBMS**.

relational database management system

See **RDBMS**.

remote access outsourcing

See **RAO**.

remote access server

Any device that enables multiple remote users to access a network. PortMaster 2 and PortMaster 3 products are remote access servers. A remote access server is sometimes called a *RAS*—or a *network access server (NAS)*. Compare **communications server**.

Remote Authentication Dial-In User Service

See **RADIUS**.

remote method invocation

See **RMI**.

remote office/branch office

See **ROBO**.

reply item

A component of a RADIUS user profile that the RADIUS server sends one or more of to the network access server to specify a user's connection when all check items in the profile have been satisfied by the access-request. See also **check item**; **SHA-1**.

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 vector-state protocol used for the transmission of IP or IPX routing information. RIP uses hop count as the only metric for determining the best path.

rlogin

Remote login. A terminal emulation program, similar to Telnet, offered in most UNIX implementations. The **rlogin** program uses the local terminal type given in an environment TERM variable as the remote terminal type.

RMI

Remote method invocation. A Java application programming interface (API) that enables a program running on one computer to call the methods of an object running on a remote computer.

roaming

A service that enables two or more Internet service providers (ISPs) to allow one another's users to dial in to any member ISP's network for service. Users traveling outside their normal area of service are provided service through another ISP.

ROBO

Remote office/branch office. An end-user segment of the internetworking market. See also **SOHO**.

route

A way for a packet to reach its target via the Internet. For example, 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 network layer device that links one network to another. Routers forward packets between networks along optimal paths. The Internet is made up of thousands of routers sending and receiving packets to and from one another. In contrast to servers, which also run routing services, routers provide service to networks rather than to client devices or software. See also **access router**; **routing table**.

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. 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, control signals, and clock signals.

RSA

Rivest-Shamir-Adelman. A public key encryption and authentication technology that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm, especially for data sent over the Internet. The technology is owned by RSA Data Security, Inc., now a subsidiary of Security Dynamics.

runt packet

A packet below the minimum size. On an Ethernet network, a runt packet has 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**.

scalable

Able to be changed in size or configuration to suit changing conditions. For example, a scalable network can be expanded from a few nodes to thousands of nodes.

schema

In a database management system (DBMS), a collection of objects that are available to a user. Schema objects are the logical structures that directly refer to the data in a database. Schema objects include such structures as tables, views, sequences, stored procedures, synonyms, indexes, clusters, and database links.

secret

See **shared secret**.

secure hash algorithm

See **SHA-1**.

Secure Sockets Layer

See **SSL**.

SecurID

An authentication system available from Security Dynamics, Inc. SecurID uses tokens and a software server to generate and confirm one-time passwords to identify users and grant or deny them network access.

selector

In a database management system (DBMS), a string used to identify a value in a database.

Serial Line Internet Protocol

See **SLIP**.

serial port

A bidirectional channel through which data flows one bit as a time. Asynchronous serial ports most often use 10 bits for a character of data including 1 start bit, 8 data bits, and 1 stop bit.

server

A computer or software program that provides one or more services to a client computer or software.

Service Advertisement Protocol

See **SAP**.

service profile identifier

See **SPID**.

SHA-1

Secure hash algorithm. An iterative cryptographic hash function for message authentication. See also **MD5**.

shared secret

A character string specified on both a server and another device or server that establishes mutual identification. A shared secret is required for RADIUS and ChoiceNet clients as well as for proxy, or remote, servers. The shared secret is used to encrypt the user's password so it does not travel across the network in clear text. The server in turn uses the shared secret to decrypt the password upon receipt.

shielded twisted pair

See **STP**.

Simple Mail Transfer Protocol

See **SMTP**.

Simple Network Management Protocol

See **SNMP**.

site list

A list of sites—each specified by its IP address or fully qualified domain name—used by a ChoiceNet filter instead of individual source or destination host addresses to permit or deny access by users.

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 that was made obsolete by Point-to-Point Protocol (PPP), for point-to-point serial connections using TCP/IP. See also **PPP**.

small office/home office

See **SOHO**.

SMDS

Switched Multimegabit Data Service. An emerging high-speed packet switched public data communications service for exchanging large amounts of data over a WAN on a nonconstant or "bursty" basis. SMDS provides an architecture and services for connecting geographically separate LANs into a WAN without a dedicated private line. SMDS is expected to be widely used by telephone companies as the basis for their data networks.

SMTP

Simple Mail Transfer Protocol. A protocol, defined in RFC 821, for exchanging email messages between servers across a network. SMTP is the principle protocol for sending email over the Internet.

SNMP

Simple Network Management Protocol. A protocol, defined in RFC 1157, for communicating between management consoles and network devices.

SOHO

Small office/home office. An end-user segment of the internetworking market. See also **ROBO**.

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*. See also **peer**.

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.

SQL

Structured query language. A language conforming to ISO and American National Standards Institute (ANSI) standards that is used to create, maintain, and query relational databases. SQL is not a full-fledged language that can create standalone applications, but is often embedded within other programming languages. SQL uses plain English words for many of its commands, making it easy to use. Although different database applications have their own versions of SQL to implement their unique features, all SQL-capable databases support a common subset of SQL. SQL supports distributed databases so that several users on a LAN can access the same database simultaneously.

SSL

Secure Sockets Layer. A program layer and protocol designed by Netscape Communications to enable encrypted and authenticated communications across the Internet. Many websites use SSL protocol to obtain confidential user information. SSL uses a public and private key encryption system from RSA Data Security, Inc., which includes use of a digital certificate.

Stac LZS data compression

A data compression algorithm for efficiently compressing packets encapsulated for the Point-to-Point Protocol (PPP). Based on the Lempel-Ziv compression algorithm, the Stac LZS data compression algorithm, described in RFC 1974, supports all file types and both single and multiple compression histories.

station

See **host**.

S/T interface

The connection for the ISDN Basic Rate Interface (BRI) switch type used in Japan, Europe, and other countries using international ISDN standards. In contrast, the United States and the rest of North America use the U interface. See also **U interface**.

STP

Shielded twisted pair. A two-pair wiring medium used in a variety of network implementations. STP cable has a layer of shielded insulation to reduce electromagnetic interference. See also **twisted pair**; **UTP**.

structured query language

See **SQL**.

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.

subclass

A class subordinate to another class—known as a *superclass*—that inherits some or all of the characteristics of the superclass. Subclasses can also define their own methods and variables that are not contained in their superclasses. See also **class**.

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 or X.25 connection. The call creates a virtual circuit between the originator and the party called.

Switched Multimegabit Data Service

See **SMDS**.

switched virtual circuit

See **SVC**.

synchronous

Occurring at the same time or at regular intervals established by a synchronized timing signal. In synchronous communication, the receiver and transmitter are synchronized, either within the data signal or by a separate clock signal, so that data is sent at a fixed rate. Data is transmitted in a block—as an entire message or frame—rather than one character at a time. Synchronous communication is faster and more efficient than asynchronous communication, but is generally more complex and expensive. Synchronous WAN ports on a PortMaster router or access concentrator provide high-speed dedicated connections between two remote LANs over leased lines, Frame Relay, switched 56Kbps lines, or ISDN lines. Compare **asynchronous**.

syslog

1) The process that handles system messages by reading and forwarding them to a log file or users depending on the priority of the message and the system facility that originated the message. 2) The log file created by the **syslog** process.

sysop

System operator. A person responsible for the day-to-day operation of a computer system or network resource—for example, server, LAN, bulletin board system (BBS), online service, or special interest group (SIG).

system operator

See **sysop**.

T

T1

A leased line digital WAN carrier system for transmitting data formatted for digital signal level 1 (DS-1) at 1.544Mbps through the telephone-switching network, using alternate mark inversion (AMI) or bipolar 8-zero substitution (B8ZS) coding. The system uses four wires and provides full-duplex communication—two wires for receiving and two for sending simultaneously. The wires can be twisted pair copper wire, coaxial cable, optical fiber, or other media. Compare **E1**; **T3**.

T3

A leased line digital WAN carrier system for carrying data formatted for digital signal level 3 (DS-3) at 44.736Mbps—about 40 times the speed of a T1 line. T3 transmissions support full-screen, full-motion video. Compare **T1**.

table

A collection of records arranged in rows and columns in a relational database. In relational database management systems (RDBMs), all user-accessible information is stored in tables.

TCP/IP

Transmission Control Protocol/ Internet Protocol. 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.

telco

Telephone company.

Telnet

The Internet standard protocol, described in RFC 854, for remote terminal connection service.

terabyte

A data measurement unit equal to 1,000 gigabytes or one trillion bytes.

terminal

A device from which you send commands to a remotely located computer, usually via a serial interface. A terminal at minimum consists of a keyboard, a display screen, and some simple circuitry. Early terminals were called *teletypes (ttys)*; later versions were known as *video display terminals (VDTs)*. Currently, terminal software in an intelligent PC or workstation at a network node can emulate a physical terminal and allow you to type commands to a remote computer. As the Internet grows in size and intelligence, simple terminals that support only communications and a browser might become the primary access to the World Wide Web.

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 or workstation screen and keyboard act like the video display terminal (VDT) 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.

token

A small hand-held device that generates dynamic or one-time passwords for user authentication. Some tokens generate a response to a challenge entered by the user. Other tokens are synchronized with the security server and independently generate a matching password on request. See also **ActivCard**; **SecurID**.

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**.

Transmission Control Protocol/Internet Protocol

See **TCP/IP**.

triple data encryption standard

See **3DES**.

Trivial File Transfer Protocol

See **TFTP**.

tty

1) A primitive teletypewriter terminal with a mechanical printer, limited character set, and poor print quality. 2) A UNIX command that displays the name of the current controlling terminal. 3) In UNIX systems, any terminal. 4) In UNIX systems, the serial communications (hardware) port on a computer.

twisted pair

Relatively low-speed transmission medium consisting of two insulated wires—shielded or unshielded—in regular spiral patterns. The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Twisted pair is common in telephone wiring and is increasingly common in data networks. It is used for 10BaseT Ethernet connections with RJ-45 connectors. See also **STP**; **UTP**.

two-way

Relating to a port configuration on the PortMaster 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. See also **S/T interface**.

UNI

User-Network Interface. 1) An interface point between Asynchronous Transfer Mode (ATM) end users and a private ATM switch, or between a private ATM switch and the public carrier ATM network; defined by physical and protocol specifications in ATM Forum UNI documents. 2) A similar connection in a Frame Relay network. 3) The interoperability standard adopted by the ATM Forum to define connections between users or end stations and a local switch. See also **ATM**; **ATM Forum**.

uniform resource locator

See **URL**.

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**.

unshielded twisted pair

See **UTP**.

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 **keepalive message**; **notification message**; **open message**; **route**.

URL

Uniform resource locator. The address of a file (resource) accessible on the Internet. The type of resource depends on the Internet application protocol. For the World Wide Web's protocol, the Hypertext Transfer Protocol (HTTP), the resource can be an HTML page, a program such as a Java applet, or any other file supported by HTTP. The URL contains the name of the protocol required to access the resource, a domain name that identifies a specific computer on the Internet, and, if necessary, a path to the resource on the computer.

user

See **RADIUS user**.

User Datagram Protocol

See **UDP**.

User-Network Interface

See **UNI**.

UTP

Unshielded twisted pair. A four-pair wire medium used in a variety of networks. UTP does not require the fixed spacing between connections necessary with coaxial connections. The five grades of UTP cable commonly used are Category 1 through Category 5; Category 5 can carry the most data. See also **STP**; **twisted pair**

UUCP

UNIX-to-UNIX Copy Program. Interactive communication system for connecting two UNIX computers to send and receive data.

V

V.25bis

An ITU-T standard for data transmission that defines how to dial on synchronous devices such as ISDN or switched 56Kbps.

V.32bis

An ITU-T standard for data transmission via modems 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 for data transmission via modems that allows data rates as high as 28.8Kbps.

V.35

An 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.

V.90

An ITU-T standard for data transmission via modems at 56Kbps. The V.90 standard resolves the difference between two modem technologies—X2 and K56flex. Both technologies now conform to V.90, and most previously manufactured 56Kbps modems can support V.90 via a software upgrade. See also **K56flex**.

V.110

An ITU-T standard for performing asynchronous rate adaptation into ISDN over a 64Kbps line. The PortMaster supports 9600bps and 19,200bps over this older standard that allows pre-ISDN devices to be adapted for ISDN.

V.120

An ITU-T standard for performing asynchronous rate adaptation into ISDN.

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 for 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 LAN

See **VLAN**.

virtual port

In Multichassis PPP, a port corresponding to the physical port of the slave.

virtual private data network

See **VPN**.

virtual private dial-up network

See **VPN**.

virtual private network

See **VPN**.

Virtual Terminal Protocol

See **VTP**.

VLAN

Virtual LAN. A group of devices on one or more LANs that communicate as if they were connected to the same wire even though they are physically located on different LAN segments. Because VLANs are configured through software rather than hardware, they are extremely flexible.

VLSM

Variable-length subnet mask. A means of specifying a different subnet mask for the same network number on different subnets. VLSMs often allow addresses to be assigned more efficiently. OSPF and BGP support classless or VLSM routes.

voice over IP

See **VoIP**.

VoIP

Voice over IP. A category of hardware and software that allows people to use the Internet as the transmission medium for telephone calls. Currently, VoIP does not offer the same quality of telephone service as direct telephone connections. VoIP is also known as *Internet telephony* and *Voice over the Internet (VOI)*.

VoIP Forum

A subgroup of the International Multimedia Teleconferencing Consortium (IMTC) that develops standards for Internet telephony. The VoIP Forum plans to define technical guidelines for two-party voice and other audio communications for compatibility with traditional telephone service networks via telephony and/or IP gateways.

VPDN

Virtual private dial-up network or virtual private data network. See **VPN**.

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.

VTP

Virtual Terminal Protocol. An ISO application for establishing a virtual terminal connection across a network. VTP provides terminal emulation that allows a computer system to appear to a remote system as if it were a directly attached terminal.

W

WAN

Wide area network. A 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**.

wide area network

See **WAN**.

World Wide Web

All the resources and users on the Internet that are using the Hypertext Transport Protocol (HTTP). The Web is made up of thousands of HTTP servers that enable text, graphics, and sound files to be mixed together and provided to users requesting access and download capability via connections to the Internet.

WWW

See **World Wide Web**.

Command Index

Subject Index

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W