

PortMaster®

Command Line Reference

Lucent Technologies

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

May 2000

950-1184H

Copyright and Trademarks

© 1996, 1997, 1998, 1999, 2000 Lucent Technologies Inc. All rights reserved.

PortMaster, ComOS, and ChoiceNet are registered trademarks of Lucent Technologies Inc. PMVision, 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

About This Reference

Audience	viii
PortMaster Documentation	viii
Additional References	ix
RFCs	ix
Books	xi
Document Conventions	xiii
Document Advisories	xiv
Contacting Lucent NetworkCare Technical Support	xiv
For the EMEA Region	xiv
For North America, CALA, and the Asia Pacific Region	xv
PortMaster Training Courses	xv
Subscribing to PortMaster Mailing Lists	xv

1. Introduction

Accessing the Command Line Interface	1-1
Rebooting a PortMaster	1-2

2. General Commands

Summary of General Commands	2-1
General Commands	2-4

3. Global Commands

Displaying Global Information	3-1
Summary of Global Commands	3-1
Global Commands	3-3

RADIUS Client Commands	3-24
ChoiceNet Client Commands	3-33
SNMP Commands	3-35
4. Ethernet Interface	
Displaying Ethernet Information	4-1
Summary of Ethernet Commands	4-2
Ethernet Commands	4-3
Ethernet Subinterface Commands	4-13
5. Asynchronous Ports	
Displaying Asynchronous Port Information	5-1
Summary of Asynchronous Commands	5-2
Asynchronous Port Types	5-4
Asynchronous Commands	5-5
Modem Commands	5-49
6. Synchronous Ports	
Displaying Synchronous Port Information	6-1
Summary of Synchronous Port Commands	6-2
Synchronous Commands	6-3
7. Users	
Displaying User Information	7-1
Summary of User Commands	7-2
User Commands	7-4
8. Locations and DLCIs	
Displaying Location Information	8-1
Summary of Location Commands	8-1
Location Commands	8-4
DLCI Commands	8-33

9. Parallel Port

Displaying Parallel Port Information	9-1
Summary of Parallel Port Commands	9-1
Parallel Port Commands.	9-2

10. Hosts

Displaying Host Information	10-1
Summary of Host Commands	10-1
Host Commands.	10-2

11. ISDN BRI Ports

Displaying ISDN Port Information	11-1
Summary of ISDN BRI Commands	11-1
ISDN BRI Commands.	11-4

12. T1, E1, and PRI

Displaying T1, E1, and PRI Diagnostic Information	12-2
Summary of T1, E1, and PRI Commands.	12-3
T1, E1, and PRI Commands	12-4

13. Filters

Displaying Filter Information.	13-1
Summary of Filter Commands.	13-2
Filter Commands	13-4

14. NAT

Displaying NAT Information	14-1
Summary of NAT Commands	14-2
NAT Commands.	14-3

15. L2TP

Displaying L2TP Diagnostic Information	15-1
Summary of L2TP Commands	15-2

L2TP Commands	15-2
16. Routing	
Displaying Routing Information.	16-1
Summary of Routing Commands.	16-1
General Routing Commands	16-3
Static Routing Commands	16-14
RIP Commands	16-18
Netmask Commands	16-22
Routing Information Commands	16-25
17. OSPF Routing	
Displaying OSPF Information.	17-1
Summary of OSPF Commands.	17-2
OSPF Commands	17-4
18. BGP Routing	
Displaying BGP Information	18-1
Summary of BGP Commands	18-2
BGP Commands	18-4
19. Debug	
Summary of Debug Commands	19-1
Debug Commands	19-2
A. Configurable Ports	
B. Basic Commands	
C. Command Values	
D. TCP and UDP Ports and Services	
Command Index	
Subject Index	

About This Reference

The *PortMaster® Command Line Reference* documents the ComOS® command line interface available on the PortMaster products of Lucent Technologies. This reference provides descriptions of the ComOS commands you use to configure, monitor, and debug your PortMaster. For more detailed information on how to use these commands, see the *PortMaster Configuration Guide*, the *PortMaster Routing Guide*, and the *PortMaster Troubleshooting Guide*.

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

Before attempting to configure your PortMaster with the command line interface, refer to your hardware installation guide for information about attaching a console.



Note – The PortMaster Office Router OR-AP is shipped with its own version of ComOS and does not use the same version as the other PortMaster Office Routers.

PMVision™ Interface. You can also configure the PortMaster with the PMVision graphical user interface (GUI) for Microsoft Windows, UNIX, and other platforms supporting the Java Virtual Machine (JVM). PMVision replaces the PMconsole™ interface to ComOS.

PMVision is a companion to the command line interface. 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 includes online help. See the *PMVision User's Guide* for more information.

Release Specific Information. The ComOS 3.9 information in this manual might not be supported by your PortMaster. Check the release notes at <http://www.livingston.com/tech/docs/release/> to find out whether your PortMaster can run ComOS 3.9 commands, keywords, and features.

The PortMaster 4 only runs ComOS 4.0 and later. See the *PortMaster 4 User Manual* for more information.

Audience

This reference is designed to be used by qualified system administrators and network managers.

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.

- *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.	<ul style="list-style-type: none">• Enter version to display the version number.• Press Enter.• Open the permit_list file.
<i>Italic font</i>	Identifies a command-line placeholder. Replace with a real name or value.	<ul style="list-style-type: none">• set <i>Ether0</i> address <i>Ipaddress</i>• Replace <i>Area</i> with the name of the OSPF area.
Square brackets ([])	Enclose optional keywords and values in command syntax.	<ul style="list-style-type: none">• set nameserver [2] <i>Ipaddress</i>• set <i>S0</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	set syslog <i>Logtype</i> {[disabled] [<i>Facility.Priority</i>]}
Vertical bar ()	Separates two or more possible options in command syntax.	<ul style="list-style-type: none">• set <i>S0 W1</i> ospf on off• set <i>S0</i> host default prompt <i>Ipaddress</i>

Document Advisories



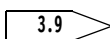
Note – means take note. Notes contain information of importance or special interest.



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.



Release note information—means this command, keyword, or feature was introduced in the ComOS version shown.

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 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>**.

The ComOS command line interface described in this reference can be used to administer any PortMaster Communications Server (PM-2 series), Internetwork Router (IRX™ series), Office Router (OR series), or Integrated Access Server (PM-3 series). When the name *PortMaster* is used in this reference, it can refer to any of these PortMaster products.

For information about the PortMaster 4 Integrated Access Concentrator (PM-4 series), see the *PortMaster 4 User Manual*.

This chapter describes how to start the command line interface and reboot the PortMaster.

Accessing the Command Line Interface

The command line interface can be used to configure your PortMaster ports. Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1 lists the configurable ports by PortMaster model.

To access the command line interface:

- 1. Connect via Telnet to the PortMaster or connect to an asynchronous port, and log in as follows:**

```
Login: !root
Password: Password
Command>
```

Password is the PortMaster administrative password.



Note – If you are unable to log in to your PortMaster, refer to the troubleshooting section in your hardware installation guide. For more information, refer to the *PortMaster Configuration Guide* and to the *PortMaster Troubleshooting Guide*.

Table B-1, “Basic PortMaster Commands,” on page B-1 lists the basic PortMaster commands. Some are complete commands; most require additional keywords or values as described in following chapters.

2. **Configure your PortMaster, referring to the port-specific, protocol-specific, or table-specific chapters in this reference and the *PortMaster Configuration Guide*.**

Rebooting a PortMaster

After configuring the following settings, you must reboot the PortMaster to activate them. You must also reboot after erasing the configuration in nonvolatile RAM or after loading software from nonvolatile RAM.

- ISDN switch provisioning or type—**set isdn-switch**
- Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP) routing—**set bgp enable | disable** or **set ospf enable | disable**
- Simple Network Management Protocol (SNMP)—**set snmp on | off**
- IPX protocol—**set ipx on | off**
- Base address and size of assigned IP address pools—**set assigned_address** *Ipaddress* and **set pool** *Number*
- Any ISDN Primary Rate Interface (PRI) line setting—**set line0 | line 1**
- Multichassis Point-to-Point Protocol (PPP)—**set endpoint** *Hex*
- ISDN Basic Rate Interface (BRI) network hardwired port for leased line ISDN—**set S10 network hardwired**

To reboot, enter the following command:

Command> **reboot**

Rebooting performs a software restart that takes approximately 30 seconds. This process resets all active ports to their saved configurations, disconnecting all active sessions. Any changes made since a **save** command was last issued are lost when you reboot, unless you first save them.

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of General Commands

Table 2-1 lists commands for troubleshooting, general administration, and displaying the configuration of the PortMaster. Definitions of general administration commands and **show** commands follow the table. For other **show** command definitions, see the pages indicated in the table.

Table 2-1 General Commands

Command Syntax	
dial <i>Locname</i> [-x]	- see page 2-4
done, quit, exit	- see page 2-5
erase all-flash comos configuration	- see page 2-6
erase file <i>String</i>	- see page 2-6
erase partition <i>Number</i>	- see page 2-6
help [<i>CommandName</i>]	- see page 2-7
ifconfig [<i>Interface</i>] [address <i>Ipaddress</i>] [netmask <i>Ipmask</i>] [destination <i>Ipaddress(dest)</i>] [ipxnet <i>Ipxnetwork</i>] [ipxframe ethernet_802.2 ethernet_802.3 ethernet_802.2_ii ethernet_ii] [up] [down] [private] [-private]	- see page 2-9
ping [<i>Ipaddress</i>]	- see page 2-11
pmlogin <i>Ipaddress</i>	- see page 2-12
ptrace [<i>Filtername</i>] [extended dump Bytes]	- see page 2-13
reboot	- see page 2-15
reset all bgp console dialer dNumber 12tp MO nat nHandle nic ospf p0 propagation S0 S10 V0 W1	- see page 2-15

Table 2-1 General Commands (Continued)

Command Syntax	
rlogin <i>Ipaddress</i>	- see page 2-17
save all <i>S0 S10 W1</i> global console filter host location map netmask p0 ports route snmp user ospf bgp	- see page 2-18
set console <i>[S0 p0]</i>	- see page 2-20
set debug	- see page 19-5
set sysname <i>[String]</i>	- see page 2-21
show all	- see page 2-22
show arp <i>Interface</i>	- see page 2-24
show bgp memory	- see page 18-43
show bgp next-hop	- see page 18-44
show bgp paths <i>[Prefix/NM [verbose]]</i>	- see page 18-46
show bgp peers <i>[verbose packets]</i>	- see page 18-49
show bgp policy <i>[Policyname]</i>	- see page 18-55
show bgp summarization <i>[all]</i>	- see page 18-56
show Ether0	- see page 4-11
show files	- see page 2-25
show filter ipxfilter sapfilter <i>Filtername</i>	- see page 13-24
show global	- see page 2-28
show ipxroutes	- see page 16-25
show isdn <i>dNumber S0</i>	- see page 11-15
show l2tp global sessions stats tunnels	- see page 15-9
show Line0	- see page 12-23
show location <i>Locname</i>	- see page 8-29
show M0	- see page 12-27
show mcppp	- see page 12-29
show memory	- see page 2-31

Table 2-1 General Commands (Continued)

Command Syntax	
show modems	- see page 12-30
show modem <i>ModemName</i>	- see page 5-49
show modules	- see page 2-32
show netconns	- see page 2-33
show netstat	- see page 2-34
show ospf areas	- see page 17-21
show ospf links [<i>router network summary external nssa</i>]	- see page 17-24
show ospf neighbor	- see page 17-27
show routes [<i>String Prefix/NM</i>]	- see page 16-27, page 17-29, page 18-58
show pots	- see page 3-23
show propagation	- see page 16-26
show route to-dest <i>Ipaddress</i>	- see page 16-29
show S0 S10 p0	- see page 2-35
show sap	- see page 2-38
show sessions	- see page 2-39
show syslog	- see page 2-40
show table	- see page 2-41
bgp filter host location modem netmask ospf sa sec-profile snmp subinterface user	
show user <i>Username</i>	- see page 7-25
show W1	- see page 6-24
telnet <i>Ipaddress</i> [<i>Tport</i>]	- see page 2-42
tftp get [<i>comos</i>] <i>Ipaddress String</i>	- see page 2-43
tracert [<i>Ipaddress</i>]	- see page 2-44
version	- see page 2-45

General Commands

The general commands are described in this section.

dial

This command initiates dialing to a network location.

dial *Locname* [-x]

Locname Name of location to dial.

-x Displays send and expect strings during dialing. Also resets some debugging values previously set with **set debug**.

Usage

This command is useful when you are testing a location configuration. Set the location to **manual**, set the console, and initiate a connection to a remote location using the **dial** command. You can watch the connection process to ensure that location-specific parameters are configured correctly.

Example

```
Command> set console

Command> dial loc1 -x
Starting dial to location loc1 using S1
send them (atdt5551212\r)
expect (CONNECT)
atdt5551212\r\r\nCONNECTgot it
send them (\r)
expect (ogin:)
38400\r\n\r\n\r\nserver login:got it
send them (john\r)
expect (ssword:)
john\r\nPassword:got it
send them (jogrtheyz\r)
```

```
expect      (PPP)
\r\nPPPgot it
Chat Succeeded - Starting PPP
LCP IPCP Open
Connection Succeeded
```

See Also

reset dialer - page 2-15

set console - page 2-20

set debug - page 19-5

done, quit, or exit

These commands exit the command line interface.

```
done
quit
exit
```

Usage

When you use these commands, the connection from your PC or terminal to the PortMaster is terminated. Depending on the PC or terminal software, a message usually appears to let you know that the connection to the PortMaster is lost.

Example

```
Command> quit
Goodbye...
```

erase

These commands erase all or part of the nonvolatile RAM in the PortMaster.

erase all-flash|comos|configuration

erase file *String*

erase partition *Number*

all-flash Erases all the nonvolatile RAM in the PortMaster, including the ComOS.

comos Removes the PortMaster ComOS, after which you can no longer boot from nonvolatile RAM.

configuration Erases configuration data, so that after the next reboot the PortMaster will be configured to the factory defaults.



Caution – In ComOS 3.8 through ComOS 3.8.x, using the **erase configuration** command also erases the **help** file. To download only the **help** file, use **pminstall**, *PMVision*, or the **tftp get** command.

file Erases a specified file from nonvolatile RAM.

String The name of the file to be erased; see **show files** on page 2-25 for filenames.

partition Use this keyword only when told to do so by Lucent technical support.

Number A partition number from 0 to 7.

Usage



Caution – Be very careful when you use this command. Refer to the *PortMaster Troubleshooting Guide* for troubleshooting information.

The erasure can take up to a minute to finish; wait until the erasure is complete before issuing any other commands.

Example

This example erases the configuration information stored in nonvolatile RAM, restoring the PortMaster to factory defaults.

```
Command> erase configuration  
Successfully erased FLASH configuration
```

help

These commands provide online help for the PortMaster commands.

help [*CommandName*]

CommandName One of the general commands listed in Table 2-1 on page 2-1.

Usage

If you type the **help** command without a command name, the online help shows a list of valid keywords, with descriptions. If you include a command name, a description or secondary keyword with description is shown.

ComOS 3.8 and later releases support context-sensitive help. Entering a question mark (?) at any point in the command line and pressing **Return** generates a list of keywords or values that can be entered at that point.

Examples

```
Command> set snmp ?
ON Off Readcommunity Writecommunity

Command> !! readcommunity ?
set snmp readcommunity ?
string256 NONE <CR>

Command> !! public
set snmp readcommunity public
SNMP read community changed to: public
```

Command> **help**

add	- Add entry to table	ptrace	- Trace packet traffic
attach	- Connect direct to port	quit exit	- Quit Console
delete	- Remove entry from table	reboot	- Restart the system
dial	- dial to a location	reset	- Reset session/port
erase	- Erase element of FLASH	rlogin	- Establish rlogin session
help	- list available commands	save	- Save current config
ifconfig	- View/configure interface	set	- Set configuration
ip ipx	- Sets the environment	show	- Show configuration
max pmconsole	- Pmconsole session limit#	telnet	- Establish Telnet session
tftp	- Transfer file from host	ping	- Send ICMP packet to Dest
tracert	- Use ICMP to detect route	pmlogin	- Establish PMD session
version	- Display ComOS version	!!	- Repeat last command

Command> **help add**

Valid add commands are:

```
filter - Add a new packet or access filter
host - Add a host to the local hosts table
route - Add a route to the static routing table
ipxroute - Add an IPX route to the static routing table
location - Add a new Dialnet dial-out location
snmp host - Add a host to the SNMP access list
netuser - Add a SLIP or PPP user to the password table
user - Add a login user to the password table
```

ifconfig

This command displays configuration values for all interfaces and allows you to modify active values.



Note – Enter this command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
ifconfig [Interface] [address Ipaddress] [netmask Ipmask]
[destination Ipaddress(dest)] [ipxnet Ipxnetwork]
[ipxframe ethernet_802.2|ethernet_802.3|ethernet_802.2_ii|ethernet_ii]
[up] [down] [private] [-private]
```

<i>Interface</i>	Interface specification—for example, ether0 , frm1 , or frmw1 .
<i>Ipaddress</i>	IP address of the interface.
<i>Ipmask</i>	Netmask for the interface IP address.
<i>Ipaddress(dest)</i>	IP address of the destination of a point-to-point connection.
<i>Ipxnetwork</i>	IPX network number of the interface.
ipxframe	Frame type used for sending IPX packets out of the Ethernet interface. Options include the four protocols that follow.
ethernet_802.2	Uses the Ethernet 802.2 protocol. This is the default encapsulation used by Novell NetWare Version 4.0.
ethernet_802.3	Uses the Ethernet 802.3 protocol. This is the default encapsulation used by Novell NetWare Version 3.11.
ethernet_802.2_ii	Uses the Ethernet 802.2_ii protocol. This encapsulation is not commonly used.
ethernet_ii	Uses the Ethernet II protocol. This is sometimes used for networks that handle both TCP/IP and IPX traffic.
up	Enables the interface.

down	Shuts down the interface.
private	Prevents routing information from being transmitted on this interface.
-private	Enables routing information to be broadcast on this interface by the Routing Information Protocol (RIP).

Usage

The **ifconfig** command allows you to view and change the active configuration of all network interfaces. The examples show **ifconfig** used to view the Ethernet parameters, and then change them. For more information, refer to the *PortMaster Configuration Guide*.

You can use **ifconfig** to modify the active Ethernet interface, but the change is only temporary until the next reboot.



Note – Changes made to the active Ethernet interface using the **ifconfig** command are not saved when you use the **save all** command. Therefore, Lucent recommends that you use the **set** commands followed by **save all** and **reboot** for permanent configuration.

Examples

```
Command> ifconfig
ether0: flags=16<IP_UP,IPX_DOWN,BROADCAST,OSPF>
inet 172.16.110.68 netmask ffffffff broadcast 172.16.110.64
area 0.0.0.64 ospf-state DROTHER mtu 1500
et01: flags=106<IP_UP,IPX_DOWN,BROADCAST,PRIVATE>
inet 192.168.55.6 netmask fffffff0 broadcast 192.168.55.255 mtu 1500

Command> ifconfig ether0 address 192.168.100.1 netmask 255.255.255.0
ether0: flags=16<IP_UP,IPX_DOWN,BROADCAST>
inet 192.168.100.1 netmask fffffff0 broadcast 192.168.100.0 mtu 1500
```

See Also

ifconfig - page 17-5

ping - page 2-11

traceroute - page 2-44

ping

This command sends ICMP echo request packets to the target, and listens for an ICMP echo reply.

ping [*Ipaddress*]

Ipaddress IP address or hostname of host to ping.

Usage

Ping is the basic connectivity test for network debugging. Ping uses the source IP address of the interface the packet leaves, except when a ping packet leaves a port or an interface that is not IP numbered.

To stop the process, type the **ping** command with no argument.

Example

```
Command> ping www.edu.com
www.edu.com (172.16.200.3) is alive
```

```
Command> ping www.edu.com
www.edu.com (172.16.200.3) is alive - round trip=15 ms
```

See Also

ptrace - page 2-13

set reported_ip - page 3-19

traceroute - page 2-44

pmlogin

This command is used for debugging purposes to establish a login session from the PortMaster, using the PortMaster login service to an **in.pmd** daemon running on a host.

pmlogin *Ipaddress*

Ipaddress IP address or hostname.

Usage

The PortMaster login service can be used only with a host that has the PortMaster **in.pmd** daemon software installed. This service uses TCP socket 1642.

Example

```
Command> pmlogin ra  
ra login:
```

See Also

rlogin - page 2-17

telnet - page 2-42

ptrace

This command is used for debugging purposes and allows you to see packet information as it passes through the PortMaster. Filters are used to define which packets you want to display.

ptrace [*Filtername*[**extended**|**dump** *bytes*]]

<i>Filtername</i>	Name of the filter defining which packets to display.
extended	Displays the name of the interface through which the packets are passing, in addition to the packets defined by the filter.
dump	Provides a raw hex dump of the contents of an Ethernet frame for any packet specified.
<i>Bytes</i>	Number of bytes in the hex dump—between 0 and 1514.

Usage

For more information about filters, see Chapter 13, “Filters.”

Packets permitted by the filter are displayed. The **ptrace** command does not display ICMP or UDP packets originating on the PortMaster itself.

To stop the **ptrace** process, issue the command without any arguments.



Caution – When debugging from a Telnet session, be very careful not to use **ptrace** on Telnet packets going between the PortMaster and the host from which you are using Telnet. Doing so can create an endless loop of messages.

Examples

```
Command> add filter x
Command> set filter x 1 permit icmp
Command> ptrace x
Packet Tracing Enabled
```

```
Command> add filter u
New Filter successfully added
Command> set filter u 1 permit udp
Filter u updated
Command> pt u extended dump 128
Packet Tracing Enabled
Command> set console
Setting CONSOLE to admin session
Command> IN ether0 UDP from 149.198.110.4.520 to 149.198.110.0.520
ffffffff ffff00c0 05001228 08004500 005c0db9 0000ff11 000095c6 6e0495c6
6e000208 02080048 2b580201 00000002 000095c6 6e400000 00000000 00000000
00010002 0000c0a8 37000000 00000000 00000000 00020002 0000c0a8 0a000000
00000000 00000000 0002c392 e5e50000 00000000 00000000 00000000 04813200
Command>
Command>
IN ether0 UDP from 149.198.110.9.520 to 149.198.110.31.520
ffffffff ffff00c0 05031d8a 08004500 0034416e 0000ff11 000095c6 6e0995c6
6e1f0208 02080020 ed5d0201 00000002 000095c6 6ec00000 00000000 00000000
00018d45 fe356330 61382030 61303030 30303020 30303030
IN ether0 UDP from 149.198.110.5.520 to 149.198.110.31.520
ffffffff ffff00c0 050028ce 08004500 007022b0 0000ff11 000095c6 6e0595c6
6e1f0208 0208005c dfd10201 00000002 000095c6 6e600000 00000000 00000000
00020002 000095c6 6ee80000 00000000 00000000 00010002 000095c6 6ee00000
00000000 00000000 00010002 000095c6 6e500000 00000000 00000000 0002ce43
```

See Also

add filter - page 13-4
set console - page 2-20
set filter - page 13-6 to page 13-22
show filter - page 13-24
show table filter - page 13-25

reboot

This command restarts the software using the currently saved configuration.

reboot

Usage

A PortMaster must be rebooted for a changed IP address, IPX address, or ISDN switch type to take effect, or for an upgrade loaded earlier into nonvolatile RAM to be used.



Note – Rebooting performs a software restart that takes approximately 30 seconds. This process resets all active ports to their saved configurations, disconnecting all active sessions. Any changes made since a **save** command was last issued are lost when you reboot, unless you first save them.

reset

This command shuts down and immediately restarts a physical or virtual port, or all ports, or certain types of settings on the ports of a PortMaster.

After making any changes to port configuration, you must reset PortMaster ports to activate any changes.

```
reset all|bgp|console|dialer|dNumber|l2tp|MO|nat|
nHandle|nic|ospf|p0|propagation|S0|S10|V0|W1
```

all Resets all ports.



Caution – This command drops active calls connected to serial and asynchronous ports on the PortMaster, forcing users to reconnect. This command does not affect the console port or the Ethernet port.

bgp See page 18-10.

console Removes the current console setting, if any.

dialer	Checks all active interfaces against the location table and creates, destroys, or times out interfaces as needed. This command manually initiates a reset that is normally a background process.
dNumber	ISDN channel. Enter this value as d immediately followed (no space) by the channel number from the first column of the show isdn output. See page 11-15 for an example display.
l2tp	See page 15-3.
<i>MO</i>	See page 12-5.
nat	See page 14-6.
nHandle	Network identifier. Enter this value as n immediately followed (no space) by a number from the first column of the show netconns output. See page 2-33 for an example display.
nic	Resets the network interface card (NIC) controller.
ospf	See page 17-6.
p0	The parallel port.
propagation	See page 16-6.
<i>S0</i>	Any asynchronous or ISDN PRI port.
<i>S10</i>	Any ISDN BRI port.
<i>V0</i>	See page 12-5.
<i>W1</i>	Any synchronous WAN port.

Usage

Resetting an asynchronous port causes the Data Terminal Ready (DTR) signal to be held low for 500ms, then keeps DTR down for 10 seconds or until the Data Carrier Detect (DCD) signal drops, whichever occurs first.

Ports are reset automatically when a connection drops. You can reset specific asynchronous or synchronous ports, or all ports, by selecting the appropriate keyword.

Example

```
Command> reset s0  
Resetting port S0
```

See Also

save console - page 2-18

set console - page 2-20

rlogin

This command is used for debugging purposes to establish a remote login from the PortMaster to a host.

rlogin *Ipaddress*

Ipaddress IP address or hostname.

Usage

Rlogin is a method for logging in to a remote machine from a workstation. Once the login and password procedures are complete, a session is started on the host.

Example

```
Command> rlogin ra  
ra login:
```

See Also

pmlogin - page 2-12

telnet - page 2-42

save

This command saves configuration information to the nonvolatile memory of the PortMaster.



Note – If you are running ComOS 3.8 and later, you must use the command **save ports** to save changes made to any port.

```
save all|bgp|console|filter|global|host|location|map|
netmask|ospf|p0|ports|route|S0|S10|snmp|user|W1
```

all	All configuration changes.	
bgp	BGP configuration.	See Chapter 18.
console	Console port setting.	See page 2-20.
filter	Filter configuration changes.	See Chapter 13.
global	Global configuration changes.	See Chapter 3.
host	Host table settings.	See Chapter 10.
location	Location table settings.	See Chapter 8.
map	NAT address map.	See Chapter 14.
netmask	Netmask table settings.	See Chapter 16.
ospf	OSPF configuration.	See Chapter 17.
p0	Parallel port settings.	See Chapter 9.
ports	All ports.	
route	Static route table settings.	See Chapter 16.
S0	Any asynchronous or ISDN PRI port.	See Chapter 5.
S10	Any ISDN BRI port.	

snmp	SNMP table settings.	See Chapter 3.
user	User table settings.	See Chapter 7.
<i>w1</i>	Any synchronous port.	See Chapter 6.

Usage

After making changes to configuration parameters or tables, you can save the changes individually using the **save** command with a specific keyword, or you can use the **save all** command to save all changes. Some configuration changes require that you reboot before the changes become effective, as noted in individual chapters and command descriptions.

Example

```
Command> save all  
Saving global configuration  
Saving ports  
User table successfully saved  
Hosts table successfully saved  
Static route table successfully saved  
Location table successfully saved  
SNMP table successfully saved  
Filter table successfully saved  
New configurations successfully saved.
```

See Also

set debug - page 19-5
show files - page 2-25

set console

This command sets the port as the PortMaster system console. System messages sent to this port can be displayed on an attached device such as a terminal.

set console [*S0*|*p0*]

S0 Any asynchronous port.

p0 Parallel port, to have console messages sent to an attached parallel printer.

Usage

If no port is specified, the current connection becomes the console. The command **reset console** removes the console, and **save console** saves the console setting to nonvolatile RAM.

Example

```
Command> set console s0  
Setting CONSOLE to port S0
```

See Also

reset console - page 2-15

save console - page 2-18

set debug - page 19-5

set sysname

This command sets the name used for the SNMP system name, IPX Service Advertising Protocol (SAP), Challenge Handshake Authentication Protocol (CHAP), and the command prompt.

set sysname [*String*]

String Name of up to 16 characters. No default.

Usage

The command prompt displays the system name instead of **Command** on a PortMaster that has the system name set. To remove a system name, enter the command without any arguments.

Example

```
Command> set sysname pm2  
System Name Successfully changed
```

See Also

set chap - page 3-6
set snmp - page 3-39

show all

This command shows a summary status of all ports.

show all

Example

```
Command> show all
Local Addr: goto.edu (192.168.96.6)      Default Host: server.edu.com
Gateway: goto-90-gw.edu.com             Netmask: 255.255.255.0
DNS Server: server.edu.com              Domain: edu.com
```

Port	Speed	Mdm	Host	Type	Status	Input	Output	Pend
----	-----	----	-----	-----	-----	-----	-----	----
C0	9600	on	server	Login	USERNAME	0	30	0
S0	28800	M2	server	Login/	COMMAND	1126499	4734323	0
S1	28800	M1	-	Device	ESTABLISHED	912355	3707007	0
S2	64000	on	ptp49	Netwrk	ESTABLISHED	783691	874518	0
S3	64000	on	server	Netwrk	CONNECTING	63057187	64106116	0
S4	64000	on	server	Login/	IDLE	99463	789349	0
.
P0	-	-	server	Device	IDLE	0	0	0

Explanation

Port	Port name.
Speed	Data rate of port in bits per second. Default is 9600 on asynchronous ports.
Mdm	Modem control status. Default is off . A value such as M1 indicates the port used by that numbered digital modem on the PortMaster.
Host	The login or device host for the port.
Type	Type of operation for which port is configured.

Status	Current port state. See Table 2-2 on page 2-23 for descriptions.
Input	Input bytes to this port since last reboot.
Output	Output bytes from this port since last reboot.
Pend	Pending output bytes on this port.

Table 2-2 Port Status Messages

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

show arp

This command shows ARP tables for the specified Ethernet or Frame Relay interface.

show arp *Interface*

<i>Interface</i>	The interface specification—for example, ether0 , frm1 , or frmw1 . Use the command ifconfig to obtain a list of available interfaces.
------------------	--

Example

```
Command> show arp ether0  
10.0.0.3 at 00:c0:05:cb:a6:44  
10.0.0.10 at 00:c0:05:6f:19:5c
```

Explanation

For Ethernet interfaces, the output shows the mapping from IP address to media access control (MAC) address in the ARP cache.

For Frame Relay, the output shows the mapping from IP address to data link connection identifier (DLCI), and includes the Q.922 value for the DLCI.

See Also

ifconfig - page 2-9

show files

This command displays filenames and lengths in bytes, and how much of the nonvolatile RAM configuration file system is in use. PortMaster 3 models have 384KB of nonvolatile RAM, and other PortMaster models have 128KB. Optional files that are not loaded, such as the SNMP table, are not displayed.

show files

Example 1

From a PortMaster PM-2:

```
Command> show files
File Name      Length
-----
confdata      312
config        12122
passwd        328
routes        10
location      348
script        143
snmp          41
filters       416
listnames     700
ipxfilt       104
sapfilt       104
ospfarea     176
-----
Total         14804
```

Example 2

From a PortMaster 3 with internal digital modems:

Command> **show files**

File Name	Length	
-----	-----	
confdata	24607	
config	218	
rti_ser	64	
passwd	216	
rti_user	44	
routes	10	
location	348	
script	196	
snmp	51	
filters	1216	
listnames	1900	
ipxfilt	208	
sapfilt	208	
alias_tab	319	
ospfarea	176	
hfile	38448	
3_18_omc	14108	(31972 uncompressed)
3_18_mnp	7813	(16418 uncompressed)
3_18_cmn	11974	(21736 uncompressed)
3_18_v32	12270	(23094 uncompressed)
3_18_ph1	10671	(21096 uncompressed)
3_18_ans	30345	(51556 uncompressed)
m2c_2.1	22665	(70982 uncompressed)
3_18_bot	354	(464 uncompressed)
3_18_ph2	19230	(46476 uncompressed)
m2d_2.1	85555	(262144 uncompressed)
wanctl.0	9951	(40746 uncompressed)

Total	293165	

Explanation

File	Contents
confdata	Extensions to port configurations, Ether1, or RADIUS.
config	Global configuration and standard port configurations.
passwd	User table.
hosttab	Host table.
routes	Static route table.
location	Location table, except for chat scripts.
script	Chat scripts for the location table.
snmp	SNMP table.
filters	IP filters.
listnames	ChoiceNet list IDs contained in filters.
ipxfilt	IPX filters.
sapfilt	SAP filters.
ospfarea	OSPF area information.
netmasks	Static netmask table.
modem	Modem table.
dialer	The inband outbound dialer code.
dlcitab	Frame Relay DLCI information.
hfile	Help file that stores information for the help command.

show global

This command shows system-wide configuration values.

show global

Example

```
Command> show global
      System Name:  pmaster
      Default Host:  server.edu.com
      Alternate Hosts:
        IP Gateway:  192.168.96.2
        Gateway Metric:  1
      Default Routing:  Quiet (Off)
        OSPF Priority:  0
        OSPF Router ID:  192.168.200.1
        BGP ID[AS]:  192.168.96.76[99999]
        BGP timers:  Connect 60 Keepalive 30 Hold 90
      BGP IGP Lockstep:  off
      Name Service:  DNS
        Name Server:  server.edu.com
        Domain:  edu.com
      Telnet Access Port:  23
        Loghost:  0.0.0.0
      Maximum PMconsole:  1
      Assigned Address:  0.0.0.0
        RADIUS Server:  server.edu.com
      Alternate Server:  0.0.0.0
      Accounting Server:  server.edu.com
      Alt. Acct. Server:  0.0.0.0
      ChoiceNet Server:  192.168.96.9
      Alt. ChNet Server:  0.0.0.0
      PPP Authentication:  PAP: on      CHAP: on
      ISDN Switch Type:  DMS-100
        ISDN MSN:  off
      ISDN numberauto:  on
      ISDN numberplan:  unknown
```

```

ISDN numbertype: local
End Point Disc: None
Disabled Modules: SNMP

```

Explanation

File	Contents	
System Name	SNMP system name.	See page 2-21.
Default Host	Host used for login services.	See page 5-21.
Alternate Hosts	Alternate host.	See page 5-21.
IP Gateway	Default route gateway address.	See page 16-12.
Gateway Metric	Metric for the default route.	See page 16-12.
Default Routing	Default routing options for all interfaces.	See page 16-18.
OSPF Priority	OSPF priority assigned to the router.	See page 17-19.
OSPF Router ID	OSPF router address or ID number.	See page 17-20.
BGP ID[AS/Clust ID]	BGP router address, with the autonomous system (AS) number, and the cluster ID—if a route reflector is configured.	See page 18-16 and page 18-12.
BGP timers	Configured BGP timed events.	See page 18-14 and page 18-15.
BGP IGP Lockstep	Status of the BGP Interior Gateway Protocol (IGP) lockstep setting.	See page 18-16.
Name Service	Service—Network Information Service (NIS) or Domain Name System (DNS)—used for resolving hostnames.	See page 3-14.
Name Server	Name server IP address or hostname.	See page 3-13.
Domain	Domain name used with hostname lookups.	See page 3-7.
Telnet Access Port	Administrative Telnet port.	See page 3-22.

Loghost	Host to which syslog messages are sent.	See page 3-11.
Maximum PMconsole	Maximum number of concurrent connections for management applications permitted into the PortMaster.	See page 3-12.
Assigned Address	Base address in the assigned address pool.	See page 3-3.
RADIUS Server	IP address or hostname of the server running the RADIUS authentication service.	See page 3-31.
Alternate Server	Alternate RADIUS authentication server.	See page 3-30.
Accounting Server	RADIUS accounting server.	See page 3-24.
Alt. Acct. Server	Alternate RADIUS accounting server.	See page 3-24.
ChoiceNet Server	ChoiceNet server.	See page 3-33.
Alt. ChNet Server	Alternate ChoiceNet server.	See page 3-33.
PPP Authentication	Configured authentication—PAP and CHAP.	See page 3-16.
ISDN Switch Type	ISDN switch type.	See page 11-9 and page 12-7.
ISDN MSN	ISDN multiple subscriber number (MSN) setting.	See page 11-4.
ISDN numberauto	Automatic determination of ISDN number plan and type for a received call.	See page 11-5.
ISDN numberplan	ISDN number plan.	See page 11-6.
ISDN numbertype	ISDN number type.	See page 11-7.
End Point Disc	The Multichassis PPP endpoint discriminator.	See page 12-6.
Disabled Modules	Disabled ComOS modules.	See page 2-32.

show memory

This command shows system memory use.

show memory

Example

```
Command> show memory
System memory 1048576 bytes - 860552 used, 188024 available
64:1 96:1 1152:1 128:1 640:2 144:3 80:1 16:10 160:0 208:1 32:11
System nbufs 1400 - 137 used, 1263 available
```

Explanation

System Memory (values from example)

First value (1048576 bytes) Total memory installed in the system.

Second value (860552 bytes) Highest amount of system memory ever used by system.

Third value (188024 bytes) Memory remaining in the free large heap. If this value is greater than zero, the system has never run out of memory.

64:1 96:1 1152:1, and so on Memory fragments, *Size:Number*:

- *Size*—size in bytes (example 64).
- *Number*—number of fragments of that size (example 1).

To determine the total free memory, add the free large heap to the sum of the fragments.

When memory is used, memory fragments are used before the free large heap.

System nbufs Network buffers showing total buffers, buffers in use by network packets, and available buffers. Each buffer is 128 bytes.

System bbufs Equivalent to system nbufs, but buffer size is increased to 1600 bytes. Seen on PortMaster Office Routers with T1 interfaces.

show modules

The PortMaster ComOS is divided into functional modules. This command shows the names and sizes of the modules that are loaded into the currently running ComOS. Optional functions that are not loaded, such as the SNMP table, are not displayed.

show modules

Example

Command> show modules			
Module	State	Start	Len
-----	-----	-----	-----
0 SNMP	HEAP	1066e4	23732
1 IPX	ACT	102814	16080
2 INIT	HEAP	ff000	14356
3 SYNC	HEAP	14a52c	16872
4 OSPF	ACT	14e714	16
5 BGP	HEAP	3a1ec	80
6 ISDN	ACT	10c89c	218216
7 ISDN-NORTH-AM	ACT	141d04	10548
8 ISDN-EUROPE	HEAP	144638	20824
9 ISDN-JAPAN	HEAP	149790	3484

Explanation

Module	The function module.
State	Module state: <ul style="list-style-type: none">• HEAP—The module is disabled.• ACT—The module is active.
Start	Memory location of the start of the module—a hexadecimal value.
Len	Length (size) of the module in bytes—a decimal value.

show netconns

This command shows the TCP and UDP network sockets open on the PortMaster.

show netconns

Example

Command> **show netconns**

Hnd	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
706	0	0	goto.offc2.com.1011	server.offc2.com.513	CONNECTING
615	0	0	goto.offc2.com.23	0.0.0.0.0	LISTEN
588	0	2	goto.offc2.com.23	xterm1.offc2.com.1389	ESTABLISHED
552	0	0	goto.offc2.com.1643	0.0.0.0.0	LISTEN
120	0	0	goto.offc2.com.1011	server.offc2.com.1642	ESTABLISHED
76	0	0	goto.offc2.com.1030	server.edu.com.53	UDP
10	0	0	goto.offc2.com.67	0.0.0.0.0	UDP

Explanation

Hnd	Network handle.
Recv-Q	Number of packets in receive queue.
Send-Q	Number of packets in send queue.
Local Address	Local hostname or IP address with TCP or UDP port number.
Foreign Address	Foreign hostname or IP address with TCP or UDP port number.
(state)	TCP connection state, or <i>UDP</i> for UDP sockets.

See Also

reset nHandle - page 2-15

show netstat

This command shows network interface statistics.

show netstat

Example

```
Command> show netstat
```

Name	Ipkts	Ierrs	Opkts	Oerrs	Collis	Resets	Queue
ether0	207757	0	215161	0	223	0	0

Explanation

Name	Interface name.
Ipkts	Number of valid packets received since reboot.
Ierrs	Number of input errors counted since reboot. All input errors cause the error counter to increase. Examples of input error sources are as follows: <ul style="list-style-type: none">• PPP frame header errors.• Frame too large or too small.• Frame alignment errors.• CRC errors.
Opkts	Number of valid packets sent since reboot.
Oerrs	Number of output errors counted since reboot. All output errors cause the error counter to increase. Examples of output error sources are as follows: <ul style="list-style-type: none">• Transmission prevented because of excess collisions.• Out-of-window collision—collision occurring outside a normal time slot.

Collis	Number of collisions since reboot.
Resets	Number of times the interface was reset since reboot, due to any of the following: <ul style="list-style-type: none"> • More than 16 collisions occurring during transmission of the same packet. • Abnormally terminated transmission. • Lost carrier. • No collision detect signal. • Out-of-window collision—collision occurring outside a normal time slot.
Queue	Number of packets waiting in a buffer to be sent from the interface.

show S0

This command shows the current status and configuration for asynchronous, ISDN PRI, ISDN BRI, and parallel ports on the PortMaster.

show S0|S10|p0

Example

Command> **show s0**

```

----- Current Status - Port S0 -----
      Status:  USERNAME
      Input:   62              Parity Errors:  0
      Output: 652             Framing Errors: 22
      Pending: 0              Overrun Errors:  0
      Modem Status: DCD+ CTS+

      Active Configuration  Default Configuration(* = Host Can Override)
      -----
      Port Type:  Login      Login (Security)
      Login Service: PortMaster PortMaster

```

Baud Rates:	115200	115200,115200,115200
Databits:	8	8
Stopbits:	1	1
Parity:	none	none
Flow Control:	None	None
Modem Control:	off	off
Hosts:	tm	default

Terminal Type:

Login Prompt: \$hostname login:

Idle Timeout: 10 minutes

Explanation

Status	State of the port. Refer to the information on port status in Table 2-2 on page 2-23.
Input/Output/ Pending	Number of bytes input, output, or pending since last reboot.
Parity Errors	Parity error count for the most recent reporting interval.
Abort Errors	<p>Number of abnormal termination errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—framing errors/device errors:</p> <p>Framing errors—This count increments when the receiver chip reports either a framing error or an abnormal termination.</p> <p>Device errors—This count increments when the frame size is 0 (zero) or greater than the maximum size of a PPP frame, or when frames overlap each other.</p>
CRC Errors	Number of cyclic redundancy check (CRC) errors occurring since last reboot.
Overrun Errors	Number of overrun errors occurring since last reboot.
Frame Errors	Number of frame errors occurring since last reboot. A slash (/) in this field indicates two separate error counts— short frame errors/large frame errors :

	Short frame errors —This count increments when a short frame is received.
	Large frame errors —This count increments when a packet is too large and must be dropped.
Modem Status	The plus signs (+) on <i>DCD</i> and <i>CTS</i> indicate that the DCD and CTS signals on the port are asserted (high). ISDN has additional + and - indicators. For modem status information for ISDN lines, refer to the ISDN connection chapter in the <i>PortMaster Configuration Guide</i> .
Active Configuration	The configuration currently active on the port.
Default Configuration	The configured port parameters, including available alternatives.
Port Type	The port type—login, device, or network. (Security) indicates that security has been set for the port. See page 5-40.
Login Service	Type of login service selected— PortMaster , rlogin , telnet , or netdata .
Baud Rates	The port speed in bits per second.
Databits	The number of data bits per byte.
Stopbits	The number of stop bits per byte.
Parity	The parity checking used.
Flow Control	Flow control used—software (XON/XOFF), hardware (RTS/CTS), or none.
Modem Control	Modem carrier detect signal setting.
Hosts	Active configuration shows the current host accessed.
Terminal Type	The terminal type selected.
Login Prompt	The user login prompt.
Idle Timeout	The idle time in minutes before a port is reset.

See Also

show W1 - page 6-24

show sap

This command shows the active Service Advertising Protocol (SAP) table.

show sap

Example

Command> show sap						
Server	Svc	Network	Host	Sock	Hops	Interface
-----	---	-----	-----	---	-----	-----
080009A8CEAA80CGNPiA8CEA	30C	COA86000:	080009A8CEAA:	400C	2	ether0
NOVELL	4	00001701:	0000000000001:	0451	2	ether0

Explanation

Server	IPX server.
Svc	IPX service available on the server. See RFC 1700 for a list of Novell SAP numbers.
Network	IPX network number of the destination.
Host	IPX address of the destination.
Sock	IPX socket number of the destination.
Hops	Hop count to the remote destination.
Interface	Interface used for sending packets.

show sessions

This command shows current use of ports.

show sessions

Usage

To display output without a pause, use PMVision or send the output to a file.

Example

Command> show sessions							
Port	User	Host/Inet/Dest	Type	Dir	Status	Start	Idle
----	-----	-----	-----	---	-----	---	--
S0	-	tm	Login	In	USERNAME	0	0
S1	-	tm	Device	Out	ESTABLISHED	1:23	1:23
S2	-	tm	Device	Out	ESTABLISHED	3	3
S3	-	-	Log/Net	In	USERNAME	0	0
S4	-	tm	Login	In	USERNAME	0	0
S5	-	tm	Log/Net	In	IDLE	0	0
S6	-	tm	Login	In	USERNAME	0	0
S7	-	tm	Login	In	USERNAME	0	0
S8	-	tm	Login	In	USERNAME	0	0
S9	-	tm	Login	In	USERNAME	0	0
S10	-	-	Netwrk	Out	IDLE	0	0
V0	john	pm3-03	Netwrk	In	ESTABLISHED	-	-

Explanation

Port	Port number. Multichassis PPP virtual ports corresponding to the physical ports of the slave unit are indicated by the letter V followed by a number.
User	Username of the user logged in on the port.
Host/Inet/Dest	Host for login users or host devices, or address of network users.
Type	Type of operation for which port is configured, or the active type for established ports.
Dir	Direction that the connection was established—inbound or outbound.
Status	State of the port. Refer to the information on port status in Table 2-2 on page 2-23.
Start	Time in minutes since the session started.
Idle	Time in minutes that the session has been idle.

show syslog

This command displays the current **syslog** settings.

show syslog

Example

Command> **show syslog**

Syslog Configuration Settings

```
admin-logins  auth.info
user-logins:  auth.info
packet-filters: auth.notice
commands:    disabled
termination: disabled
nat:         auth.notice
```

Explanation

This example displays the default settings. These default settings can be changed with the **set syslog** command (see page 3-20).

See Also

set loghost - page 3-11

show table

This command displays the contents of tables stored in the memory of the PortMaster. Each command is covered in more detail in the chapter for that table.

**show table bgp|filter|host|location|modem|netmask|ospf|snmp|
subinterface|user**

bgp	See page 18-49.
filter	See the following example and page 13-25.
host	See page 10-3.
location	See page 8-32.
modem	See page 5-50.
netmask	See page 16-31.
ospf	See page 17-21.
subinterface	See page 4-18.
user	See page 7-24.

Example

To see a list of filters in the filter table:

```
Command> show table filter
next.in      sapo.out      ether.in      inter.in      general.in
general.out  hosts.in
```

To see the contents of a specific filter:

```
Command> show filter inter.in
1  deny 192.168.200.0/24 0.0.0.0/0 ip
2  permit 0.0.0.0/0 0.0.0.0/0 tcp estab
3  permit 0.0.0.0/0 0.0.0.0/0 udp dst eq 53
4  permit 0.0.0.0/0 0.0.0.0/0 tcp dst eq 53
5  permit 0.0.0.0/0 0.0.0.0/0 tcp dst eq 25
```

telnet

This command is used for debugging purposes to establish a login from the PortMaster to a host using the Telnet protocol.

telnet *Ipaddress* [*Tport*]

Ipaddress IP address or hostname.

Tport Number of the designated TCP port—a 16-bit decimal number from 1 to 65535. Default is 23.

See Table D on page D-1 for a list of the port numbers 20 through 1701 commonly assigned to TCP and UDP services.

Usage

Telnet is an Internet standard protocol used for remote terminal service.

Note – The parser for this command does not allow the use of 0 as value for *Tport*.



Example

```
Command> telnet ra  
ra login:
```

See Also

pmlogin - page 2-12
rlogin - page 2-17

tftp

This command retrieves a file of configuration commands or a ComOS image from a host using the Trivial File Transfer Protocol (TFTP).

tftp get [**comos**] *IpAddress String*



Note – The **tftp get comos** command is available only on the PortMaster 3.

comos	Use for upgrading from ComOS 3.1.2-and-later to ComOS 3.7-and-later releases.
<i>IpAddress</i>	IP address or 39-character hostname of the TFTP server.
<i>String</i>	Name of the file to be retrieved from the TFTP server.

Usage

See your system administration manual for instructions on how to set up a TFTP server on your host.

You can use either **pminstall** or **tftp get comos** to upgrade a PortMaster 3 from ComOS release 3.1.2 and later to ComOS release 3.7 and later. However, you cannot use the **tftp get comos** command to upgrade from ComOS release 3.1.1 or earlier, or to upgrade to ComOS release 3.5 or earlier. For these upgrades you must use the **pminstall** utility instead.

Example

```
Command> tftp get 192.168.1.70 pm2.cfg  
Requesting tftp of pm2.cfg from host 192.168.1.70 (192.168.1.70)  
Output from configuration commands in file /tftpboot/pm2.cfg appears here.  
tftp complete
```

traceroute

This command traces a network route by sending UDP packets with a time-to-live timer set to between 1 and 30 hops and printing the addresses that send back ICMP Time Expired packets.

traceroute [*Ipaddress*]

Ipaddress IP address of destination to which route is to be traced.

Usage

The **traceroute** command takes its source address from the interface through which it exits.

To stop the traceroute process, issue the command with no argument.

Example

```
Command> traceroute 172.16.1.2  
traceroute to (172.16.1.2), 30 hops max  
1 192.168.96.2  
2 192.168.1.3  
3 172.16.1.2
```

See Also

ping - page 2-11
ptrace - page 2-13

version

This command displays the ComOS software version number and the uptime since the last boot.

version

Usage

Always include the version number when reporting problems to Lucent NetworkCare technical support.

Example

```
Command> version  
Livingston Enterprises PortMaster Version 3.5  
System uptime is 21 days 15 hours 34 minutes
```


This chapter describes how to use the command line interface for global configuration. Detailed command definitions follow a command summary table. Detailed command definitions and summary tables are also provided for RADIUS (page 3-24), ChoiceNet (page 3-33), and SNMP (page 3-35) configuration commands.

The command line interface can be used to configure global settings, allowing you to set default and alternate hosts, set gateways and metrics, set the name service used by the PortMaster, and set the administrative password of the PortMaster.

Displaying Global Information

To display information about your configuration, use the following global commands:

- **show all**—see page 2-22
- **show global**—see page 2-28

For general information about using the command line interface, refer to Chapter 1, “Introduction.”

Summary of Global Commands

Table 3-1 contains the global configuration commands that affect the entire PortMaster.

For a summary of other global commands, see the following:

- RADIUS commands - see page 3-24
- ChoiceNet commands - see page 3-33
- SNMP commands - see page 3-35

Table 3-1 Global Configuration

Command Syntax	
clear alarm <i>Alarm-id</i> all	- see page 3-37
set assigned_address <i>Ipaddress</i>	- see page 3-3
set call-check on off	- see page 3-4
set chap on off	- see page 3-6
set default on off broadcast listen	- see page 16-18
set domain <i>String</i> none	- see page 3-7
set gateway <i>Ipaddress</i> [<i>Metric</i>]	- see page 16-12
set host 1 2 3 4 <i>Ipaddress</i>	- see page 3-8
set ipx on off	- see page 3-9
set ipxgateway <i>Network</i> <i>Node Metric</i>	- see page 3-10
set loghost <i>Ipaddress</i>	- see page 3-11
set maximum pmconsole <i>Number</i>	- see page 3-12
set nameserver [1 2] <i>Ipaddress</i>	- see page 3-13
set namesvc dns nis	- see page 3-14
set netbios on off	- see page 3-15
set pap on off	- see page 3-16
set password [<i>Password</i>]	- see page 3-17
set pool <i>Number</i>	- see page 3-17
set pots on off	- see page 3-18
set reported_ip <i>Ipaddress</i>	- see page 3-19

Table 3-1 Global Configuration (Continued)

Command Syntax	
set serial-admin on off	- see page 3-20
set syslog Logtype {[disabled] [Facility.Priority]}	- see page 3-20
set telnet Tport	- see page 3-22
set user-netmask on off	- see page 16-13
show alarms [Alarm-id]	- see page 3-41
show all	- see page 2-22
show global	- see page 2-28
show pots	- see page 3-23

Global Commands

These commands are used to configure global settings on a PortMaster.

set assigned_address

This command sets the base IP address of the assigned address pool.

set assigned_address *Ipaddress*

Ipaddress

Base IP address assigned. Set *Ipaddress* to 0.0.0.0 to deselect the assigned address.

Usage

The PortMaster allocates a pool of addresses starting at the assigned base address and counting up. The total number of addresses is equal to the number of ports configured for network dial-in. If someone dials in and requests an unused address from the pool, that is assigned. If someone dials in and requests any address, the next address from the pool is assigned. If someone disconnects, their address is placed at the end of the pool for reuse.



You must use the command **save all** and reboot the PortMaster after setting or changing the base IP address.

Example

Command> **set assigned 172.16.200.220**

First Assigned address changed from 0.0.0.0 to 172.16.200.220

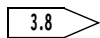
See Also

set pool - page 3-17

set user destination - page 7-7

set call-check

This command provides the choice of supporting or disabling the call-check feature on PortMaster products that support ISDN PRI or in-band signaling.



set call-check on|off

- | | |
|------------|---|
| on | Enables the call-check feature on the PortMaster connected to the PRI or in-band signaling interface. |
| off | Disables the call-check feature. This is the default. |



Caution – To support the call-check feature, you must configure RADIUS Call-Check-User entries; otherwise, the PortMaster issues a busy signal to every call.

For more information about enabling RADIUS call-check features, refer to the *PortMaster Configuration Guide*.

Usage

ComOS 3.8 and later releases support the call-check feature to enable services without authenticating the user at the point of entry. This feature is useful when you want to provide guest access or establish tunnels based on dial number information services. Call checking can be done against the calling number ID (CNID) or calling line ID (CLID) or both. The RADIUS attributes are Called-Station-Id and Calling-Station-Id, respectively.

If the call-check feature is set to **on**, the PortMaster sends a ringing message to the switch while the service information is being looked up in RADIUS.

RADIUS either rejects the message with a busy signal, acknowledges the call and allows the call to be completed with no special service type determined during the call, or, allows the creation of a netdata clear channel TCP connection to the destination specified in the RADIUS accept record.

Use the **show global** command to find out if call-check is enabled on your PortMaster.

Example

```
Command> set call-check on
Call Check changed from off to on
```

```
Command> show global
Alt. Acct. Server: 0.0.0.0
PPP Authentication: PAP: on    CHAP: off
ISDN Switch Type:   (Call Check Enabled)
End Point Disc: None
```

set chap

This command provides the choice of supporting or disabling the Challenge Handshake Authentication Protocol (CHAP) authentication for dial-in users.

set chap on|off

- | | |
|------------|---|
| on | If PPP is detected on a port and PAP is disabled, the PortMaster allows the user to negotiate CHAP as the authentication protocol. This is the default. |
| off | CHAP authentication is disabled. |

Usage

If you do not want to support CHAP authentication, you must set CHAP to **off**. With both PAP and CHAP off, the only authentication method allowed is a username-password login.

Example

```
Command> set chap off  
CHAP authentication changed from on to off
```

See Also

set location chap - page 8-8
set pap - page 3-16
show global - page 2-28

set domain

This command sets the domain name to use with hostname lookups.

set domain *String* | **none**

String Domain name. Maximum of 31 characters.

none Disables the domain feature.

Usage

Enter the domain name of your network in this command, after you have selected the Network Information Service (NIS) or Domain Name System (DNS) as your name service and have set a name server address.

Example

```
Command> set domain edu.edu  
Domain changed from    to edu.edu
```

See Also

set nameserver - page 3-13

set namesvc - page 3-14

set host

This command sets the default IP address or hostname for login sessions for all PortMaster products except PortMaster IRX products.

set host [1|2|3|4] *Ipaddress*

Ipaddress IP address or hostname of a login host or device host.

1|2|3|4 Specifies alternate hosts, with the primary host being 1.
The default is 1.

Usage

Use this command only if you want the PortMaster to provide login or host device service. Setting **host** to 0.0.0.0 removes the entry.

Example

```
Command> set host 172.16.200.1  
Default host changed from to 172.16.200.1
```

See Also

set S0 host - page 5-21
set S0 service_device - page 5-41
set S0 service_login - page 5-42
set user host - page 7-10
set user service - page 7-22

set ipx

This command enables or disables PortMaster support for the Novell Internet Packet Exchange (IPX) protocol.

set ipx on|off

on Enables support for the IPX protocol.

off Disables support for the IPX protocol. This is the default.

Usage

To enable support for IPX, you must use this command. After changing the IPX setting, you must use the **save all** command and reboot the PortMaster before the change takes effect.

Example

```
Command> set ipx on
IPX will be enabled after next reboot
```

See Also

set Ether0 ipxframe - page 4-8
set Ether0 ipxnet - page 4-9
set location ipxnet - page 8-15
set S0 ipxnet - page 5-25
set W1 ipxnet - page 6-16
show modules - page 2-32

set ipxgateway

This command sets a static default route for all IPX packets not routed by a more specific route.

set ipxgateway *Network|Node Metric*

<i>Network</i>	32-bit hexadecimal address of the IPX network of the gateway router.
<i>Node</i>	48-bit hexadecimal node address of the gateway router. This is usually the MAC address of the gateway router.
<i>Metric</i>	An integer with a value between 1 and 15 that determines the hop count.

Usage

When troubleshooting IPX routing problems, you can reset the IPX gateway by resetting the network and node numbers to zeros. For more information on troubleshooting IPX routing problems, refer to the *PortMaster Troubleshooting Guide*.

Example

Command> **set ipxgateway tyche:010101010101 1**
IPX Gateway set to tyche:010101010101, metric = 1

Command> **set ipxgateway 00000000:000000000000**
IPX gateway reset

set loghost

This command sets the IP address or name of the host to which the PortMaster sends **syslog** messages.

set loghost *Ipaddress*

Ipaddress Loghost IP address or 39-character hostname.

Usage

Informational **syslog** messages are sent to the host with the following defaults:

- Facility—**auth**
- Priority—**info**

Setting the IP address to 0.0.0.0 disables **syslog** at the PortMaster and deselects the host.



Note – You must use the command **save all** and reboot PortMaster after making changes to the loghost address. You can also use the **reset nHandle** command to reset the UDP port 514 connection.

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



Note – Do not use a loghost at a location configured for on-demand connections, because doing so will keep the connection up or bring up the connection each time a **syslog** message is queued for the **syslog** host.

Example

```
Command> set loghost 192.168.200.2  
Loghost changed from 0.0.0.0 to 192.168.200.2
```

See Also

set syslog - page 3-20

set maximum pmconsole

This command sets the maximum number of concurrent connections for management applications allowed into the PortMaster.

set maximum pmconsole *Number*

Number Maximum number of concurrent connections to allow.
Default is 1; maximum is 10.

Usage

The programs PMVision, ChoiceNet, **pmconsole**, **pminstall**, **pmreadconf**, **pmreadpass**, **pmcommand**, **pmreset**, and other applications connect to TCP port 1643 on the PortMaster. If you set the maximum number of connections to 2 or higher, more than one program can connect at the same time.

If you use ChoiceNet to download filters dynamically, be sure to set the maximum number of connections to 10.



Note – If two or more GUIs are used to configure the PortMaster at the same time, each might not see the change made by the others.

All 1643 network connections must disconnect from the PortMaster for the new settings to take effect. Use the **reset nHandle** command to reset network handles. To view open network connections, use the **show netconns** command.

Example

```
Command> set maximum pmconsole 2
Maximum PMconsole sessions changed from 0 to 2
```

See Also

set serial-admin - page 3-20
set telnet - page 3-22

set nameserver

This command sets the name server IP address.

set nameserver [1|2] *Ipaddress*

1 Sets the primary name server. This is the default.

2 Sets an alternate name server.

Ipaddress IP address in dotted decimal notation.

Usage

This command sets the server used for DNS or NIS hostname lookups. Setting *Ipaddress* to 0.0.0.0 cancels the setting.

Example

```
Command> set nameserver 172.16.200.2
Name Server changed from 0.0.0.0 to 172.16.200.2
```

See Also

set domain - page 3-7

set namesvc - page 3-14

set namesvc

This command sets the service (NIS or DNS) used for resolving hostnames.

set namesvc dns|nis

dns	Uses the Domain Name System (DNS) for hostname lookups.
nis	Uses the Network Information Service (NIS) for hostname lookups.

Usage

A name service should be selected only if users are prompted for hosts that require a name service for resolution to an IP address, or to display hostnames instead of addresses in the administrative command line interface. If the service is set to DNS, the PortMaster sends DNS server information to PPP dial-in users as specified in RFC 1877.

Example

```
Command> set namesvc dns  
Name Service changed from NIS to DNS
```

See Also

set domain - page 3-7
set nameserver - page 3-13

set netbios

This command sets the NetBIOS parameter for use with IPX.

set netbios on|off

on	The PortMaster broadcasts type 20 packets.
off	Type 20 packets are not broadcast across the router. The default is off .

Usage

Full NetBIOS protocol compliance requires that this command be set to **on**. The PortMaster then propagates and forwards type 20 broadcast packets across your IPX network. Be aware of this behavior before changing from the default of **netbios off**.

Example

```
Command> set netbios on  
NetBIOS changed from off to on
```

See Also

set ipx - page 3-9

set pap

This command provides the choice of accepting either Password Authentication Protocol (PAP) or CHAP authentication for dial-in users, or CHAP only.

set pap on|off

- | | |
|------------|---|
| on | If PPP is detected on a port, the PortMaster allows the user to negotiate PAP as the authentication protocol. If PAP is refused, the user is prompted to authenticate with CHAP. This is the default. |
| off | The PortMaster does not request or accept PAP authentication. |

Usage

With PAP set to **off**, the default is to support CHAP. If you do not want to support CHAP authentication, you must disable CHAP (see page 3-6).

Example

```
Command> set pap off  
PAP authentication changed from on to off
```

See Also

set chap - page 3-6
show global - page 2-28

set password

This command sets the PortMaster administrative password.

set password [*Password*]

Password String of up to 15 characters. Default is no password.

Usage

When shipped, the PortMaster has no password. You must enter a password to protect the PortMaster administrative features. Using the command **set password** without a *Password* value erases the administrative password.

The password string cannot start with a question mark (?).

Example

```
Command> set password supercalifragil
!root password changed from   to supercalifragil
```

set pool

This command explicitly sets the size of the assigned pool of IP addresses.

set pool *Number*

Number The number of IP addresses to allocate to the pool.
The valid range is from 0 to 64 on the PortMaster 3.

Usage

After you set or change the pool size of IP addresses, you must reboot the PortMaster for the change to take effect.

Example

Command> **set pool 12**
Assigned address pool size changed from 0 to 12

See Also

set assigned-address - page 3-3

set pots

This command enables or disables the analog PHONE port on the Office Router OR-ST-AP and OR-U-AP.

set pots [on|off]

- | | |
|------------|---|
| on | Enables the analog PHONE port. This is the default. |
| off | Disables the analog PHONE port. |

Usage

To receive data over voice (DOV) calls on the OR-ST-AP or the OR-U-AP units, you must set the PHONE port to **off**.

Example

Command> **set pots off**
Pots port disabled

Command> **set pots on**
Pots port enabled

See Also

show pots - page 3-23

set reported_ip

This command reports an IP address different from the *Ether0* address used during PPP negotiation and Serial Line Internet Protocol (SLIP) startup.

set reported_ip *Ipaddress*

Ipaddress IP address.

Usage

The IP address of any PortMaster device can be used with this command. This feature is valuable for sites that require a number of PortMaster devices to appear as a single IP address to other networks. With PPP, this information is placed in the startup message, and the PortMaster devices report this address to other networks. With SLIP, this information is placed in the startup message.

Setting *Ipaddress* to 0.0.0.0 cancels the setting.

Example

```
Command> set reported_ip 172.16.200.1  
Reported IP address changed from 0.0.0.0 to 172.16.200.1
```

See Also

set Ether0 address - page 4-3
set user local-ip-address - page 7-15

set serial-admin

This command enables or disables administrative logins on the serial ports of the PortMaster.

set serial-admin on|off

on	Enables administrative logins on serial ports. This is the default.
off	Disables administrative logins on serial ports.

Usage

If administrative logins—**!root**—are disabled, you can still use port S0 (or C0) for **!root** login by setting the console DIP switch to the up position.

Example

```
Command> set serial-admin off
Serial Administration changed from on to off
```

set syslog

This command changes the **syslog** settings for logged events.

set syslog Logtype {[disabled] [Facility.Priority]}

<i>Logtype</i>	Sets logging for the following five areas. Use the following keywords:
admin-logins	!root and administrative logins.
user-logins	Nonadministrative logins. You might want to disable this type of logging if you already use RADIUS accounting.
packet-filters	Packets that match filter 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.
disabled	Turns off logging for the <i>Logtype</i> specified.
<i>Facility.Priority</i>	Sets the facility and priority to be assigned to syslog messages. See Table 3-2 on page 3-21 and Table 3-3 on page 3-22 for <i>Facility</i> and <i>Priority</i> keywords. Enter the <i>Facility</i> and <i>Priority</i> keywords separated by a period (.) with no spaces.

Usage

The keywords to use for *Facility* and *Priority* are shown in Table 3-2 and Table 3-3. Lucent recommends that you use the **auth** facility or **local0** through **local7** facilities for receiving **syslog** messages from PortMaster products, but all the facilities listed in Table 3-2 are provided. See your operating system documentation for information on configuring **syslog** on your host.

Table 3-2 **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 3-3 **syslog** Priority Keywords

Priority	Priority Number	Typical Use
emerg	0	System is unusable.
alert	1	Action must be taken immediately.
crit	2	Critical messages.
err	3	Error messages.
warning	4	Warning messages.
notice	5	Normal but significant message.
info	6	Informational message.
debug	7	Debug-level messages.

Examples

```
Command> set syslog commands local0.debug
Syslog setting for commands changed from disabled to local0.debug

Command> set syslog nat auth.notice
Syslog setting for nat changed from disabled to auth.notice
```

See Also

set loghost - page 3-11

set telnet

This command sets the Telnet administrative port.

set telnet *Tport*

Tport Telnet administrative port—integer from between 0 and 9999.
Default is 23.

Usage

This command allows the administrator to use the Telnet protocol to maintain the PortMaster. If set to 0, the PortMaster disables the Telnet administration function. Ports numbered 10000 through 10100 are reserved for outbound users and must not be used for this function.

Example

```
Command> set telnet 23  
Setting Telnet Administration port to 23
```

See Also

set maximum pmconsole - page 3-12
set serial-admin - page 3-20
telnet - page 2-42

show pots

This command displays the status of the analog PHONE port and the B channel associated with it.

show pots

Usage

This command is supported on the Office Routers OR-U-AP and OR-ST-AP only.

Example

```
Command> show pots  
Pots port status  
Pots port enabled  
State idle
```

See Also

set pots - page 3-18

RADIUS Client Commands

The RADIUS commands in Table 3-4 configure the PortMaster to use a RADIUS server. RADIUS is consulted if a port is set for **security on** and a user is not found in the PortMaster user table.

Table 3-4 RADIUS Client Configuration

Command Syntax		
set accounting [1 2] <i>Ipaddress</i> [<i>Uport</i>]		- see page 3-24
set accounting count <i>Number</i>		- see page 3-26
set accounting interval <i>Seconds</i>		- see page 3-27
set alternate_auth_server <i>Ipaddress</i> [<i>Uport</i>]		- see page 3-30
set authentication failover on off		- see page 3-29
set authentication interval <i>Seconds</i>		- see page 3-30
set authentication_server <i>Ipaddress</i> [<i>Uport</i>]		- see page 3-31
set secret <i>String</i>		- see page 3-32

The following commands configure the PortMaster as a RADIUS client. For RADIUS server configuration information, see the *RADIUS for UNIX Administrator's Guide*.

set accounting

This command designates a host as the primary or alternate RADIUS accounting server.

set accounting [1|2] *Ipaddress* [*Uport*]

- 1
- Designates the primary RADIUS server. This is the default.

2	If present, designates a host as the alternate accounting server.
<i>Ipaddress</i>	IP address or 39-character hostname running a RADIUS accounting server on UDP port 1646. Set <i>Ipaddress</i> to 0.0.0.0 to deselect the accounting server.
<i>Uport</i>	Integer between 0 and 65535 that specifies the UDP port to be used for RADIUS accounting. Setting the port number to 0 or not specifying a port number, sets the UDP port to 1646.

Usage

You can designate both primary and alternate RADIUS accounting servers. The accounting server daemon must be present on the host before the RADIUS accounting server will function correctly.



Note – Do not assign the authentication server and the alternate authentication server to the same IP address.

A PortMaster uses **one** of the following criteria to determine whether to send accounting packets to a secondary accounting server instead of the primary accounting server:

- The primary RADIUS accounting server does not respond within 10 minutes. The PortMaster retries the accounting server once every 45 seconds.
- The primary RADIUS accounting server does not respond, and 50 accounting packets are waiting to be sent.

Examples

Command> **set accounting 10.0.0.3**

Accounting Server changed from 0.0.0.0 1646 to 10.0.0.3 1646

Command> **set accounting 10.0.0.3 1813**

Accounting Server changed from 10.0.0.3 1646 to 10.0.0.3 1813

Command> **set accounting 2 10.0.0.4 1813**

Alternate Accounting Server changed from 0.0.0.0 1646 to 10.0.0.4 1813

See Also

set authentication_server - page 3-31

set secret - page 3-32

set accounting count

This command sets the number of times the PortMaster attempts to send a RADIUS accounting packet to a RADIUS accounting server.

3.9

set accounting count *Number*

Number

Number of times the PortMaster attempts to send a RADIUS accounting packet to a RADIUS accounting server if it does not receive an acknowledgement from a RADIUS accounting server.

Integer between 1 and 99.

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.

When the PortMaster attempts to send a RADIUS accounting packet to the RADIUS accounting server and it does not receive an acknowledgement, it retransmits the packet the number of times set with this command.

If no acknowledgment is sent from the primary accounting server in response to the first packet, the PortMaster sends the packet to both the primary and alternate RADIUS accounting servers.

If an acknowledgement is received from the RADIUS accounting server, the PortMaster no longer tries to resend the accounting packet.

To view the accounting count setting, use the **show global** command.

Example

Command> **set accounting count 45**
Accounting retry count changed from 23 to 45

See Also

set accounting interval - page 3-27

set accounting interval

This command sets the interval between accounting packet retransmissions to a RADIUS accounting server.



set accounting interval *Seconds*

Seconds

Number of seconds that elapse between RADIUS accounting packet retransmissions if not acknowledged by an accounting server.

Integer between 1 and 255. The default is 30 seconds.

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.

When the PortMaster attempts to send a RADIUS accounting packet to the RADIUS accounting server and it does not receive an acknowledgement, it retransmits the packet the number of times set with **set accounting count** command. Use the **set accounting interval** command to set the time interval between attempts to resend the RADIUS accounting packet.

If no acknowledgment is sent from the primary accounting server in response to the first packet, the PortMaster sends the packet to both the primary and alternate RADIUS accounting servers.

To view the accounting count and the accounting interval settings, use the **show global** command.

Example

Command> **set accounting interval 60**
Accounting retry interval changed from 30 to 60 sec

See Also

set accounting count - page 3-26

set alternate_auth_server

This command sets the alternate RADIUS authentication server, which is used if the primary server does not respond.

set alternate_auth_server *Ipaddress* [*Uport*]

<i>Ipaddress</i>	RADIUS alternate authentication server IP address or 39-character hostname. Set <i>Ipaddress</i> to 0.0.0.0 to deselect the alternate authentication server.
<i>Uport</i>	Integer between 0 and 65535 that specifies the UDP port to be used for RADIUS accounting. Setting the port number to 0 or not specifying a port number, sets the UDP port to 1645.

Usage

This address must be different from that of the primary RADIUS authentication server.

Example

Command> **set alternate 10.0.0.4**
Alternate Authentication Server changed from 0.0.0.0 1645 to 10.0.0.4 1645

Command> **set alternate 10.0.0.4 1812**
Alternate Authentication Server changed from 10.0.0.4 1645 to 10.0.0.4 1812

See Also

set authentication_server - page 3-31

set authentication failover

This command enables the PortMaster to dynamically switch primary and alternate RADIUS authentication servers based on their response to authentication requests.

3.9

set authentication failover on|off

- | | |
|------------|--|
| on | If the primary authentication server fails to respond to three consecutive requests, the PortMaster sends seven requests to both the primary and secondary servers.

If the secondary server replies before the primary server, it becomes the primary server. |
| off | The PortMaster always tries the primary server first. This is the default. |

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.

This command enables the failover feature on the PortMaster. When failover is enabled, the PortMaster does the following:

1. Sends three access-request packets to the primary authentication server and awaits a response.
2. Sends seven requests to both the primary and secondary authentication servers and awaits a response.
3. If the secondary server responds first, designates it as the primary authentication server and sends it the authentication request from the next login attempt.
4. If the designated primary server does not respond after three attempts, starts the failover process again.

The server currently designated as primary is marked with an asterisk (*) in the output of the **show global** command.

To set the request interval, use the **set authentication interval** command.

Example

```
Command> set authentication failover off
Auth failover changed from on to off
```

See Also

set authentication interval - page 3-30

set authentication interval

This command sets the number of seconds that a PortMaster waits for a response from a RADIUS authentication server when the failover feature is enabled, and also sets the failover interval.

 3.9

set authentication interval *Seconds*

Seconds

Value between 1 and 255. The number of seconds that must elapse between RADIUS access-request retransmissions if the PortMaster receives no response from a RADIUS authentication server. The default is 3 seconds, and 0 resets the value to the default. If the primary server does not respond, failover occurs after two times the *Seconds* value. For example, if **set authentication interval 6** is used, failover occurs in 12 seconds.

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.

If you enable the failover feature with the **set authentication failover** command, you can set the access-request interval with the **set authentication interval** command.

The *Seconds* value determines how long the PortMaster waits before sending a subsequent request to the authentication server. In addition, the PortMaster waits two times this value to initiate failover.

Example

```
Command> set authentication interval 15  
Auth retry interval changed from 5 to 15 sec
```

See Also

set authentication failover - page 3-29

set authentication_server

This command sets the primary RADIUS authentication server.

set authentication_server *Ipaddress* [*Uport*]

<i>Ipaddress</i>	IP address or 39-character hostname for a host running a RADIUS authentication server on UDP port 1645. Set <i>Ipaddress</i> to 0.0.0.0 to deselect the primary authentication server.
<i>Uport</i>	Integer between 0 and 65535 that specifies the UDP port to be used for RADIUS accounting. Setting the port number to 0 or not specifying a port number, sets the UDP port to 1645.

Usage

For more information about setting up a RADIUS authentication server, refer to the *RADIUS for UNIX Administrator's Guide*.

Example

```
Command> set authentication 10.0.0.3  
Authentication Server changed from 0.0.0.0 1645 to 10.0.0.3 1645
```

```
Command> set authentication 10.0.0.3 1812
Authentication Server changed from 10.0.0.3 1645 to 10.0.0.3 1812
```

See Also

set accounting - page 3-24
set alternate_auth_server - page 3-30
set secret - page 3-32
set \$0 security - page 5-40

set secret

This command sets the RADIUS shared secret.

set secret *String*

<i>String</i>	Shared secret, which has a maximum of 15 printable, nonspace ASCII characters. The string cannot begin with a question mark (?).
---------------	--

Usage

This value functions as the user's password in a RADIUS Access-Request, and must match the secret used by the RADIUS server.

Example

```
Command> set secret expli7%QZixZZy7
Authentication Secret successfully changed
```

See Also

set authentication_server - page 3-31
set \$0 security - page 5-40

ChoiceNet Client Commands

The ChoiceNet commands in Table 3-5 configure the PortMaster to use a ChoiceNet server.

Table 3-5 ChoiceNet Client Configuration

Command Syntax	
set choicenet [1 2] <i>Ipaddress</i> [<i>Uport</i>]	- see page 3-33
set choicenet-secret <i>String</i>	- see page 3-34
set debug choicenet on off	- see page 19-5

The following commands configure the PortMaster as a ChoiceNet client. For ChoiceNet server configuration, see the *ChoiceNet Administrator's Guide*.

set choicenet

This command designates a host as the primary or alternate ChoiceNet server.

set choicenet [1|2] *Ipaddress* [*Uport*]

- 1

Designates the primary ChoiceNet server. This is the default.
- 2

If present, designates a host as the alternate ChoiceNet server.
- Ipaddress*

IP address or 39-character hostname of the host running a ChoiceNet server on UDP port 1647. Set *Ipaddress* to 0.0.0.0 to deselect the ChoiceNet server.
- Uport*

Integer between 0 and 65535 that specifies the UDP port to be used for RADIUS accounting. Setting the port number to 0 or not specifying a port number, sets the UDP port to 1647.

Usage

You can designate both primary and alternate ChoiceNet servers, but do not set them to the same IP address.

Example

Command> **set choicenet 10.0.0.5**

ChoiceNet Server changed from 0.0.0.0 1647 to 10.0.0.5 1647

Command> **set choicenet 10.0.0.5 6047**

ChoiceNet Server changed from 10.0.0.5 1647 to 10.0.0.5 6047

set choicenet-secret

This command sets the ChoiceNet secret.

set choicenet-secret *String*

String Shared secret. Maximum length is 15 printable, nonspace ASCII characters. The string cannot begin with a question mark (?).

Usage

The shared secret is used to authenticate communications between the PortMaster and the ChoiceNet server.

Example

Command> **set choicenet-secret vizkaRg76poj**

ChoiceNet Secret successfully changed

See Also

set choicenet - page 3-33

SNMP Commands

The commands in Table 3-6 allow you to configure the PortMaster as a Simple Network Management Protocol (SNMP) agent. Use SNMP writes only if you understand the risks involved.

Table 3-6 SNMP Commands

Command Syntax	
add snmphost reader writer any none <i>Ipaddress</i>	- see page 3-35
clear alarm <i>Alarm-id</i> all	- see page 3-37
delete snmphost reader writer <i>Ipaddress</i>	- see page 3-38
save snmp	- see page 3-38
set snmp on off	- see page 3-39
set snmp readcommunity writecommunity <i>String</i>	- see page 3-40
set sysname <i>String</i>	- see page 2-21
show alarms [<i>Alarm-id</i>]	- see page 3-41
show table snmp	- see page 3-42

add snmphost

This command allows you to control SNMP security by specifying the addresses of the read or write hosts that are permitted to access SNMP information.

add snmphost reader|writer any|none *Ipaddress*

- reader** Adds a read host.
- writer** Adds a write host.

any	All hosts using the correct read or write community string are permitted to read or write SNMP information.
none	No SNMP reads or writes are accepted by the PortMaster.
<i>Ipaddress</i>	IP address or hostname—up to 39 characters—of the read or write host.

Usage

The specification of read and write hosts allows another level of security beyond the community strings. If SNMP hosts are specified, each host wanting to access SNMP information must possess the correct community string and must also be on the read or write host list.

Example

```
Command> add snmphost reader 192.168.1.99  
New SNMP reader 192.168.1.99 successfully added  
Command> add snmphost writer none
```

See Also

delete snmp host - page 3-38
save snmp - page 3-38
set snmp - page 3-39
show table snmp - page 3-42

clear alarm

This command deletes recorded instances of SNMP traps—notifications of certain events.

clear alarm *Alarm-id* | **all**

Alarm-id Number that identifies a specific instance of an alarm. Use the **show alarms** command to display alarm IDs.

all All alarms.

Usage

A recorded instance of an alarm remains unless you use the command **clear alarm**.

Examples

Command> **clear alarm 4763864**

Command> **show alarms**

Alarm Id	Age	Severity	Alarm Message
-----	-----	-----	-----
4764168	19:11	0	Modem failure: card(0) modem(8)
4772816	19:11	0	Modem failure: card(0) modem(9)

Command> **clear alarm all**

Command> **show alarms**

Alarm Id	Age	Severity	Alarm Message
-----	-----	-----	-----

See Also

show alarms - page 3-41

delete snmphost

This command deletes read or write hosts that are allowed to access SNMP information.

delete snmphost reader|writer *Ipaddress*

reader Use to delete a read host.

writer Use to delete a write host.

Ipaddress IP address or hostname of the read or write host.

Example

```
Command> delete snmphost reader 192.168.1.99  
SNMP reader 192.168.1.99 successfully deleted
```

See Also

add snmphost - page 3-35

save snmp

This command saves the settings of the SNMP parameters in the SNMP table.

save snmp

Usage

This command writes the SNMP table settings to the nonvolatile RAM of the PortMaster. You can also use **save all**.

Example

```
Command> save snmp  
SNMP table successfully saved
```

See Also

set snmp - page 3-39

set snmp

This command allows you to enable or disable PortMaster support for SNMP monitoring.

set snmp on|off

on	Enables support for SNMP.
off	Disables support for SNMP. This is the default.

Usage

To enable support for SNMP, you must use **set snmp on**.



Note – After enabling or disabling SNMP, you must use the **save snmp** or **save all** command and reboot the PortMaster before the change takes effect.

Example

```
Command> set snmp on  
SNMP will be enabled after next reboot
```

See Also

add snmp host - page 3-35

save snmp - page 3-38

show modules - page 2-32

show table snmp - page 3-42

set snmp readcommunity|writecommunity

This command sets the read and write community strings used for SNMP security.

set snmp readcommunity|writecommunity *String*

readcommunity Sets the read community.

writecommunity Sets the write community.

String String up to 16 characters long. Default for read is **public**;
default for write is **private**.



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 a different value for the write community string.

Usage

Community strings allow you to control access to the Management Information Base (MIB) information on selected SNMP devices (such as the PortMaster).

A host must know the read community string to read the MIB information, and must know the write community string to set information on the SNMP agent.

Example

```
Command> set snmp read public  
SNMP read community changed to: public
```

See Also

add snmphost - page 3-35
save snmp - page 3-38
set snmp - page 3-39
show table snmp - page 3-42

show alarms

This command displays instances of SNMP traps—notifications of certain events—that have occurred.

3.8

show alarms [*Alarm-id*]

Alarm-id Number that identifies a specific instance of an alarm.

Usage

An alarm is an instance of a trap. The command **show alarms** generates a list of all traps that have occurred—except for recurring traps, which are summarized and identified by an asterisk (*). If SNMP is enabled and a reader is specified, the reader receives traps for PRI, modem, T1 expansion card, and BRI failures.

Examples

For Line0 or Line1:

Command> **show alarms**

Alarm Id	Age	Severity	Alarm Message
-----	-----	-----	-----
4763864	19:11	0	T1 line(0) down
4764168	19:09	0	Modem failure: card(0) modem(8)
4772816	19:09	0	Modem failure: card(0) modem(9)

Command> **show alarms 4763864**

```

----- Alarm Details -----
Alarm Id: 4763864                Alarm Message: T1 line(0) down
Alarm in minutes: 19:11          Alarm repeated: 1 times
Severity: 0                      Reported: SNMP
For line2, on the T1 expansion card:

```

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

See Also

clear alarm - page 3-37

show table snmp

This command shows the settings in the SNMP table.

show table snmp

Usage

The SNMP table is used to check the settings for the SNMP read and write communities, which should be set so that configuration information is not changed by unauthorized users.

Example

Command> **show table snmp**
SNMP Readers (public): Any
SNMP Writers (private): None

See Also

save snmp - page 3-38

set snmp - page 3-39

This chapter describes how to use the command line interface to configure the Ethernet interface and subinterfaces of the PortMaster. Detailed command definitions follow a command summary table.

Examples in this chapter are from a PortMaster 2R, which uses Ether0 for its Ethernet interface. All PortMaster products use this same designation. In addition, the PortMaster IRX-211 uses Ether1 for a second Ethernet interface.

Displaying Ethernet Information

To display information about your configuration, use the following commands:

- **ifconfig**—see page 2-9
- **show all**—see page 2-22
- **show arp** *Ether0*—see page 2-24
- **show** *Ether0*
- **show global**—see page 2-28
- **show netconns**—see page 2-33
- **show netstat**—see page 2-34
- **show table subinterface**

For general information about command line interface commands, refer to Chapter 1, “Introduction.”

Summary of Ethernet Commands

The Ethernet commands in Table 4-1 configure the Ether0 Ethernet interfaces and—except as noted—the Ether1 interface on the IRX-211.

Ethernet subinterface commands are summarized in Table 4-2, on page 4-13.

Table 4-1 Ethernet Configuration

Command Syntax	
set Ether0 address <i>Ipaddress</i> [/NM] [Netmask]	- see page 4-3
set Ether0 broadcast high low	- see page 4-4
set Ether0 ifilter <i>Filtername</i>	- see page 4-5
set ether0 ip enabled disabled ¹	- see page 4-6
set ether0 ipx enabled disabled ¹	- See page 4-7
set Ether0 ipxframe ethernet_802.2 ethernet_802.2_ii ethernet_802.3 Ethernet_ii	- See page 4-8
set Ether0 ipxnet <i>Ipxnetwork</i>	- See page 4-9
set Ether0 nat inmap outmap defaultnapt Mapname blank [outsourc]	- see page 14-14
set Ether0 nat log sessionfail sessionsuccess syslog console on off	- see page 14-16
set Ether0 nat sessiontimeout tcp other Number[minutes seconds]	- see page 14-17
set Ether0 nat session-direction-fail-action drop icmproject passthrough	- see page 14-19
set Ether0 netmask <i>Ipmask</i>	- see page 16-7
set Ether0 ofilter <i>Filtername</i>	- see page 4-10
set Ether0 ospf accept-rip on off	- see page 17-7

Table 4-1 Ethernet Configuration (Continued)

Command Syntax	
set Ether0 ospf on off [cost Number] [hello-interval Seconds]	- see page 17-8
set Ether0 rip broadcast listen on off	- see page 16-19
set Ether0 route-filter incoming outgoing Filtername	- see page 16-8
show Ether0	- see page 4-11

1. This command is available only on the Ethernet port, even on the IRX-211.

Ethernet Commands

These commands affect the Ethernet interface of the PortMaster. The Ethernet interface of the PortMaster is called Ether0 on all models. In addition, the IRX-211 has a second Ethernet interface called Ether1. All Ether0 commands can be used for Ether1, except as noted in this section.

set Ether0 address

This command sets the IP address of the Ethernet interface.

set Ether0 address Ipaddress [/NM] [Netmask]

<i>Ether0</i>	Ethernet interface.
<i>Ipaddress</i>	IP address or hostname.
<i>/NM</i>	Optional netmask—an integer between 1 and 32 that indicates the number of high-order bits set to 1. Enter a slash (/) between the IP address and the netmask in bits.
<i>Netmask</i>	Optional netmask expressed in dotted decimal notation. Enter a space between the IP address and the netmask.

Usage

For more information about setting the IP address, refer to the hardware installation guide for your PortMaster.



Note – If you change the IP address of the Ethernet interface, you must disable and then re-enable IP on the Ethernet interface for the change to take effect.

Example

```
Command> set ether0 address 172.16.200.1
Local (ether0) address changed from    to 172.16.200.1
```

See Also

set Ether0 netmask - page 16-7

set Ether0 broadcast

This command determines which broadcast address the PortMaster will use.

set Ether0 broadcast high|low

<i>Ether0</i>	Ethernet interface.
high	Use a host part of all ones (for example, 192.168.1.255) in the broadcast address.
low	Use a host part of all zeros (for example, 192.168.1.0) in the broadcast address. This is the default.

Usage

This setting must match the broadcast address used by all hosts and routers on the same network segment.

Example

Command> **set ether0 broadcast high**
ether0 broadcast address changed from low to high

set Ether0 ifilter

This command sets a packet filter for evaluating packets entering the PortMaster on the Ethernet interface.

set Ether0 ifilter *Filtername*

Ether0 Ethernet interface.

Filtername Input filter name that is in the filter table. *Filtername* can be up to 15 characters.

Usage

The filter must be created before it can be used. Refer to the *PortMaster Configuration Guide* for more information on how to construct a filter. If the filter is changed, this command must be re-entered for the changes to take effect on the Ethernet interface.

Neither the interface nor the PortMaster needs to be reset or rebooted for the filter to be effective. You remove the filter by entering the command without a filter name.



Note – You can set the *filtername* to the Ethernet interface before the filter is created, but doing so allows packets to pass through without any packet filtering.

Example

```
Command> set ether0 ifilter ether0.in
ether0 filters enabled: in = ether0.in, out =
```

See Also

set Ether0 ofilter - page 4-10
show filter - page 13-24
show table filter - page 13-25

set ether0 ip

This command enables or disables the IP protocol on the Ether0 interface.

set ether0 ip enabled|disabled

enabled	Enables IP. This is the default.
disabled	Disables IP.

Usage

This command is available only on the Ether0 interface, even on the IRX-211.

Example

```
Command> set ether0 ip enabled
ether0 status for protocol IP changed from Disabled to Enabled
```


set ether0 ipx

This command enables or disables the IPX protocol on the Ether0 interface.

set ether0 ipx enabled|disabled

enabled Enables IPX. This is the default.

disabled Disables IPX.

Usage

This command is available only on the Ether0 interface, even on the IRX-211.

Example

Command> **set ether0 ipx enabled**
ether0 status for protocol IPX changed from Disabled to Enabled

See Also

set ipx on - page 3-9

set Ether0 ipxframe

This command sets the IPX frame type.



Note – Enter this command on one line, without any breaks. The line break shown here is due to the limited space available.

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

<i>Ether0</i>	Ethernet interface.
ethernet_802.2	Uses the Ethernet 802.2 protocol. This is the default encapsulation used by Novell NetWare 4.0.
ethernet_802.2_ii	Uses the Ethernet 802.2_ii protocol. This encapsulation is not commonly used.
ethernet_802.3	Uses the Ethernet 802.3 protocol. This is the default encapsulation used by Novell NetWare 3.11.
ethernet_ii	Uses the Ethernet II protocol. This encapsulation is sometimes used for networks that handle both TCP/IP and IPX traffic.

Usage

The encapsulation method and frame type were selected when your Novell IPX network servers were installed. The PortMaster IPX settings must match those of your IPX network.

Example

```
Command> set ether0 ipxframe ethernet_ii  
ether0 IPX frame type set to ethernet_ii
```

See Also

set Ether0 ipxnet - page 4-9

set ipx on - page 3-9

set Ether0 ipxnet

This command sets the IPX network number for the Ethernet interface.

set Ether0 ipxnet Ipxnetwork

Ether0 Ethernet interface.

Ipxnetwork A 32-bit hexadecimal value.

Usage

Enter the IPX network number in hexadecimal format, as shown in the example. You must enable IPX before using this command.

Example

Command> **set ether0 ipxnet 0x0000000f**
ether0 IPX network changed from 00000000 to 0x0000000f

See Also

set Ether0 ipxframe - page 4-8

set ipx on - page 3-9

set user ipxnet - page 7-14

set Ether0 ofilter

This command sets a packet filter for evaluating packets exiting the PortMaster on the Ethernet interface.

set Ether0 ofilter *Filtername*

Ether0 Ethernet interface.

Filtername Output filter name, up to 15 characters, that is in the filter table.

Usage

The filter must be created before it can be used. Refer to the *PortMaster Configuration Guide* for more information on how to construct a filter. If the filter is changed, this command must be re-entered for the changes to take effect on the Ethernet interface.

Neither the interface nor the PortMaster needs to be reset or rebooted for the filter to be effective. You remove the filter by entering the command without a filter name.



Note – You can set the *filtername* to the Ethernet interface before the filter is created, but doing so allows packets to pass through without any filtering.

Example

```
Command> set ether0 ofilter ether0.out  
ether0 filters enabled: in = ether0.in, out = ether0.out
```

See Also

set Ether0 ifilter - page 4-5
show filter - page 13-24
show table filter - page 13-25

show Ether0

Shows configuration values for the Ethernet interface.

show Ether0

Command> **show ether0**

Ethernet Status: IP - Enabled IPX - Disabled

Interface Addr: pm2.edu.com (192.168.96.6)

Netmask: 255.255.255.0

Broadcast Address: 192.168.96.0

IPX Network: 00000000

IPX Frame Type: ETHERNET_802.2

Ethernet Address: 00:c0:05:01:06:20

Routing: OSPF, RIP(Listen)

OSPF Accept RIP: off

OSPF Cost: 1

OSPF Hello Interval: 10

OSPF Dead Time: 40

Input Filter:

Output Filter:

Explanation

Ethernet Status	Shows IP and IPX protocols enabled for the Ethernet port.
Interface Addr	The IP address for the Ethernet interface.
Netmask	The netmask used on the network.
Broadcast Address	The IP address used as the local broadcast address.
IPX Network	The IPX network segment address.
IPX Frame Type	The IPX frame type that identifies the encapsulation method used on the IPX interfaces.
Ethernet Address	The Ethernet hardware MAC address.
Routing	<ul style="list-style-type: none">• Broadcast—the PortMaster broadcasts route information on the local Ethernet.• Listen—the PortMaster listens for route information from other routers on the local Ethernet.
OSPF Accept RIP	RIP routes learned on the Ethernet interface that are propagated into OSPF as Type 2 external routes.
OSPF Cost	Cost of sending a packet on the interface.
OSPF Hello Interval	Interval in seconds that elapses between the transmission of hello packets on the interface.
OSPF Dead Time	Number of seconds the PortMaster waits after ceasing to receive a neighbor router's hello packets and before identifying the remote router as unreachable.
Input Filter	The name of the input filter attached to the Ethernet interface.
Output Filter	The name of the output filter attached to the Ethernet interface.

Ethernet Subinterface Commands

In ComOS 3.8 and later, you can configure a single Ethernet port for multiple IP subnets. The MAC address for the subinterfaces is the same as for the primary interface.



Note – IPX, RIP, OSPF, packet filtering, and route propagation are not supported on the subinterfaces.

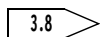
The commands in Table 4-2 configure and manage Ether0 and Ether1 for subinterfaces.

Table 4-2 Ethernet Subinterface Configuration

Command Syntax	
add subinterface <i>Name</i>	- see page 4-14
delete subinterface <i>Name</i>	- see page 4-14
set subinterface <i>Name</i> address <i>Ipaddress</i> [<i>/NM</i>] [<i>Netmask</i>]	- see page 4-15
set subinterface <i>Name</i> broadcast <i>high low</i>	- see page 4-16
set subinterface <i>Name</i> netmask	- see page 4-16
set subinterface <i>Name</i> port <i>Portlabel</i>	- see page 4-17
show table subinterface	- see page 4-18

add subinterface

This command adds a subinterface entry to the subinterface table.



add subinterface *Name*

Name Name of the subinterface configuration in the subinterface table. *Name* can contain up to 11 characters.

Usage

The new interface is displayed in the **ifconfig** output after the subinterface is configured with an IP address and a port label. The interface name is system generated.

Example

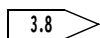
Command> **add subinterface net2**
New subinterface net2 successfully added

See Also

show table subinterface - page 4-18

delete subinterface

This command removes a subinterface entry from the table.



delete subinterface *Name*

Name Name of an existing subinterface configuration.

Usage

You must use *Name* exactly as it is listed in response to a **show table subinterface** command.

Example

Command> **delete subinterface net2**

set subinterface address

This command assigns an IP address or an IP address and netmask to the subinterface configuration.

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

<i>Name</i>	Name of the subinterface configuration. <i>Name</i> can be up to 11 characters.
<i>Ipaddress</i>	IP address or 39-character hostname.
<i>/NM</i>	Optional netmask—an integer between 1 and 32 that indicates the number of high-order bits set to 1. Enter a slash (/) between the IP address and the netmask in bits.
<i>Netmask</i>	Optional netmask expressed in dotted decimal notation. Enter a space between the IP address and the netmask.

Examples

Command> **set subinterface net2 address 192.168.11.1 255.255.255.0**

Overlapping with interface et01

net2 changed from 192.168.11.1/24 to 192.168.11.1/24

Command> **set subinterface net2 address 192.168.55.6/27**

net2 changed from 192.168.55.6/24 to 192.168.55.6/27

Command> **set subinterface net2 netmask 255.255.255.0**

net2 netmask changed from 0.0.0.0 to 255.255.255.0

set subinterface broadcast

This command determines the broadcast address for the subinterface.

 **set subinterface** *Name* **broadcast high|low**

Name Name of the subinterface configuration. *Name* can be up to 11 characters.

high Uses a host part of all ones in the broadcast address.

low Uses a host part of all zeros in the broadcast address.

Example

Command> **set subinterface net2 broadcast high**
net2 broadcast address changed from low to high

See Also

set Ether0 broadcast - page 4-4

set subinterface netmask

This command sets the netmask in dotted decimal notation for the subinterface configuration.

 **set subinterface** *Name* **netmask** *Netmask*

Name Name of the subinterface configuration. *Name* can be up to 11 characters.

Netmask Netmask expressed in dotted decimal notation.

Usage

This command is not needed if you set the netmask using either the classless interdomain routing (CIDR) notation (/xx) or dotted decimal notation in the **set subinterface address** command.

Example

```
Command> set subinterface net2 netmask 255.255.255.0
net2 netmask changed from 0.0.0.0 to 255.255.255.0
```

See Also

set subinterface address - page 4-15

set subinterface port

This command associates the subinterface configuration with a physical port.

 **set subinterface** *Name* **port** *Portlabel*

Name The name of the subinterface configuration in the subinterface table. *Name* can be up to 11 characters.

Portlabel **ether0** or **ether1**.

Example

```
Command> set subinterface net2 port ether0
net2 changed from to ether0
```

show table subinterface

This command displays the subinterface table.



show table subinterface

Example

Command> show table subinterface				
Subinterface	Interface	Addr	Netmask	Broadcast Addr Port Name

net2	192.168.55.6		255.255.255.0	192.168.55.255 ether0

This chapter describes how to use the command line interface to configure asynchronous ports. Detailed command definitions follow a command summary table. A summary table for the modem table commands also appears in this chapter, followed by a description of the commands.

Asynchronous ports can be configured as login, device, or network ports, or any combination of these.

Examples in this chapter are from a PortMaster 2R, which uses the indicator *S0* for the first asynchronous port. Some PortMaster models use this same designation for the first asynchronous port, while others use the designation *C0*. See Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1 for the range of asynchronous ports available on each PortMaster model.

Many commands in this chapter also show the designation *S10* to indicate commands you can use to configure ISDN BRI ports. See Chapter 11, “ISDN BRI Ports,” for more information.

Note – After making any configuration changes to an asynchronous port, you must use the **reset s0** command for the changes to take effect.



Displaying Asynchronous Port Information

To display information about your configuration, use the following commands:

- **show S0**—see page 2-35
- **show all**—see page 2-22
- **ifconfig**—see page 2-9
- **show sessions**—see page 2-39

For general information about command line interface commands, refer to Chapter 1, “Introduction.”

Summary of Asynchronous Commands

The asynchronous port commands in Table 5-1 configure asynchronous serial ports. Commands marked with a leading bullet (•) can be used only if the port is configured for a dedicated network connection with the **set network hardwired** command.

Commands for modems attached to asynchronous port are summarized in Table 5-4, on page 5-49.

Table 5-1 Asynchronous Port Configuration

Command Syntax	
add modem <i>ModemName(short) ModemName(long) Speed String</i>	- see page 5-5
attach <i>S0</i>	- see page 5-6
delete modem <i>ModemName(short)</i>	- see page 5-8
reset <i>S0</i>	- see page 2-15
save ports	- see page 2-18
save <i>S0</i>	- see page 2-18
set <i>S0 all access on off</i>	- see page 5-9
• set <i>S0 address Ipaddress</i>	- see page 5-10
set <i>S0 all cd on off</i>	- see page 5-11
• set <i>S0 compression on off stac vj</i>	- see page 5-13
set <i>S0 all databits 5 6 7 8</i>	- see page 5-14
• set <i>S0 destination Ipaddress [Ipmask]</i>	- see page 5-15
set <i>S0 device Device [network dialin dialout twoway]</i>	- see page 5-16
set <i>S0 all dialback_delay Seconds</i>	- see page 5-17
set <i>S0 all dtr_idle on off</i>	- see page 5-18
set <i>S0 extended on off</i>	- see page 5-19
set <i>S0 all group Group</i>	- see page 5-19
set <i>S0 all hangup on off</i>	- see page 5-20
set <i>S0 all host default prompt [1 2 3 4]Ipaddress</i>	- see page 5-21
set <i>S0 all idletime Number [minutes seconds]</i>	- see page 5-22
• set <i>S0 all ifilter [Filtername]</i>	- see page 5-24

Table 5-1 Asynchronous Port Configuration (Continued)

Command Syntax	
• set S0 ipxnet Ipxnetwork	- see page 5-25
set S0 all login [network dialin dialout twoway]	- see page 5-26
• set S0 all map Hex	- see page 5-27
set S0 all message String	- see page 5-28
set S0 all modem-type ModemName	- see page 5-29
• set S0 all mtu MTU	- see page 5-30
set S0 nat inmap outmap defaultnapt Mapname blank [outsource]	- see page 14-14
set S0 nat log sessionfail sessionsuccess syslog console on off	- see page 14-16
set S0 nat sessiontimeout tcp other Number[minutes seconds]	- see page 14-17
set S0 nat session-direction-fail-action drop icmproject passthrough	- see page 14-19
• set S0 netmask Ipmask	- see page 5-31
set S0 all network dialin dialout twoway	- see page 5-32
set S0 all network hardwired	- see page 5-33
• set S0 all ofilter Filtername	- see page 5-34
• set S0 ospf on off [cost Number] [hello-interval Seconds][dead-time Seconds] [nbma point-to-multipoint wan-as-stub-ptmp]	- see page 17-9
set S0 all override xon rts speed parity databits on off	- see page 5-35
set S0 all parity even none odd strip	- see page 5-36
set S0 all prompt String	- see page 5-37
• set S0 protocol slip ppp x75-sync	- see page 5-38
• set S0 all rip on off broadcast listen	- see page 16-19
set S0 route-filter incoming outgoing Filtername	- see page 16-8
set S0 all rts/cts on off	- see page 5-39
set S0 all security on off	- see page 5-40

Table 5-1 Asynchronous Port Configuration (Continued)

Command Syntax	
set S0 all	- see page 5-41
service_device netdata portmaster rlogin telnet [Tport]	
set S0 all service_login	- see page 5-42
netdata portmaster rlogin telnet [Tport]	
set S0 all speed [1 2 3] 300 600 1200 2400 4800 9600 19200 38400 57600 76800 115200	- see page 5-43
set S0 all stopbits 1 2	- see page 5-44
set S0 all termtype String	- see page 5-45
set S0 twoway Device [network dialin dialout twoway]	- see page 5-46
set S0 username autolog [String]	- see page 5-47
set S0 all xon/xoff on off	- see page 5-48
show all	- see page 2-22
show S0	- see page 2-35

Asynchronous Port Types

Asynchronous port types are described in Table 5-2. The first three options can be combined with the last three options. A port configured as a network hardwired port cannot be combined with another port type.

Table 5-2 Asynchronous Port Types

Port Type	Description
login	The port allows a user to log in and establish a terminal session to a host on the network.
device	The port allows a user to access a shared device—for example, a printer or modem—via a host on the network, which can originate a connection to the port.
twoway	The port allows both inbound and outbound connections—user login and shared modem device connections, in this case.

Table 5-2 Asynchronous Port Types (Continued)

Port Type	Description
network hardwired	The port provides a permanent network connection—for example, a WAN link over a dedicated point-to-point asynchronous leased line.
network dialin	The port allows a dial-in network user to establish a network connection using SLIP or PPP.
network dialout	The port allows network users to dial out to remote locations—the Internet or another office, for example—defined in the location table.
network twoway	The port allows both inbound and outbound connections—network dial-in and network dial-out connections, in this case.

Asynchronous Commands

These commands affect the asynchronous ports of the PortMaster. Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1 lists the range of asynchronous ports available on each PortMaster model.

add modem

This command adds modem details and configuration information to the modem table.

add modem *ModemName(short)* "*ModemName(long)*" *Speed* "*String*"

<i>ModemName(short)</i>	Abbreviated name used to identify the modem. Up to a maximum of 16 characters.
" <i>ModemName(long)</i> "	Long name that includes modem information—for example, the manufacturer or model name. Enclose the name in quotation marks. Up to a maximum of 64 characters.
<i>Speed</i>	The DTE speed in bits per second.

"String"

The initialization **send/expect** string for the modem. Enclose the string in quotation marks. Use a **\r** for a carriage return, and a caret (^) to separate the send and expect characters in the string. The PortMaster expects **OK**, as shown in the example.

Usage

The short and long names are chosen by the user.

Example

```
Command> add modem multitech-v34
"at&f&w\r^OK^at&c1&d3$ba0$sb115200s0=1&w\r^OK"
New script entry successfully added.
Modem multitech-v34 successfully added.
```

See Also

show modem - page 5-49

show table modem - page 5-50

attach S0

This command allows you to communicate directly to a device attached to a specified asynchronous or ISDN PortMaster port.

attach S0|S10

Usage

Typical uses of this command are as follows:

- Programming a modem attached to an asynchronous port on the PortMaster
- Debugging a dial-out location on the PortMaster

You can use AT commands with a host attached to an analog modem connected to a PortMaster asynchronous port.

When your host is attached to a modem connected to an ISDN BRI or PRI line, you can use the following special AT commands to make an outbound call with the following services:

at&n—Unrestricted 64Kbps data connection.

at&n0—3.1KHz audio service. On a PortMaster 3, use this command to place a modem call.

at&n1—Speech service. On a PortMaster 3, use this command to place a modem call.

at&n55—3.1KHz audio service.

at&n56—Restricted 56Kbps data connection.

at&n64—Unrestricted 64Kbps data connection.



Note – The speech service and 3.1KHz audio service each uses a single voice-grade channel. The speech service, however, can be used with compression and encoding techniques that are appropriate only for human speech. The 3.1KHz audio service is useful for data-over-voice communications between countries using T1 lines—such as the U.S.A., and countries using E1 lines—such as those in Europe.

Each of these special AT commands returns an “OK.” You must then enter the **atdt + telephone number** command to place the call.

Example

To communicate directly to an analog modem attached to asynchronous port S5, and configure the modem with the AT command **at&f1s0=1&w**, use the **attach** command as follows:

```
Command> attach s5
Trying 192.168.1.1
Connected - Escape character is '^]' (Ctrl + Right bracket)
at&f1s0=1&w
OK
^]
telnet> send esc
Connection Closed
Command>
```

See Also

add modem - page 5-5
set location script - page 8-24
reset nHandle - page 2-15

delete modem

This command deletes a modem entry from the modem table.

delete modem *ModemName(short)*

<i>ModemName(short)</i>	The abbreviated name used to identify the modem when it was added to the modem table.
-------------------------	---

Usage

Use the modem short name in the command, exactly as it is listed in the response to a **show table modem** command.

Example

Command> **delete modem att-v34**
Modem att-v34 successfully deleted.

See Also

show modem - page 5-49
show table modem - page 5-50

set S0|all access

This command sets the access override for a single asynchronous port or all asynchronous ports, and is used in conjunction with the access filter.

set S0|all access on|off

on Turns access override on.

off Turns access override off. This is the default.

Usage

When access override is set to **on**, users can override the port's access filter with their own access filter by providing a correct username and password. User access filters must first be defined before you can use this option. Refer to the *PortMaster Configuration Guide* for more information on defining access filters.

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

Example

Command> **set s0 access on**

Access Enhancement for port S0 changed from off to on

See Also

set S0 ifilter - page 5-24

set S0 address

This command sets the local IP address of a selected network hardwired asynchronous port to create a numbered interface.

set S0|S10 address *Ipaddress*

Ipaddress IP address or hostname of from 1 to 39 characters.

Usage

If the local IP address is set to 0.0.0.0, the PortMaster uses the *Ether0* IP address for this end of the serial link. If the local IP address is set to 255.255.255.255, the PortMaster negotiates an IP address for the hardwired connection.



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.

Example

Command> **set s0 address 192.168.7.2**
Port S0 local address changed from 0.0.0.0 to 192.168.7.2

See Also

set Ether0 address - page 4-3
set reported_ip - page 3-19

set S0|all cd

This command enables the PortMaster to monitor the presence of the data carrier detect (DCD) signal on a modem attached to the asynchronous port to determine whether the line is in use.

set S0|all cd on|off

- on** Monitors presence of the DCD signal.
- off** Does not monitor presence of the DCD signal. This is the default.

Usage

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

If set **on**, the PortMaster tracks the actual state of the DCD signal as input on the port. If set **off**, the PortMaster assumes that DCD is always asserted—DCD is high.

Table 5-3 indicates the effect of DCD assertion for each port type.

Table 5-3 Effect of DCD Assertion on Ports

Asynchronous Port Type	Effect of DCD Assertion	
	DCD Low—Not Asserted	DCD High—Asserted
login	The port is unavailable.	The PortMaster initiates authentication and displays a login prompt.
device	The port is unavailable.	The port is available for the device service.
twoway	The port is available for device services.	The port attempts to establish an inbound connection and disable the device service.

Table 5-3 Effect of DCD Assertion on Ports (Continued)

Asynchronous Port Type	Effect of DCD Assertion	
	DCD Low—Not Asserted	DCD High—Asserted
network hardwired	The port is unavailable.	The port attempts to establish a network connection.
network dialin	The port is unavailable.	The PortMaster initiates authentication and displays a login prompt.
network dialout	The transition of DCD from asserted to not asserted resets the port.	The port is unaffected. However, a change in DCD to not asserted resets the port.
network twoway	The port is available for network dial-in.	The port attempts to establish a network connection and disable the network dial-in.

Example

Command> set s0 cd on
CD required for port S0 changed from off to on

See Also

add modem - page 5-5
show table modem - page 5-50

set S0 compression

This command sets Van Jacobson TCP/IP header compression and/or Stac LZS data compression on a network hardwired asynchronous port.

set S0 compression on|off|stac|vj

- | | |
|-------------|---|
| on | Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and 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 Office Router products. |
| vj | Enables Van Jacobson TCP/IP header compression only. |

Usage

Van Jacobson TCP/IP header compression can be used for SLIP and PPP connections. With SLIP, both sides need to be configured identically. For PPP connections, the PortMaster supports both bidirectional and unidirectional 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.



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.

Example

```
Command> set s0 compression on
Compression for port S0 changed from off to on
```

See Also

set location compression - page 8-9

set S0 protocol - page 5-38

set user compression - page 7-8

set S0|all databits

This command sets the number of data bits per byte for a single asynchronous port or all asynchronous ports.

set S0|all databits 5|6|7|8

5	5 data bits.
6	6 data bits.
7	7 data bits.
8	8 data bits. This is the default.

Usage

The default of 8 is the most widely used.

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

Example

Command> **set s0 databits 8**

Data bits for port S0 changed from 7 to 8

See Also

set S0 modem-type - page 5-29

set S0 parity - page 5-36

set S0 speed - page 5-43

set S0 stopbits - page 5-44

set S0 destination

This command sets the IP address and the netmask of the remote router for a network hardwired asynchronous port connection.

set S0 destination *Ipaddress* [*Ipmask*]

Ipaddress IP address or hostname, from 1 to 39 characters, of the remote router.

Ipmask IP netmask in dotted decimal notation.

Usage

If the remote destination is set to 255.255.255.255 for PPP connections, the PortMaster attempts to learn the remote system IP address. If the destination is set to 0.0.0.0, the port is disabled.



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

Example

Command> **set s0 destination 255.255.255.255**
Port S0 destination changed from 0.0.0.0 to 255.255.255.255

See Also

set W1 destination - page 6-9

set S0 device

This command sets an asynchronous port to provide access to a shared network device via a host—or for device sharing and remote dial-in and/or dial-out access.

set S0|S10 device Device [network dialin|dialout|twoway]

<i>Device</i>	Designation for the shared host device—usually a printer or modem—for example, /dev/ttyp0 or /dev/network .
dialin	In addition to allowing device sharing, the port accepts dial-in-only network connections. The remote system is required to enter a username and password. Dial-in connections to the network are controlled by the RADIUS server or the user table.
dialout	In addition to allowing device sharing, the port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial-out connections from the network are controlled by the location table.
twoway	In addition to allowing device sharing, the port accepts dial-in connections to the network, as well as being available for dial-out to remote destinations.

Usage

An asynchronous port configured as a device port operates as a host device. You must also do the following to establish device sharing:

- Define a login host with the **set S0 host** command.
- Define the method used to connect the user to the port and device by selecting a device service with the **set S0 device_service** command.

To use the PortMaster device service, you must have the PortMaster **in.pmd** daemon installed and running on the specified host.

In addition to setting an asynchronous port for device sharing, you can also set it for network dial-in and/or dial-out use by multiple users. Multiple users can dial in to the network through the port from remote locations, dial out from the network through the port to remote locations—like another office or the Internet—or both.

In the following example, a PortMaster shared device—**/dev/ttyp0**—is shown. Note that two ports cannot have the same tty designation.

Example

```
Command> set s0 device /dev/ttyp0
Port type for port S0 changed from User Login to Host Device(/dev/ttyp0)
```

See Also

set S0 host - page 5-21
set S0 login - page 5-26
set S0 twoway - page 5-46

set S0|all dialback_delay

This command sets the delay between the disconnection of a callback user and the time when the PortMaster can return the user's call to establish a connection.

set S0|S10|all dialback_delay Seconds

Seconds The delay time from 0 to 60, in seconds. The default is 0.

Usage

Modems that take a long time to reset after DTR drops require a callback delay, so that the modem is ready to accept dial commands after the PortMaster has disconnected the user.

You can simultaneously set the delay time for all ports by using the **set all dialback_delay** command.

Example

```
Command> set s0 dialback_delay 5
Dialback delay for port S0 changed from 0 to 5
```

See Also

set user dialback - page 7-9

set S0|all dtr_idle

This command turns the DTR signal off to enable bidirectional communications, or turns it back on.

set S0|all dtr_idle on|off

on DTR is on, and any DTR drop is for 500ms. This is the default.

off DTR is off. Allows bidirectional communications.

Usage

This command changes the behavior of the port to better accommodate connecting the PortMaster to systems or hosts that do not support TCP/IP, but do have serial ports. This type of connection requires that you connect the PortMaster port to the host, typically with a null modem cable.

Set DTR idle when you want to connect a PortMaster to a bulletin board service (BBS) or other host allowing bidirectional communications. You can simultaneously turn DTR on or off on all ports by using the **set all dtr_idle** command.

Refer to the *PortMaster Configuration Guide* for more information.

Example

```
Command> set s0 dtr_idle off  
DTR Idle for port S0 changed from on to off
```

See Also

set S0 hangup - page 5-20

set S0 modem-type - page 5-29

set S0|all extended

This command sets the extended mode on or off for a single asynchronous port, or for all asynchronous ports.

set S0|S10|all extended on|off

on Turns extended mode on.

off Turns extended mode off. This is the default.

Usage

When extended mode is **on**, the **show** command provides more detailed output.

Example

Command> **set s0 extended on**

Extended mode for port S0 changed from off to on

set S0|all group

This command assigns asynchronous ports to modem pools for use by dial-out locations. A group number is assigned to each location in the location table. Refer to Chapter 8, “Locations and DLCIs,” for more information.

set S0|S10|all group Group

Group Group number, from 0 to 100. Default is 0.

Usage

For dial-out modem pools to work, each port must be assigned to a dial group, and each location must specify a dial group. All ports can be assigned to a single group with the **set all group Group** command.

Example

Command> **set s0 group 2**

Group number for port S0 changed from 0 to 2

See Also

set location group - page 8-11

set S0|all hangup

This command controls whether the DTR signal on a port, or on all ports, is dropped for 500 milliseconds (ms) after the termination of a user session.

set S0|S10|all hangup on|off

on DTR is dropped after the session terminates.
This is the default.

off DTR is not dropped after the session terminates.

Usage

Resetting the port administratively with the **reset** command always drops the DTR signal.

Example

Command> **set s0 hangup on**

DTR Hangup for port S0 changed from off to on

See Also

reset S0 - page 2-15

set dtr_idle - page 5-18

set S0|all host

This command sets the default IP address or hostname for login sessions for a single asynchronous port or all asynchronous ports.

```
set S0|S10|all host default|prompt| [1|2|3|4] Ipaddress
```

default	Uses the default host setting.
prompt	Displays the host prompt before the login prompt. The user is required to enter a valid hostname or Internet address for a host on the network. Entering PPP or SLIP at the prompt returns a login prompt.
<i>Ipaddress</i>	A specified IP address or hostname of a login host or device host.
1 2 3 4	Used to specify alternate hosts, with the primary host being 1. The default is 1.



Note – Global host setting is not available on PortMaster IRX products.

Usage

The login host is the host to which the user is connected upon login, in one of the three ways. Use the **set host** command to define a default host. After you set the login host on a port, prompts are displayed in the following order:

```
host:
login:
Password:
```

You can set the login host for all asynchronous ports simultaneously by using the **set all host** command, as shown in the example.

If you do not want the PortMaster to provide login or host device service, do not use this command. Setting the hostname to 0.0.0.0 removes the entry.

Examples

Command> **set host 172.16.200.1**
Default host changed from to 172.16.200.1

Command> **set s0 host prompt**
User will be prompted for host on port S0

Command> **set all host default**
Host changed to default for all ports

See Also

set S0 service_device - page 5-41
set S0 service_login - page 5-42
set user host - page 7-10

set S0|all idletime

This command indicates how long the PortMaster waits after outbound activity stops on a single asynchronous port or all asynchronous ports, before disconnecting a dial-in connection.

set S0|S10|all idletime *Number* [**minutes**|**seconds**]

Number Timeout value in minutes or seconds. Any value from 0 to 240.
The default value is 0.

minutes Sets the idle time in minutes. This is the default.

seconds Sets the idle time in seconds.

Usage

If the idle time value is set to 0, the idle timer is disabled.

If the idle time is 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 and becomes available to another user. Setting the idle time to 1 second turns off the idle timer after the user logs in. If the value is set to 2 seconds or a longer interval, the port is reset after having no traffic for the designated time.



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 was 1 minute.

You can set the idle time of all asynchronous ports simultaneously by using the **set all idletime** command as shown in the second example.

Examples

Command> **set s0 idletime 15**

Idle timeout for S0 changed from 0 minutes to 15 minutes

Command> **set all idletime 120 seconds**

Idle timeout for S0 changed from 0 minutes to 120 seconds

Idle timeout for S1 changed from 0 minutes to 120 seconds

Idle timeout for S2 changed from 0 minutes to 120 seconds

.
.

Idle timeout for S29 changed from 0 minutes to 120 seconds

See Also

set S0 cd on - page 5-11

set S0|all ifilter

This command sets an input packet filter for packets entering the PortMaster on a single network hardwired asynchronous port, or all network hardwired asynchronous ports. The command can also be used to set an access filter for login users on these ports.

set S0|S10|all ifilter [*Filtername*]

Filtername Input filter name that is in the filter table. Maximum of 15 characters.

Usage

When an input filter is specified on a network hardwired port, all packets received from the interface are evaluated against the rule set for this filter.

This filter is used as an access filter for login users who are prompted for a host, and as the input filter for network hardwired ports. Filters become effective after the port is reset and when a user logs in.

This setting is not used for dial-in and dial-out networking. Filters for dial-in users are set in the user table or RADIUS, and filters for dial-out locations are set in the location table.

You remove the filter by entering the command without a filter name.

You can set the input filter for all hardwired asynchronous ports simultaneously by using the **set all ifilter** command.



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.

Example

Command> **set s0 ifilter s0.in**
Input filter for port S0 changed from to s0.in

See Also

add filter - page 13-4

set S0 ofilter - page 5-34

set S0 ipxnet

This command sets the IPX network number for the network hardwired asynchronous or synchronous connection.

set S0 ipxnet *Ipxnetwork*

Ipxnetwork IPX network number—a 32-bit hexadecimal value.

Usage

IPX traffic can be passed through a port if you assign an IPX network number to the hardwired network connection. The serial link itself must have a unique IPX network number that is different from those at each end of the Ethernet.



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

Example

Command> **set s0 ipxnet 0XC009C801**

Port S0 ipxnet changed from 00000000 to **0XC009C801**

See Also

set Ether0 ipxnet - page 4-9

set ipx on - page 3-9

set W1 ipxnet - page 6-16

set S0|all login

This command sets a single asynchronous port or all asynchronous ports for user login—or for user login and remote dial-in and/or dial-out access.

set S0|S10|all login [network dialin|dialout|twoway]

- | | |
|----------------|--|
| dialin | In addition to allowing user login, the port accepts dial-in-only network connections. The remote system is required to enter a username and password. Dial-in connections to the network are controlled by the RADIUS server or the user table. |
| dialout | In addition to allowing user login, the port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial-out connections from the network are controlled by the location table. |
| twoway | In addition to allowing user login, the port accepts dial-in connections to the network, as well as being available for dial-out to remote destinations. |

Usage

Using the **set S0 login** command with no optional keywords sets the port for user login. You must also do the following if the host and service settings are not configured in the user profile:

- Define a login host with the **set S0 host** command.
- Define a login service with the **set S0 service_login** command.

After being verified, or authenticated, a login session is established to the host computer.

In addition to setting an asynchronous port for user login, you can also set it for network dial-in and/or dial-out use by multiple users. Multiple users can dial in to the network through the port from remote locations, dial out from the network through the port to remote locations—like another office or the Internet—or both.

By using the **all** keyword, you can set the port type to user login—and to **network dialin**, **network dialout**, or **network twoway**—for all asynchronous ports simultaneously, as shown in the second example.

Examples

Command> **set s0 login network dialin**

Port type for port S0 changed from Login to User Login/Network(dialin)

Command> **set all login network twoway**

Port type for port S0 changed from Netwrk to User Login/Network(twoway)

Port type for port S1 changed from Netwrk to User Login/Network(twoway)

Port type for port S2 changed from Netwrk to User Login/Network(twoway)

· · · · ·
Port type for port S29 changed from Network to User Login/Network(twoway) ·

See Also

set S0 device - page 5-16

set S0 host - page 5-21

set S0 service_login - page 5-42

set S0|all map

This command sets the PPP asynchronous map for the interpretation of nonprinting ASCII characters found in the data stream for a single network hardwired asynchronous port, or all network hardwired asynchronous ports.

set S0|all map Hex

Hex A 32-bit hexadecimal number. The default is 0x00000000.

Usage

The PPP protocol supports the replacement of nonprinting ASCII data in the PPP stream. These characters are not sent through the line, but instead are replaced by a special set of characters that the remote site interprets as the original characters. The PPP asynchronous map is a bit map of characters that should be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments should set the asynchronous map to 0 (zero) to achieve maximum throughput. This command does not apply to the Serial Line Internet Protocol (SLIP).

You can set the PPP asynchronous map for all the hardwired asynchronous ports simultaneously by using the **set all map** command. The command **set S0 map 0** disables the asynchronous mapping.



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.

Example

Command> **set s0 map 0xc0a86000**

Async Char Map for port S0 changed from 0x0 to 0xc0a86000

See Also

set location map - page 8-17

set S0 protocol - page 5-38

set user map - page 7-16

set S0|all message

This command sets the login message to be displayed to the user prior to the login prompt on a single asynchronous port or all asynchronous ports.

set S0|S10|all message *String*

<i>String</i>	Login message—maximum is 224 characters, or 224 characters minus the login prompt, if set.
---------------	--

Usage

The value for this parameter is a string. Use the caret symbol (^) to designate new lines. It can be helpful to include network identification information in this message.

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



Note – The combined maximum length of the strings in **set S0 message** and **set S0 prompt** must not exceed 224 characters.

Example

```
Command> set s0 message Welcome to the Network (PMI/0)
New message:
Welcome to the Network (PMI/0)
For ports: S0
```

See Also

set S0 prompt - page 5-37

set S0|all modem-type

This command selects a modem from the modem table.

set S0|all modem-type *ModemName*

ModemName Name of modem from the modem table. The modem name can contain from 0 to 16 characters.

Usage

Before you can select a modem name, you must first define the names and associated parameters in the modem table. (Refer to Table 5-4, “Modem Table Commands,” on page 5-49 for more information.)

You can set all ports for the same modem type by using the **set all modem-type** command.

Example

```
Command> set s0 modem-type usr-v34
Modem type for port S0 changed from to usr-v34
```

See Also

add modem - page 5-5

show table modem - page 5-50

set S0|all mtu

This command sets the maximum transmission unit (MTU) for a single network hardwired asynchronous port, or all network hardwired asynchronous ports.

set S0|all mtu *MTU*

MTU Valid values for MTU are between 100 and 1500 bytes.

Usage

The MTU defines the largest frame or packet that can be sent through this port, without fragmentation or discard. A packet that exceeds this value is automatically fragmented if IP, or discarded if IPX. PPP connections have a maximum of 1500 bytes, and SLIP connections have a maximum of 1006. For IPX, the MTU should be set to 1500.

You can set the MTU for all hardwired asynchronous ports simultaneously by using the **set all mtu** command.



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.

Example

Command> **set s0 mtu 1500**

MTU for port S0 changed from 0 to 1500

See Also

set S0 protocol - page 5-38

set S0 netmask

This command sets the IP netmask of the remote router for a network hardwired asynchronous port.

set S0 netmask *Ipmask*

Ipmask IP netmask in dotted decimal notation.

Usage



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.

Example

Command> **set s0 netmask 255.255.255.0**
S0 netmask changed from 0.0.0.0 to 255.255.255.0

See Also

set Ether0 netmask - page 16-7
set location netmask - page 8-21
set user netmask - page 7-19
set W1 netmask - page 6-19

set S0|all network dialin|dialout|twoway

This command sets a single asynchronous port or all asynchronous ports to provide dial-in network access to multiple remote users, dial-out access for multiple users from the network to remote locations—or both—via PPP or SLIP.

set S0|S10|all network dialin|dialout|twoway

dialin	The port accepts dial-in-only network connections. When a DCD signal is detected by the PortMaster system, PPP packets are forwarded, and PAP or CHAP authentication is initiated automatically with no prompt for a username or password. Dial-in connections to the network are controlled by the RADIUS server or the user table.
dialout	The port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial-out connections from the network are controlled by the location table.
twoway	The port accepts dial-in connections to the network, as well as being available for dial-out to remote destinations.

Usage

An asynchronous port set for any of these three network uses can also be configured to support user login and/or device sharing concurrently.

By using the **all** keyword, you can set the port type to **network dialin**, **network dialout**, or **network twoway** for all asynchronous ports simultaneously, as shown in the second example.

Examples

```
Command> set s0 network twoway  
Port type for port S0 changed from Login to Network(twoway)
```

```
Command> set all network dialin  
Port type for port S0 changed from Netwrk to Network(dialin)  
Port type for port S1 changed from Netwrk to Network(dialin)
```

Port type for port S2 changed from Login to Network(dialin)

· · · · ·
Port type for port S29 changed from Netwrk to Network(dialin) ·

See Also

set S0 device - page 5-16

set S0 login - page 5-26

set S0 twoway - page 5-46

set S0|all network hardwired

This command sets a single asynchronous port or all asynchronous ports for a permanent network connection that requires no dialing or authentication.

set S0|all network hardwired

Usage

Use this command for ports used in a dedicated or hardwired network connection between two sites. The port immediately begins running the specified protocol. None of the other port types can be combined with **network hardwired**.

You can set the port type to **network hardwired** for all the asynchronous ports simultaneously by using the **set all network hardwired** command.

You must also set the address of the other end of the network hardwired connection with the **set S0 destination** command.

Example

Command> **set s0 network hardwired**

Port type for port S0 changed from Login to Network(hardwired)

See Also

set S0 destination - page 5-15

set S0|all ofilter

This command sets a packet filter for packets exiting the PortMaster on a single network hardwired asynchronous port, or all network hardwired asynchronous ports.

set S0|S10|all ofilter *Filtername*

Filtername Output filter name that is in the filter table. Maximum of 15 characters.

Usage

When this command is specified, all packets being sent from the network hardwired port are evaluated against the rule set for this filter. Only packets permitted by this filter are sent out of the PortMaster.

You remove the filter by entering the command without a filter name.

You can set the output filter for all hardwired asynchronous ports simultaneously by using the **set all ofilter** command.



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.

Example

```
command> set s0 ofilter s0.out  
Output filter for port S0 changed from     to s0.out
```

See Also

add filter - page 13-4
set S0 ifilter - page 5-24

set S0|all override

This command sets a single asynchronous port or all asynchronous port parameters as overrideable by the host in Host Device mode.

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

xon	Software flow control.
rts	Hardware flow control.
speed	Baud rate.
parity	Parity checking.
databits	Number of data bits per byte.
on	Allows the host to override the selected parameter.
off	Does not allow the host to override the selected parameter. The default is that all overrides are off.

Usage

The PortMaster allows overrides to be set for baud rate, parity, databits, and flow control. 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).

You can set an override parameter for all the asynchronous ports simultaneously by using the **set all override** command.

Example

Command> **set s0 override speed on**

Host override of speed for port S0 changed from off to on

See Also

set S0 device - page 5-16
set S0 modem-type - page 5-29
set S0 parity - page 5-36
set S0 speed - page 5-43

set S0|all parity

This command sets the parity checking to be used for a single asynchronous port or all asynchronous ports.

set S0|all parity even|none|odd|strip

even	Set for even parity.
none	Set for no parity bit. This is the default.
odd	Set for odd parity.
strip	Set to strip the parity bit from the data stream when it is received by the PortMaster.

Usage

When **strip** is selected, the parity bit is removed upon receipt by the PortMaster. For most purposes, **none** must be selected.

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

Example

```
Command> set s0 parity none  
Parity for port S0 changed from even to none
```

See Also

set S0 databits - page 5-14
set S0 modem-type - page 5-29
set S0 speed - page 5-43
set S0 stopbits - page 5-44

set S0|all prompt

This command sets the user login prompt for a single asynchronous port or all asynchronous ports.

set S0|S10|all prompt *String*

String Login prompt— maximum is 244 printable ASCII characters, or 244 characters minus the login message, if set. The default is **\$hostname login:**.

Usage

Any printable ASCII characters can be entered. If the string **\$hostname** is included in the login prompt, the hostname for the port is substituted for the string. Use the caret symbol (^) to designate new lines. The command **set S0 prompt** returns the prompt to its default setting of **\$hostname login:**.

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



Note – The combined maximum length of the strings in **set S0 message** and **set S0 prompt** must not exceed 224 characters.

Example

```
Command> set s0 prompt $hostname login:
New Login Prompt:
$hostname login:
For ports: S0
```

See Also

set host - page 5-21
set message - page 5-28
set S0 username - page 5-47

set S0 protocol

This command sets the transport protocol for a single network hardwired asynchronous port, or all network hardwired asynchronous ports.

set S0 protocol slip|ppp|x75-sync

slip SLIP protocol.

ppp PPP protocol.



x75-sync X.75 protocol.

Usage



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.

Example

Command> **set s0 protocol slip**
Protocol for port S0 changed from ppp to slip

See Also

- set debug** - page 19-5
- set S0 compression** - page 5-13
- set S0 mtu** - page 5-30

set S0|all rts/cts

This command sets the use of hardware flow control on a single asynchronous port or all asynchronous ports.

set S0|all rts/cts on|off

on Turns on hardware flow control for the port.

off Turns off hardware flow control for the port. This is the default.

Usage

This parameter is used by devices that require hardware flow control. When the PortMaster is able to receive data from the attached device, it raises the RTS signal on pin 4 of the RS-232 connector. Output from the PortMaster occurs only if the modem line on pin 5 of the RS-232 connector has CTS raised by the attached device.

You can set the hardware flow control for all the asynchronous ports simultaneously by using the **set all rts/cts** command.

Example

Command> **set s0 rts/cts on**

RTS/CTS flow control for port S0 changed from off to on

See Also

set S0 modem-type - page 5-29

set S0 xon/xoff - page 5-48

set S0|all security

This command sets the security level for a single asynchronous port or all asynchronous ports.

set S0|S10|all security on|off

on Enables security; disables passthrough logins.

off Disables security; enables passthrough logins.
This is the default.

Usage

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

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

Example

```
Command> set s0 security on  
Security for port S0 changed from off to on
```

See Also

set authentication_server - page 3-31

set S0|all service_device

This command sets the device service to be used by a single asynchronous port or all asynchronous ports.

set S0|S10|all service_device netdata|portmaster|rlogin|telnet [*Tport*]

netdata	Allows netdata connections to this port from the network.
portmaster	Provides host device emulation from a host with the in.pmd daemon installed. This is the default.
rlogin	Allow rlogin connections to this port from the network.
telnet	Allow telnet connections to this port from the network.
<i>Tport</i>	Specifies the TCP port for the connection. Range is from 1 to 65535.

Usage

If the port type is **device** or **twoway**, you can set the device service. This command allows users to connect through the PortMaster to shared devices such as printers or modems.

You can set the device service for all asynchronous ports simultaneously by using the **set all service_device** command.

Example

```
Command> set s0 service_device portmaster
Device Service for port S0 changed from telnet to portmaster
```

See Also

set S0 device - page 5-16
set S0 host - page 5-21
set S0 login - page 5-26

set S0|all service_login

This command sets the network service to use in establishing login sessions for a selected asynchronous port, or all asynchronous ports.

set S0|S10|all service_login netdata|portmaster|rlogin|telnet [*Tport*]

netdata	Uses the netdata login service.
portmaster	Uses the PortMaster login service to connect to in.pmd on the login host. This is the default.
rlogin	Uses remote login to connect to the login host.
telnet	Uses Telnet to connect to the login host.
<i>Tport</i>	Specifies the designated TCP port on the host. Range is from 1 to 65535.

Usage

When you set the port type as **login** or **twoway**, you can specify the login service to be used for login sessions.

You can set the network service for all asynchronous ports simultaneously by using the **set all service_login** command.

Example

Command> **set s0 service_login telnet**
Login service for port S0 changed from portmaster to telnet

See Also

set S0 login - page 5-26
set S0 modem-type - page 5-29
set S0 service-device - page 5-41
set telnet - page 3-22
telnet - page 2-42

set S0|all speed

This command sets the baud rate for a single asynchronous port or all asynchronous ports.

**set S0|all speed [1|2|3] 300|600|1200|2400|4800|9600|19200|
38400|57600|76800|115200**

1|2|3 Indicates which of the three baud rates is being set: 1, 2, or 3.
Default is 1.

300|600, and so on Indicates the data terminal equipment (DTE) rate. Default is 9600bps.

Usage

Modern modems must be set to run at a fixed rate. To define a fixed rate, lock the DTE rate by setting all three baud rates to the same value.

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

Examples

Command> **set s0 speed 115200**
Speed for port S0 (1) changed from 9600 to 115200

Command> **set s0 speed 2 115200**
Speed for port S0 (2) changed from UNKNWN to 115200

Command> **set s0 speed 3 115200**
Speed for port S0 (3) changed from UNKNWN to 115200

See Also

set S0 modem-type - page 5-29

set S0|all stopbits

This command sets the number of stop bits in the data frame on a single asynchronous port or all asynchronous ports.

set S0|all stopbits 1|2

- | | |
|----------|----------------------------------|
| 1 | 1 stop bit. This is the default. |
| 2 | 2 stop bits. |

Usage

The default of 1 is the most widely used.

You can set the stop bits for all the asynchronous ports simultaneously by using the **set all stopbits** command.

Example

Command> **set s0 stopbits 1**
Stop bits for port S0 changed from 2 to 1

See Also

set S0 databits - page 5-14
set S0 modem-type - page 5-29
set S0 parity - page 5-36
set S0 speed - page 5-43

set S0|all termtype

This command sets the terminal type in the user's environment on a single asynchronous port or all asynchronous ports that are set for user login or two-way operation via the **rlogin** or PortMaster login service.

set S0|S10|all termtype *String*

String Terminal type, 0 to 15 characters.

Usage

If the port is set for either login or two-way operation, this terminal type is set in the user's environment when a new session is established to the host. Make sure that the terminal type is valid on the host that the user is connected to with the **rlogin** or PortMaster login service.

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

Example

```
Command> set s0 termtype vt100  
Terminal Type for port S0 changed from    to vt100
```

See Also

set S0 login - page 5-26
set S0 twoway - page 5-46

set S0 twoway

This command sets an asynchronous port for “two-way” operation—both user login and device sharing—or for two-way operation **and** remote dial-in and/or dial-out access.

set S0|S10 twoway Device [network dialin|dialout|twoway]

twoway	<p>The first use of the keyword twoway sets the port for both user login and device sharing—combining the commands set S0 login and set S0 device.</p> <p>The second use of the keyword twoway sets the port to two-way use for both dial-in from remote users and dial-out to remote locations.</p>
Device	Designation for the device—for example, /dev/ttyp0 or /dev/network .
dialin	In addition to allowing both user login and device sharing, the port accepts dial-in-only network connections. The remote system is required to enter a username and password. Dial-in connections to the network are controlled by the RADIUS server or the user table.
dialout	In addition to allowing both user login and device sharing, the port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial-out connections from the network are controlled by the location table.

Usage

A PortMaster asynchronous port can be configured for several different types of operation. For example, a port set for login users can also be set to access host devices. This combined inbound and outbound use is called two-way operation. You must also do the following to establish two-way operation:

- Define a login host with the **set S0 host** command.
- Define a login service with the **set S0 service_login** command.
- Define a device service with the **set S0 device_service** command.

If the port type is set to **twoway**, the port operates in user login mode when a data carrier detect (DCD) signal 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.

In addition to setting an asynchronous port for user login, you can also set it for network dial-in and/or dial-out use by multiple users. Multiple users can dial in to the network through the port from remote locations, dial out from the network through the port to remote locations—like another office or the Internet—or both.

Example

Command> **set s0 twoway /dev/ttyp0**

Port type for port S0 changed from Login to TwoWay(/dev/ttyp0)

See Also

set S0 device - page 5-16

set S0 host - page 5-21

set S0 login - page 5-26

set S0 network twoway - page 5-32

set S0 service_device - page 5-41

set S0 service_login - page 5-42

set S0 username|autolog

This command sets an automatic login name for the asynchronous port.

set S0|S10 username|autolog [*String*]

<i>String</i>	Username for automatic login—a maximum of 8 printable ASCII characters.
---------------	---

Usage

If this command is used, the user does not receive the standard login prompt. Instead, the PortMaster initiates a session to the default host as if the user had typed *String* in response to the login prompt.

To disable the automatic login, use the command **set s0 autolog** without a value *String*.

Example

Command> **set s0 autolog posales**
Username for port S0 changed from off to posales

See Also

set S0 message - page 5-28
set S0 prompt - page 5-37

set S0|all xon/xoff

This command sets the use of software flow control on a single asynchronous port or all asynchronous ports.

set S0|all xon/xoff on|off

on	Turns on software flow control for the port. This is the default.
off	Turns off software flow control for the port.

Usage

The PortMaster uses software flow control, with the ASCII control characters DC1 and DC3, to communicate with the attached device to start and stop the flow of data. Use this command only if Request To Send/Clear To Send (RTS/CTS) flow control is not available on the attached device.

You can set the software flow control for all the asynchronous ports simultaneously by using the **set all xon/xoff** command.

Example

Command> **set s0 xon/xoff off**
Xon/Xoff flow control for port S0 changed from on to off

See Also

set S0 rts/cts - page 5-39

Modem Commands

The modem table commands in Table 5-4 are used to view and configure the modem table, which stores configuration information for modems you commonly use. See also the following commands for external modems attached to asynchronous ports:

- **attach** *S0*—see page 5-6
- **set** *S0* **cd**—see page 5-11
- **set** *S0* **group**—see page 5-19
- **set** *S0* **modem-type**—see page 5-29

Table 5-4 Modem Table Commands

Command Syntax	
add modem <i>ModemName(short)</i> " <i>ModemName(long)</i> " <i>Speed</i> " <i>String</i> "	- see page 5-5
delete modem <i>ModemName(short)</i>	- see page 5-8
show modem <i>ModemName(short)</i>	- see page 5-49
show table modem	- see page 5-50



Note – When the console diagnostic switch is up, the PortMaster does not attempt to configure the modem specified for the console port. This feature allows a terminal to be attached to the console even if a modem was previously attached.

show modem

This command shows configuration information on individual modems that are in the modem table.

show modem *ModemName(short)*

ModemName(short) Short name given to the modem when the configuration information was added to the modem table.

Usage

Use the modem short name in the command, exactly as it is listed in the **show table modem** response.

Example

```
Command> show modem att-v34
      Short Name:  att-v34
      Long  Name:  AT&TV.34
Optimal Speed: 115200
      Type:  User Defined
      Init Script: Send Command
                                     Wait for
                                     Reply
                                     -----
                                     AT&FS0=1&W
                                     OK
```

See Also

- add modem** - page 5-5
- delete modem** - page 5-8
- show table modem** - page 5-50

show table modem

This command displays a table listing the modems currently configured in the modem table.

show table modem

Usage

The list provides the names of the modems, which can then be used to display details of the modem configuration.

Example

```
Command> show table modem
```

Short Name	Long Name	Type
-----	-----	-----
att-v34	AT&TV.34	User
hayes	HayesOptimaV34	User

See Also

- add modem** - page 5-5
- delete modem** - page 5-8
- show modem** - page 5-49

This chapter describes how to use the command line interface to configure synchronous ports. Detailed command definitions follow a command summary table.

The command line interface can configure a PortMaster synchronous serial port for use with a leased line, Frame Relay, ISDN or switched 56Kbps connection.

Examples in this chapter are from a PortMaster 2R, where the synchronous port is labeled W1. In contrast, the synchronous ports on PortMaster IRX Routers are labeled S1 through S4.



Note – After making any configuration changes to a synchronous port, you must use the **reset W1** command for the changes to take effect.

Displaying Synchronous Port Information

To display information about your configuration, use the following commands:

- **show W1**
- **show all**—see page 2-22
- **ifconfig**—see page 2-9
- **show sessions**—see page 2-39
- **show netstat**—see page 2-34
- **show arp**—see page 2-24

For general information about command line interface commands, refer to Chapter 1, “Introduction.”

Summary of Synchronous Port Commands

The synchronous port commands in Table 6-1 configure synchronous serial ports. Commands marked with a leading bullet (•) can be used only for network hardwired ports.

Table 6-1 Synchronous Port Configuration

Command Syntax	
• add dlci ipdlci ipxdlci <i>W1</i> <i>Dlci</i> [: <i>Ipaddress</i> : <i>Ipxnode</i>]	- see page 6-10
• delete dlci ipdlci ipxdlci <i>W1</i> <i>Dlci</i>	- see page 6-4
reset <i>W1</i>	- see page 2-15
save ports	- see page 2-18
save <i>W1</i>	- see page 2-18
• set <i>W1</i> address <i>Ipaddress</i>	- see page 6-5
• set <i>W1</i> annex-d <i>Seconds</i>	- see page 6-6
set <i>W1</i> cd on off	- see page 6-7
set <i>W1</i> compression on off stack vj	- see page 6-8
• set <i>W1</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]	- see page 6-9
• set <i>W1</i> dlcilist <i>Dlci_list</i>	- see page 6-10
set <i>W1</i> extended on off	- see page 6-12
set <i>W1</i> group <i>Group</i>	- see page 6-12
set <i>W1</i> hangup on off	- see page 6-13
set <i>W1</i> idletime <i>Number</i> [<i>minutes</i> <i>seconds</i>]	- see page 6-14
• set <i>W1</i> ifilter [<i>Filtername</i>]	- see page 6-15
• set <i>W1</i> ipxnet <i>Ipxnetwork</i>	- see page 6-16
• set <i>W1</i> lmi [<i>Seconds</i>]	- see page 6-17
• set <i>W1</i> mtu <i>MTU</i>	- see page 6-18
set <i>W1</i> nat inmap outmap defaultnapt <i>Mapname</i> blank outsource	- see page 14-14
set <i>W1</i> nat log sessionfail sessionsuccess syslog console on off	- see page 14-16

Table 6-1 Synchronous Port Configuration (Continued)

Command Syntax	
<code>set W1 nat sessiontimeout tcp other Number[minutes seconds]</code>	- see page 14-17
<code>set W1 nat session-direction-fail-action drop icmproject passthrough</code>	- see page 14-19
<ul style="list-style-type: none"><code>set W1 netmask Ipmask</code>	- see page 6-19
<code>set W1 network dialin dialout twoway hardwired</code>	- see page 6-20
<ul style="list-style-type: none"><code>set W1 ofilter [Filtername]</code>	- see page 6-21
<ul style="list-style-type: none"><code>set W1 ospf on off [cost Number] [hello-interval Seconds][dead-time Seconds] [nbma point-to-multipoint wan-as-stub-ptmp]</code>	- see page 17-9
<ul style="list-style-type: none"><code>set W1 protocol slip ppp frame x75-sync</code>	- see page 6-22
<ul style="list-style-type: none"><code>set W1 rip on off broadcast listen</code>	- see page 16-19
<code>set W1 route-filter incoming outgoing Filtername</code>	- see page 16-8
<code>set W1 speed 9600 14400 19200 38400 56000 57600 64000 76800 115200 1344k 1536k 2048k t1 t1e e1</code>	- see page 6-23
<code>show all</code>	- see page 2-22
<code>show W1</code>	- see page 6-24

Synchronous Commands

These commands affect the synchronous interface of the PortMaster. Examples in this chapter are from a PortMaster 2R or 2ER, labeled *W1*. In contrast, the PortMaster IRX-114 uses *S1* through *S4* for synchronous ports. See Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1 for the range of synchronous ports available on each PortMaster model.



Note – Always set the port type to **network** for synchronous ports.

delete dlci

This command deletes data link connection identifiers (DLCIs) for Frame Relay service on a network hardwired synchronous port.

delete dlci | **ipdlci** | **ipxdlci** *W1* *Dlci*

ipdlci or **dlci** Use for IP connections.

ipxdlci Use for IPX connections.

Dlci DLCI number, from 1 to 1023. You can delete only one DLCI number at a time.

Usage



Note – These commands are used only for network hardwired synchronous ports. The list of DLCIs used on a port always includes those created with the **set W1 dlclist** command and those created with the **add dlci W1** command.

Example

```
Command> delete dlci w1 16
DLCI successfully deleted
```

See Also

add dlci - page 6-10
set W1 annex-d - page 6-6
set W1 dlclist - page 6-10
set W1 lmi - page 6-17

set W1 address

This command sets the local IP address of the network hardwired synchronous port to create a numbered interface.

set W1 address *Ipaddress*

Ipaddress IP address in dotted decimal notation or hostname of between 1 and 39 characters.

Usage

If the local IP address of the port is set to 0.0.0.0 for PPP, the PortMaster uses the Ether0 IP address for this end of the serial link. If the address is set to 0.0.0.0 for Frame Relay, the port is disabled.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 address 192.168.7.2**

Port W1 local address changed from 0.0.0.0 to 192.168.7.2

See Also

set S0 address - page 5-10

set W1 annex-d

This command sets the Annex-D polling interval for a network hardwired synchronous port to allow the Frame Relay switch to monitor link status.

set W1 annex-d *Seconds*

Seconds Keepalive interval in seconds, from 0 to 240. The default value is 10.

Usage

The Annex-D default value is 10 seconds. However, if your telephone company chooses another value, change this value as they instruct you. Enabling Annex-D (or LMI) causes the DLCI list to be completed automatically. Setting the interval to 0 (zero) seconds, or enabling LMI, disables Annex-D. You can display Annex-D activity using the **set debug 0x51** command.



Note – Check with your Frame Relay service provider to determine whether they use LMI or Annex-D; both can be referred to as LMI.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 annex-d 10**
ANNEX-D keepalive timer for S1 changed from 0 to 10

See Also

set debug - page 19-5
set W1 dlci list - page 6-10
set W1 lmi - page 6-17

set W1 cd

This command enables the PortMaster to monitor the presence of the data carrier detect (DCD) signal on a modem attached to the synchronous port to determine whether the line is in use.

set W1 cd on|off

on Monitors presence of the DCD signal.

off Does not monitor presence of the DCD. This is the default.

Usage

Modem control defaults to **off** for synchronous connections. In this default state, the PortMaster assumes the DCD signal is always high.

Set this command to **on** only if you want to make use of the DCD signal from the attached device. When set to **on**, the PortMaster uses the signal to determine if the line is in use.

For leased lines or Frame Relay, this control is usually set to **off**, but can be turned on if the CSU/DSU is configured accordingly.

Example

```
Command> set w1 cd on  
CD required for port W1 changed from off to on
```

See Also

set S0 cd - page 5-11

set w1 compression

This command sets Van Jacobson TCP/IP header compression and/or Stac LZS data compression on a synchronous port.

set w1 compression on|off|stac|vj

- | | |
|-------------|---|
| on | Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and 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 Office Router products. |
| vj | Enables Van Jacobson TCP/IP header compression only. |

Usage

Van Jacobson TCP/IP header compression can be used for SLIP and PPP connections. With SLIP, both sides need to be configured identically. For PPP connections, the PortMaster supports both bidirectional and unidirectional 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.

Example

Command> **set w1 compression on**
Compression for port w1 changed from off to on

See Also

set location compression - page 8-9
set s0 compression - page 5-13
set user compression - page 7-8

set W1 destination

This command sets the IP address and the netmask of the remote router for a network hardwired synchronous port connection.

set W1 destination *Ipaddress* [*Ipmask*]

Ipaddress IP address in dotted decimal notation or hostname of
 between 1 and 39 characters.

Ipmask IP mask in dotted decimal notation.

Usage

If the remote destination is set to 255.255.255.255 for PPP connections, the PortMaster attempts to learn the remote IP address. If set to 0.0.0.0, the port is disabled.



Note – Use this command only for network hardwired synchronous ports.

Example

Command> **set w1 destination 255.255.255.255**
Port W1 destination changed from 0.0.0.0 to 255.255.255.255

See Also

set S0 destination - page 5-15
set S10 destination - page 11-10

set W1 dlcilist

Use these commands to add or set data link connection identifiers (DLCIs) for Frame Relay service on a network hardwired synchronous port.

```
set W1 dlcilist Dlcilist
```

```
add dlcilist|ipdlci|ipxdlci W1 Dlcilist [:Ipaddress]:Ipxnode]
```



Note – **set W1 dlcilist** and **add dlcilist** perform the same function except that the command **add dlcilist** does not have a 244-character limitation. **ipdlci** is a synonym for **dlci**.

<i>Dlcilist</i>	Space-separated list of DLCI numbers from 1 to 1023, up to a maximum of 244 characters. Each DLCI can also include an IP address or IPX node address preceded by a colon (:).
ipdlci or dlci	Use for IP connections.
ipxdlci	Use for IPX connections.
<i>Dlcilist</i>	DLCI number, from 1 to 1023. You can add only one DLCI number at a time.
<i>:Ipaddress</i>	Optional IP address of the router attached to the permanent virtual circuit (PVC) represented by the DLCI.
<i>:Ipxnode</i>	IPX node address of the PortMaster attached to the permanent virtual circuit (PVC) represented by the DLCI. This value is the PortMaster MAC address—a 48-bit number.

Usage

With LMI or Annex-D, DLCIs can be learned dynamically. However, if LMI or Annex-D is not used, you must enter the DLCI list manually. Your Frame Relay service provider might provide a DLCI list.

When using Frame Relay, you can enter a list of DLCIs accessible through this interface via the Frame Relay network. The PortMaster attempts to use Inverse ARP requests to learn the IP addresses of routers attached to the permanent virtual circuits (PVCs)

represented by these DLCIs. Alternatively, you can specify IP addresses by appending a colon (:) and IP address after the DLCI. If an address is specified, the PortMaster statically configures that entry into its ARP table for this interface.



Note – These commands are used only for network hardwired synchronous ports. The list of DLCIs used on a port always includes those created with the **set W1 dlcilist** command and those created with the **add dlci W1** command.

Examples

```
Command> set w1 dlcilist 16 17 18  
New DLCI List: 16 17 18
```

```
Command> set w1 dlcilist 16:192.168.2.1 17:192.168.2.3  
New DLCI List: 16:192.168.2.1 17:192.168.2.3
```

```
Command> add dlci w1 16:192.168.2.3  
New dlci successfully added
```

See Also

delete dlci - page 6-4
set W1 annex-d - page 6-6
set W1 lmi - page 6-17

set W1 extended

This command sets the extended mode on or off for the synchronous port.

set W1 extended on|off

on Turns extended mode on.

off Turns extended mode off. This is the default.

Usage

When extended mode is on, the **show** command provides more detailed output.

Example

```
Command> set w1 extended on  
Extended mode for port W1 changed from off to on
```

set W1 group

This command assigns synchronous ports to pools for use by V.25bis dial-out locations.

set W1 group Group

Group Group number, from 0 to 100. Default is 0.

Usage

For pools to work, each port must be assigned to a dial group, and each location must specify a dial group. A group number is assigned to each location in the location table. See page 8-11 for more information.

Example

Command> **set w1 group 1**
Group number for port W1 changed from 0 to 1

See Also

set location group - page 8-11
set S0 group - page 5-19

set W1 hangup

This command controls whether the DTR signal on the synchronous port is dropped for 500ms to cause a hangup after the termination of a user session.

set W1 hangup on|off

- on** DTR is dropped after the session terminates. This is the default.
- off** DTR is not dropped after the session terminates.

Usage

Resetting the port administratively with the **reset** command always drops the DTR signal.

Example

Command> **set w1 hangup on**
DTR Hangup for port W1 changed from off to on

See Also

reset W1 - page 2-15

set W1 idletime

This command sets how long the PortMaster waits after activity stops on the synchronous port before disconnecting.

set W1 idletime *Number* [**minutes**|**seconds**]

Number Idle time value in minutes or seconds, as specified. Any value from 0 to 240. The default value is 0.

minutes Sets the idle time in minutes. This is the default.

seconds Sets the idle time in seconds.

Usage

If the idle timeout value is set to 0, the idle timer is disabled.

If the value is set to 2 seconds or a longer interval, the port is reset after having no traffic for the designated time. RIP, keepalive, and Service Advertising Protocol (SAP) packets are not counted as traffic.

Example

Command> **set w1 idletime 120**

Idle timeout for W1 changed from 0 minutes to 120 minutes

See Also

set W1 cd - page 6-7

set W1 ifilter

This command sets an input packet filter for packets entering the PortMaster on a network hardwired synchronous port from a leased line or Frame Relay.

set W1 ifilter [*Filtername*]

Filtername Input filter name that is in the filter table. Maximum of 15 characters.

Usage

When an input filter is specified on a network hardwired synchronous port, all packets received from the interface are evaluated against the rule set for this filter. Only packets that are permitted by this filter are allowed to enter the PortMaster. If the filter is changed, the port must be reset for the change to take effect.

This setting is not used for dial-in and dial-out networking; filters for dial-in users are set in the user table or RADIUS, and filters for dial-out locations are set in the location table.

You remove the filter by entering the command without a filter name.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 ifilter internet.in**

Input filter for port W1 changed from to internet.in

See Also

add filter - page 13-4

set W1 ofilter - page 6-21

show table filter - page 13-25

set W1 ipxnet

This command sets the IPX network number for the point-to-point connection on a network hardwired synchronous port.

set W1 ipxnet *Ipxnetwork*

Ipxnetwork IPX network number. A 32-bit hexadecimal value.

Usage

IPX traffic can be passed through a port if you assign an IPX network number to the hardwired network connection. The serial link itself must have an IPX network number that is different from those at each end of the Ethernet.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 ipxnet 0XC009C801**
Port W1 ipxnet changed from 00000000 to 0XC009C801

See Also

set Ether0 ipxnet - page 4-9

set ipx on - page 3-9

set S0 ipxnet - page 5-25

set W1 lmi

This command sets the Local Management Interface (LMI) polling interval for a network hardwired synchronous port to allow the Frame Relay switch to monitor link status.

set W1 lmi [*Seconds*]

Seconds Keepalive interval in seconds, from 0 to 240. Default value is 10.

Usage

The LMI default value is 10 seconds. However, if your telephone company chooses another keepalive value, change this value as they instruct you. Annex-D keepalives are also available. Enabling LMI (or Annex-D) causes the data link connection identifier (DLCI) list to be completed automatically. Setting the interval to zero seconds, or re-entering the command **set W1 lmi**, disables LMI. You can display LMI activity using the **set debug 0x51** command.



Note – Check with your Frame Relay service provider to determine whether they use LMI or Annex-D; both can be referred to as LMI.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 lmi 10**
LMI keepalive timer for W1 changed from 0 to 10

See Also

set debug - page 19-5
set W1 annex-d - page 6-6
set W1 dlci list - page 6-10

set W1 mtu

This command sets the maximum transmission unit (MTU) for the network hardwired synchronous port.

set W1 mtu MTU

MTU Valid values for MTU are between 100 and 1500 bytes.

Usage

The MTU defines the largest frame or packet that can be sent through this port. A packet that exceeds this value is automatically fragmented if IP, or discarded if IPX.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 mtu 1500**
MTU for port W1 changed from 0 to 1500

See Also

set W1 protocol - page 6-22

set W1 netmask

This command sets the IP netmask of the remote router for a network hardwired synchronous port.

set W1 netmask *Ipmask*

Ipmask IP netmask in dotted decimal notation.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 netmask 255.255.255.0**
W1 netmask changed from 0.0.0.0 to 255.255.255.0

See Also

set Ether0 netmask - page 16-7

set S0 netmask - page 5-31

set W1 network

This command sets the network type for the synchronous port.

set W1 network dialin|dialout|twoway|hardwired

dialin	<p>The port accepts dial-in network connections. The remote system is required to authenticate using PAP or CHAP. Dial-in network connections are controlled by the user table or the RADIUS server.</p> <p>A remote host can connect to the port. This setting is used for ISDN or switched 56Kbps connections.</p>
dialout	<p>The port is available for dialing to remote destinations and initiating network connections to those destinations. Dial-out network connections are controlled by the location table.</p> <p>The port is available for dial-out use by the location table using V.25bis dialing. This setting is used for ISDN or switched 56Kbps connections.</p>
twoway	<p>The port accepts dial-in network connections, as well as being available for dial-out to remote destinations.</p>
hardwired	<p>This setting is for ports being used in a dedicated network connection between two sites. No modem dialing or authentication is required. The port immediately begins running the specified protocol. The port is connected to a synchronous leased line or Frame Relay using a V.35 or suitable RS-232 cable. Refer to the appropriate hardware configuration guide for more information. You must also set the remote destination address with set W1 destination.</p>

Usage

Network service parameters are set on the port when hardwired, in the user table or by RADIUS for dial-in users, and in the location table for dial-out locations.

Example

Command> **set w1 network hardwired**

Port type for port W1 changed from Netwrk to Network(hardwired)

See Also

set S0 network - page 5-32

set W1 ofilter

This command sets a packet filter for packets exiting the PortMaster on a network hardwired synchronous port.

set W1 ofilter [*Filtername*]

Filtername Output filter name that is in the filter table. Maximum of 15 characters.

Usage

When an output filter is specified, all packets being sent to the network hardwired port are evaluated against the rule set for this filter. Only packets permitted by this filter are allowed to leave the PortMaster. If the filter is changed, the port must be reset for the changes to take effect.

You remove the filter by entering the command without a filter name.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 ofilter w1.out**

Output filter for port W1 changed from to w1.out

See Also

add filter - page 13-4

set w1 ifilter - page 6-15

show table filter - page 13-25

set w1 protocol

This command sets the transport protocol for a network hardwired synchronous port.

set w1 protocol slip|ppp|frame|x75-sync

slip	SLIP protocol.
ppp	PPP. Used for leased lines, ISDN, and switched 56Kbps connections.
frame	Frame Relay.
x75-sync	X.75 Protocol.

Usage

Select PPP for direct leased line connections between routers, for ISDN, or for switched 56Kbps. Select Frame Relay when attaching the port to a Frame Relay network via a Frame Relay switch.



Note – This command is used only for network hardwired synchronous ports.

Example

Command> **set w1 protocol ppp**

Protocol for port W1 changed from frame relay to ppp

See Also

set debug - page 19-5
set w1 annex-d - page 6-6
set w1 lmi - page 6-17

set w1 speed

This command sets the reference speed for the synchronous port.

**set w1 speed 9600|14400|19200|38400|56000|57600|64000|76800|115200|
1344k|1536k|2048k|t1|t1e|e1**

9600|14400, and Indicates DTE rate in bits per second.
so on

t1, t1e, e1 Reference for T1, extended superframe T1, or E1 line types.

Usage

The true line speed is set by the external clock signal on the device to which the PortMaster is connected, or by the telephone company network. Speed or line type settings on synchronous ports are for administrative notation only and do not affect the operation of the port.

Example

Command> **set w1 speed 64000**
Speed for port W1 changed from 9600 to 64000

See Also

set S0 speed - page 5-43

show W1

Shows the current status and configuration for synchronous ports on the PortMaster.

show W1

Example

```
Command> show w1
----- Current Status - Port W1 -----
      Status:  ESTABLISHED
      Input:   507781                Abort Errors:  56/1
      Output:  882686                CRC Errors:   27
      Pending: 0                    Overrun Errors: 0
      TX Errors: 0                  Frame Errors:  0
      Modem Status: DCD+ CTS+

              Active Configuration  Default Configuration
              -----
      Port Type:  Netwrk              Netwrk (Hardwired)
      Line Speed: Ext 1536K            Ext Clock
      Modem Control: off              off
      Remote Host: 172.16.0.37        255.255.255.255
      Netmask:    255.255.255.0       255.255.255.0
      Interface:  ptpW1 (PPP, Routing) (PPP, Routing)
      Mtu:        1500                0
      Dial Group: 0
```


Explanation

Status	State of the port. Refer to the information on port status in Table 2-2, on page 2-23.
Input/Output/ Pending	Number of bytes input, output, or pending since last reboot.
TX Errors	Number of transmission errors since last reboot.
Abort Errors	<p>Number of abnormal termination errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—framing errors/device errors:</p> <p>Framing errors—This count increments when the receiver chip reports either a framing error or an abnormal termination.</p> <p>Device errors—This count increments when the frame size is 0 (zero) or greater than the maximum size of a PPP frame, or when frames overlap each other.</p>
CRC Errors	Number of cyclic redundancy check (CRC) errors occurring since last reboot.
Overrun Errors	Number of overrun errors occurring since last reboot.
Frame Errors	<p>Number of frame errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—short frame errors/large frame errors:</p> <p>Short frame errors—This count increments when a short frame is received.</p> <p>Large frame errors—This count increments when a packet is too large and must be dropped.</p>
Modem Status	<p>The plus signs (+) on DCD and CTS indicate that the DCD and CTS signals on the port are asserted (high).</p> <p>For modem status information for ISDN lines, refer to the ISDN connection chapter in the <i>PortMaster Configuration Guide</i>.</p>
Active Configuration	The configuration currently active on the port.

Default Configuration	The configured port parameters, including available alternatives.
Port Type	The port type—login, device, or network. (Security) indicates that security has been set for the port. See page 5-40.
Line Speed	Ext. indicates external line speed in kilobits per second.
Modem Control	Modem carrier detect signal setting.
Remote Host	IP address of remote host. If the destination address is set to 255.255.255.255 for PPP connections, the PortMaster attempts to learn the remote IP address.
Netmask	The netmask of the local network.
Interface	The interface specification used by the port.
Mtu	The maximum transmission unit (MTU) set for the port.
Dial Group	The dial group number allocated to the port.

See Also

show p0 - page 2-35

show S0 - page 2-35

show S10 - page 2-35

This chapter describes how to use the command line interface to configure the user table. Detailed command definitions follow a command summary table.



Note – Whenever possible, especially if you have 100 or more users, use RADIUS for user authentication rather than the user table. To use RADIUS, see Chapter 3, “Global Commands,” and the *RADIUS for UNIX Administrator’s Guide*.

The user table enables the PortMaster to authenticate and provide operational parameters on a user-by-user basis.

You can use the command line interface to create, edit, and delete four kinds of users:

- **Normal login user** begins an active shell session to a host on the network.
- **Dialback login user** is disconnected by the PortMaster, which then dials back to the user at a predefined telephone number.
- **Normal network user** establishes an active PPP or SLIP connection to the network.
- **Dialback network user** is disconnected by the PortMaster, which then dials back to the user at a predefined location. For more information about locations, refer to Chapter 8, “Locations and DLCIs.”



Note – After making changes to a user, you must reset the port that the user is using.

Displaying User Information

To display information about your configuration, use the following user table commands:

- **show table user**
- **show user** *Username*

For general information about command line interface commands, refer to Chapter 1, “Introduction.”

Summary of User Commands

The user commands in Table 7-1 configure the user table used to authenticate dial-in users. The **User Type** column in the table denotes commands for login users (L) and network users or **netusers** (N). RADIUS can also be used to authenticate dial-in users; the user table is always consulted first.

Table 7-1 User Table Configuration

User Type	Command Syntax	
N	add netuser <i>Username</i> [password <i>Password</i>]	- see page 7-4
L	add user <i>Username</i> [password <i>Password</i>]	- see page 7-5
L/N	delete user <i>Username</i>	- see page 7-6
L/N	save user	- see page 7-6
N	set user <i>Username</i> address destination assigned negotiated <i>Ipaddress</i>	- see page 7-7
N	set user <i>Username</i> compression on off	- see page 7-8
L/N	set user <i>Username</i> dialback callback <i>Locname String none</i>	- see page 7-9
L	set user <i>Username</i> host default prompt <i>Ipaddress</i>	- see page 7-10
L/N	set user <i>Username</i> idle <i>Number</i> [minutes seconds]	- see page 7-11
L/N	set user <i>Username</i> ifilter [<i>Filtername</i>]	- see page 7-12
N	set user <i>Username</i> ipxnet <i>Ipxnetwork</i>	- see page 7-14
N	set user <i>Username</i> local-ip-address <i>Ipaddress</i>	- see page 7-15
N	set user <i>Username</i> map <i>Hex</i>	- see page 7-16
L/N	set user <i>Username</i> maxports <i>Number</i>	- see page 7-17
N	set user <i>Username</i> mtu <i>MTU</i>	- see page 7-18

Table 7-1 User Table Configuration (Continued)

User Type	Command Syntax	
N	set user <i>Username</i> nat inmap outmap defaultnapt Mapname blank [outsources]	- see page 14-14
N	set user <i>Username</i> nat log sessionfail sessionsuccess syslog console on off	- see page 14-16
N	set user <i>Username</i> nat sessiontimeout tcp other <i>Number</i> [minutes seconds]	- see page 14-17
N	set user <i>Username</i> nat session-direction-fail-action drop icmproject passthrough	- see page 14-19
N	set user <i>Username</i> netmask <i>Ipmask</i>	- see page 7-19
N	set user <i>Username</i> ofilter [<i>Filtername</i>]	- see page 7-20
L/N	set user <i>Username</i> ospf on off [cost <i>Number</i>] [hello-interval <i>Seconds</i>] [dead-time <i>Seconds</i>] [nbma point-to-multipoint wan-as-stub-ptmp]	- see page 17-9
L/N	set user <i>Username</i> password <i>Password</i>	- see page 7-21
N	set user <i>Username</i> protocol slip ppp x75-sync	- see page 7-21
N	set user <i>Username</i> rip on off broadcast listen	- see page 16-21
L/N	set user <i>Username</i> route-filter incoming outgoing <i>Filtername</i>	- see page 16-8
L	set user <i>Username</i> service netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 7-22
L/N	set user <i>Username</i> session-limit <i>Minutes</i>	- see page 7-23
L/N	show table user	- see page 7-24
L/N	show user <i>Username</i>	- see page 7-25

User Commands

These commands configure the user table of the PortMaster.



Note – All **set** commands can use **user** and **netuser** interchangeably, except that you cannot use **set netuser** for a login user. The **add** command requires **add netuser** for network users and **add user** for login users.

add netuser

This command adds an entry to the user table for a network user.

add netuser *Username* [**password** *Password*]

Username Network username of 1 through 8 characters.

Password Network user password of 0 through 16 characters.

Usage

A network user must be added to the user table before other netuser parameters can be configured. You cannot add network users with blank network usernames.

Example

```
Command> add netuser jaime password 1mno+vwab  
New User successfully added
```

See Also

delete user - page 7-6

add user

This command adds an entry to the user table for a login user. Optionally, the user password can be added at the same time.

add user *Username* [**password** *Password*]

Username A login username of 1 through 8 characters. Usernames cannot begin with a quotation (") mark or a question mark (?).

Password A login user password of 0 through 16 characters.

Usage

A user must be added to the user table before other user parameters can be configured.

Example

```
Command> add user sam password yzgixcel  
New User successfully added
```

delete user

This command deletes a user or network user, password, and associated information from the user table.

delete user *Username*

Username Username of a login user or network user.

Example

```
Command> delete user sam  
Password successfully deleted
```

See Also

show table user - page 7-24

save user

This command writes any changes in the user table to the nonvolatile RAM of the PortMaster.

save user

Usage

The **save all** command can also be used.

Example

```
Command> save user  
User table successfully saved  
New configurations successfully saved.
```


set user address|destination

This command sets the IP address of the network user.

```
set user Username address|destination assigned|negotiated Ipaddress
```

<i>Username</i>	Name of a network user.
address destination	Keywords address and destination are synonyms and generate the same result.
assigned	The PortMaster assigns a temporary IP address for this user from the assigned pool.
negotiated	This option is valid only for PPP sessions. The PortMaster attempts to learn the IP address of the remote host by IP Control Protocol (IPCP) negotiation.
<i>Ipaddress</i>	Uses the specified IP address, or hostname with a maximum of 39 characters. If <i>Ipaddress</i> is 0.0.0.0, the PortMaster does not use IP for this user.

Usage

Address 255.255.255.255 is the same as **negotiated**. Address 255.255.255.254 is the same as **assigned**.

Example

```
Command> set user jaime destination assigned  
Username: jaime                Type: Dial-in Network User  
Address: Assigned              Netmask: 0.0.0.0  
Protocol: PPP                  Options: Quiet, Listen  
MTU: 1500
```

See Also

set assigned_address - page 3-3

set user compression

This command sets Van Jacobson TCP/IP header compression and Stac LZS data compression for a network user.

set user *Username* **compression on|off**

Username Name of a network user.

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

off Disables compression.

Usage

Van Jacobson TCP/IP header compression can be used for SLIP and PPP connections. With SLIP, both sides need to be configured identically. For PPP connections, the PortMaster supports both bidirectional and unidirectional compression.

Example

Command> **set user joe compression on**

Username:	joe	Type:	Dial-in Network User
Address:	Negotiated	Netmask:	0.0.0.0
Protocol:	SLIP	Options:	Quiet, Compression
MTU:	1006		

set user dialback

This command sets the callback telephone number for a callback login user, or the location for a callback network user.

set user *Username* **dialback|callback** *Locname|String|none*

<i>Username</i>	Username of a login user or network user.
dialback callback	Keywords dialback and callback are synonyms and generate the same result.
<i>Locname</i>	Network user location name that is in the location table. <i>Locname</i> must be between 1 and 12 characters in length.
<i>String</i>	Login user callback telephone number—a maximum of 32 characters.
none	Disables callback for this user, who then becomes a normal login or network user.

Usage

To set callback for a **login** user, enter the string of characters that follows the Hayes-compatible **ATDT** command to return the user’s call. If you enter a telephone number, the user is changed to a callback login user.

To set a callback for a **network** user, enter the name of the location—already in the location table—to which the PortMaster establishes a network connection back to the user.

Examples

Command> **set user sam dialback 5551212**

Username:	sam	Type:	Login User
Host:	default	Login Service:	portmaster
Dialback No:	5551212		

Command> **set user mario dialback office**

Username:	mario	Type:	Dialback Network User
Location:	office		

See Also

set S0 dialback_delay - page 5-17

set user host

This command indicates the login host for the login user.

set user *Username* **host default|prompt|Ipaddress**

<i>Username</i>	Username of a login user.
default	Connects the user to the default host for the serial port.
prompt	Allows the user to select a host (by IP address or name) to begin a login session.
<i>Ipaddress</i>	Connects the user to the specified IP address or hostname of between 1 and 39 characters.

Usage

The login host parameter defines the host to which the user is connected. If you set the user login host in the user table, prompts are displayed in the following order:

login:
prompt:
host:

Setting the IP address to 0.0.0.0 sets the host to the default.

Example

```
Command> set user jack host 192.168.1.2
Username:  jack                               Type:  Login User
Host:  192.168.1.2       Login Service:  portmaster
```

See Also

set S0 host - page 5-21

set user idle

This command sets the length of time the line can be idle—in both directions—before the PortMaster disconnects the user.

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

<i>Username</i>	Name of a user.
idle <i>Number</i>	Timeout value from 0 to 240. The default value is 0.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.

Usage

If the idle time value is set to 0, the idle timer is disabled. If the value is set to 2 seconds or a longer interval, the user is disconnected after there is no traffic for the designated time.

You can set user idle timeout in the user table using this command, or you can use the RADIUS Idle-Timeout attribute. The RADIUS attribute is specified in seconds, but when greater than 240 seconds it is rounded up to minutes by the PortMaster.

Examples

```
Command> set user joe idle 30
      Username:  joe                      Type:  Dial-in Network User
      Address:   Negotiated                Netmask: 0.0.0.0
      Protocol:  PPP                      Options: Quiet, Compression
      MTU:       1500                     Async Map: 00000000
      Port Limit: 2                      Idle Timeout: 30
```

See Also

set user session-limit - page 7-23

set user ifilter

This command sets the input packet filter for packets entering the PortMaster on the interface established by the network user.

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

Username Name of a user.

Filtername Input filter name. The maximum is 15 characters.

Usage

When an input packet filter is specified, all packets received from the serial interface are evaluated against the rule set for this filter, which has been defined and is in the filter table. Only packets that are permitted by this filter are allowed to enter the PortMaster.

An access control filter, using a valid filter name from the filter table, can be set for login users to restrict which hosts they can log into, as follows:

1. The user logs in and 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; otherwise, the connection is denied.

You remove the filter by entering the command without a filter name.

Example

```
Command> set user joe ifilter student.in
      Username:  joe                      Type:  Dial-in Network User
      Address:   Negotiated                Netmask: 0.0.0.0
      Protocol:  SLIP                      Options: Quiet, Compression
      MTU:       1006
      Packet Filters:  student.in/
```

See Also

add filter - page 13-4
set user host prompt - page 7-10
set user ofilter - page 7-20

set user ipxnet

This command sets the IPX network number for the user's network connection.

set user *Username* **ipxnet** *Ipxnetwork*

Username Name of a network user.

Ipxnetwork Number of IPX network to be used for a serial link—a 32-bit hexadecimal value.

Usage



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

The PPP protocol must be used with IPX. If you set the IPX network number to 0XFFFFFFFE, the PortMaster dynamically assigns an IPX network for the user by using an address from the assigned pool as an IPX network number.

Example

Command> **set user hideo ipxnet ox0f012345**

IPX network set to F012345

Username:	hideo	Type:	Dial-in Network User
Address:	Assigned	Netmask:	255.255.255.0
IPX Network:	0F012345		
Protocol:	PPP	Options:	Quiet, Listen
MTU:	1500		

See Also

set assigned_address - page 3-3

set ipx on - page 3-9

set user local-ip-address

This command allows a network user to set a local IP address on a PortMaster dialout port (asynchronous or ISDN) for numbered IP networks. It is used only when a unique IP subnet is required for a point-to-point network connection.

set user *Username* **local-ip-address** *Ipaddress*

Username Name of a network user.

Ipaddress IP address. A hostname is not accepted.

Usage

This function is not available in RADIUS. This command is used to create a dial-out point-to-point network connection when both ends require an IP address.



Note – The point-to-point connection is a network of two nodes and requires its own IP subnet.

Example

```
Command> set user rani local-ip-address 192.168.96.6
Username:  rani                               Type:  Dial-in Network User
Address:   Negotiated                         Netmask: 0.0.0.0
Lcl Address: 192.168.96.6
Protocol:   PPP                               Options: Quiet, Compression
MTU:       1500                               Async Map: 00000000
```

See Also

set user destination - page 7-7

set reported_ip - page 3-19

set user map

This command sets the PPP asynchronous map to replace nonprinting ASCII characters found in the data stream.

set user *Username* **map** *Hex*

Username Name of a network user.

Hex A 32-bit hexadecimal number. The default is 0x00000000.

Usage

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 must be replaced. The lowest-order bit corresponds to the first ASCII character NUL and so on. Most environments must use the default. This command does not apply to the Serial Line Internet Protocol (SLIP).

The command **set user** *Username* **map 0** disables the asynchronous mapping.

Example

Command> **set user joe map 0x00009000**

Username:	joe	Type:	Dial-in Network User
Address:	Negotiated	Netmask:	0.0.0.0
Protocol:	PPP	Options:	Quiet, Compression
MTU:	1500	Async Map:	0x00009000
Packet Filters:	student.in/student.out		

set user maxports

This command, if set, limits the number of network dial-in ports the user can use on the PortMaster for Multilink V.120, Multilink PPP, and asynchronous multiline load-balancing.

set user *Username* **maxports** *Number*

Username Name of a user.

Number Number between 0 and 64.

Usage

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 set the dial-in port limit using the RADIUS Port-Limit attribute.

Example

Command> **set user joe maxports 2**

Username:	joe	Type:	Dial-in Network User
Address:	Negotiated	Netmask:	0.0.0.0
Protocol:	PPP	Options:	Quiet, Compression
MTU:	1500	Async Map:	00000000
Port Limit:	2	Idle Timeout:	0

See Also

set location maxports - page 8-18

set user mtu

This command sets the maximum transmission unit (MTU) for the network user.

set user *Username* **mtu** *MTU*

Username Name of a network user.

MTU MTU value from 100 to 1500 bytes.

Usage

The MTU defines the largest frame or packet that can be sent, without fragmentation. A packet that exceeds this value is automatically fragmented if IP, or discarded if IPX. PPP connections have a maximum MTU of 1500 bytes, and SLIP connections have a maximum of 1006 bytes.

Example

```
Command> set user joe mtu 1500
      Username:  joe                               Type:  Dial-in Network User
      Address:   Negotiated                         Netmask: 0.0.0.0
      Protocol:  PPP                               Options: Quiet, Compression
      MTU:       1500                               Async Map: 00000000
      Packet Filters: student.in/student.out
```

See Also

set user protocol - page 7-21

set user netmask

This command defines the netmask of the user's system on the remote end of the connection.

set user *Username* **netmask** *Ipmask*

Username Name of a network user.

Ipmask IP netmask in dotted decimal notation.

Usage

Enter the netmask number in dotted decimal notation. For more information, see the section on netmasks in the *PortMaster Configuration Guide*.

Example

Command> **set user jaime netmask 255.255.255.0**

Username:	jaime	Type:	Dial-in Network User
Address:	Assigned	Netmask:	255.255.255.0
Protocol:	SLIP	Options:	Quiet, Listen
MTU:	1006		

See Also

set user-netmask - page 16-13

set user ofilter

This command sets the output packet filter for packets leaving the PortMaster on the interface established by this dial-in network user.

set user *Username* **ofilter** [*Filtername*]

Username Name of a network user.

Filtername Output filter name. The maximum is 15 characters.

Usage

When an output packet filter is specified, packets being sent to the serial interface are evaluated against the rule set for this filter, which has been defined and is in the filter table. Only packets that are permitted by this filter are allowed to leave the PortMaster.

You remove the filter by entering the command without a filter name.



Note – This command does not apply to login users.

Example

Command> **set user joe ofilter student.out**

Username:	joe	Type:	Dial-in Network User
Address:	Negotiated	Netmask:	0.0.0.0
Protocol:	SLIP	Options:	Quiet, Compression
MTU:	1006		
Packet Filters:	/student.out		

See Also

add filter - page 13-4

set user ifilter - page 7-12

set user password

This command sets the password for a login user or network user.

set user *Username* **password** *Password*

Username Username of a login user or network user.

Password User password of 0 through 16 characters.

Usage

As shown in the example, the password is not displayed by any of the responses to a **set** or **show** command.

Example

Command> **set user marie password zasq2-ab**

Username: marie

Type: Dial-in Network User

Address: Negotiated

Netmask: 0.0.0.0

Protocol: SLIP

Options: Quiet, Listen

MTU: 1006

set user protocol

This command sets the transport protocol for a network user.

set user *Username* **protocol** **slip|ppp|x75-sync**

Username Name of a network user.

slip SLIP protocol. This is the default.

ppp PPP protocol.

x75-sync X.75 protocol.

Usage

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

Example

```
Command> set user mario protocol ppp
      Username: mario                      Type: Dial-in Network User
      Address:  Negotiated                  Netmask: 0.0.0.0
      Protocol: PPP                        Options: Quiet, Listen
      MTU: 1500                           Async Map: 0x00000000
```

See Also

set S0 network dialin - page 5-32

set user service

This command selects the login service for the login user.

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

<i>Username</i>	Name of a login user.
netdata	Uses a netdata connection (TCP clear channel).
portmaster	Uses the PortMaster login service to connect to in.pmd on the login host. This is the default.
rlogin	Uses the rlogin protocol to connect to the login host.
telnet	Uses Telnet to connect to the login host.
<i>Tport</i>	Designated TCP port on the host, a 16-bit number from 1 through 65535. The default is 23.

Example

Command> **set user sam service rlogin**

Username: sam

Type: Login User

Host: default

Login Service: rlogin (513)

See Also

set S0 service_login - page 5-42

set user session-limit

This command sets the maximum length of a session permitted before the PortMaster disconnects the user.

set user *Username* session-limit *Minutes*

Username Name of a user.

Minutes Session limit in minutes, any value from 0 to 240.
The default is 0.

Usage

You can set the user session limit in the user table using this command, or you can use the RADIUS Session-Timeout attribute. The RADIUS attribute is specified in seconds, but is rounded up to minutes by the PortMaster.

Examples

```
Command> set user joe session-limit 60
      Username:  joe                      Type:  Dial-in Network User
      Address:   Negotiated                Netmask: 0.0.0.0
      Protocol:  PPP                      Options: Quiet, Compression
      MTU:       1500                     Async Map: 00000000
      Port Limit: 2                      Idle Timeout: 30
      Session Lim: 60
```

See Also

set user idle - page 7-11

show table user

This command shows the current users in the user table.

show table user

Example

```
Command> show table user
```

Name	Type	Address/Host	Netmask/ Service	RIP
-----	-----	-----	-----	----
bill	Netuser	Assigned	ffffff00	No
hideo	Dialback User	default	Telnet	
marie	Netuser	192.168.1.74	fffffff	No
kwasi	Login User	default	PortMaster	
jill	Netuser	Negotiated	fffffff	Yes

See Also

show user - page 7-25

show user

This command shows the configuration of the specified user.

show user *Username*

Username A username of 1 through 8 characters.

Example

```
Command> show user jack
      Username:  jack                      Type:  Login User
      Host:      default                    Login Service:  portmaster
```

See Also

show table user - page 7-24

This chapter describes how to use the command line interface to configure the location table used for dial-out network connections. Detailed command definitions follow a command summary table. A summary table and details for the data link connection identifier (DLCI) table used for Frame Relay subinterfaces are also described.



Note – After making changes to a location that is in use, you must reset the port that the location is using.

Displaying Location Information.

Use the following commands to display information about the location table:

- **show table location**
- **show location** *Locname*
- **dial** *Locname* **-x**—see page 2-4
- **ifconfig**—see page 2-9

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of Location Commands

The commands in Table 8-1 are used to configure the location table for network dial-out.

DLCI commands begin on page 8-33.

Table 8-1 Location Table Commands

Command Syntax	
add location <i>Locname</i>	- see page 8-4
delete location <i>Locname</i>	- see page 8-5
save location	- see page 8-5
set location <i>Locname</i> analog on off	- see page 8-6
set location <i>Locname</i> automatic manual on_demand	- see page 8-7
set location <i>Locname</i> chap on off	- see page 8-8
set location <i>Locname</i> compression on off stac vj	- see page 8-9
set location <i>Locname</i> destination <i>Ipaddress</i>	- see page 8-10
set location <i>Locname</i> group <i>Group</i>	- see page 8-11
set location <i>Locname</i> high_water <i>Number</i>	- see page 8-12
set location <i>Locname</i> idletime <i>Number</i> [minutes seconds]	- see page 8-13
set location <i>Locname</i> ifilter [<i>Filtername</i>]	- see page 8-14
set location <i>Locname</i> ipxnet <i>Ipxnetwork</i>	- see page 8-15
set location <i>Locname</i> local-ip-address assigned Ipaddress	- see page 8-16
set location <i>Locname</i> map <i>Hex</i>	- see page 8-17
set location <i>Locname</i> maxports <i>Number</i>	- see page 8-18
set location <i>Locname</i> mtu <i>MTU</i>	- see page 8-19
set location <i>Locname</i> multilink on off	- see page 8-20
set location <i>Locname</i> nat inmap outmap defaultnapt Mapname blank [outsource]	- see page 14-14

Table 8-1 Location Table Commands (Continued)

Command Syntax	
set location <i>Locname</i> nat log sessionfail sessionsuccess syslog console on off	- see page 14-16
set location <i>Locname</i> nat sessiontimeout tcp other <i>Number</i> [minutes seconds]	- see page 14-17
set location <i>Locname</i> nat session-direction-fail-action drop icmpreject passthrough	- see page 14-19
set location <i>Locname</i> netmask <i>Ipmask</i>	- see page 8-21
set location <i>Locname</i> ofilter [<i>Filtername</i>]	- see page 8-21
set location <i>Locname</i> ospf on off [cost <i>Number</i>] [hello-interval <i>Seconds</i>] [dead-time <i>Seconds</i>] [nbma point-to-multipoint wan-as-stub-ptmp]	- see page 17-9
set location <i>Locname</i> password <i>Password</i>	- see page 8-22
set location <i>Locname</i> protocol slip ppp frame_relay x75-sync	- see page 8-23
set location <i>Locname</i> rip on off broadcast listen	- see page 16-20
set location <i>Locname</i> route-filter incoming outgoing <i>Filtername</i>	- see page 16-8
set location <i>Locname</i> script v25bis <i>RuleNumber</i> "String1" "String2"	- see page 8-24
set location <i>Locname</i> telephone <i>String</i>	- see page 8-26
set location <i>Locname</i> username <i>Username</i>	- see page 8-27
set location <i>Locname</i> voice on off	- see page 8-28
show location <i>Locname</i>	- see page 8-29
show table location	- see page 8-32

Location Commands

These commands configure the location table of the PortMaster.

add location

This command adds a location to the location table.

add location *Locname*

Locname Name of a remote location, up to 12 characters.

Usage

The location name is usually an identifier that represents an entire location—for example, a city or a company name at that location. It is not usually the name of a single system.

Example

```
Command> add location hq  
Location hq successfully added
```

See Also

delete location - page 8-5

save location - page 8-5

show table location - page 8-32

delete location

This command deletes a location from the location table.

delete location *Locname*

Locname Location name that is in the location table.

Example

```
Command> delete location hq
Location hq successfully deleted
```

See Also

add location - page 8-4

save location - page 8-5

show table location - page 8-32

save location

This command writes any changes to the location table to the nonvolatile memory of the PortMaster.

save location

Usage

The **save all** command can also be used.

Example

```
Command> save location
Location table successfully saved
New configurations successfully saved.
```

set location analog

This command sets the digital modems of a PortMaster 3 to analog modem service for dialing out to the specified location.

set location *Locname* **analog on|off**

<i>Locname</i>	Location name that is in the location table.
on	Enables analog modem service on dial-out.
off	Disables analog modem service on dial-out, and causes the service to revert to ISDN.

Usage

Use this command when analog rather than digital modem service is required for dial-out network connections.

Example

```
Command> set location hq analog on  
hq voice dial changed from off to on
```

See Also

set location voice - page 8-28

set location automatic|manual|on_demand

This command modifies configuration parameters for the specified location.

set location *Locname* **automatic|manual|on_demand**

<i>Locname</i>	Location name that is in the location table.
automatic	Sets the PortMaster to dial out to the location at boot time and to redial after a delay of 30 seconds if the connection drops.
manual	Sets the PortMaster to dial to the remote location when the administrator uses the dial command or pmdial utility. This keyword is also used for network dialback users. This is the default.
on_demand	Sets the PortMaster to dial to the remote location when packets are queued for that location.

Usage

For Automatic Dialing. If the telephone connection is lost, the PortMaster redials to that location. The redial mechanism in automatic mode is based on a back-off algorithm that begins at 30 seconds and continues forever.

For Manual Dialing. The request for connection can use the **dial** command, or it can be invoked from the **pmdial** utility installed on a network host. You can schedule connections by using the UNIX **cron** scheduler to call **pmdial**.

For On-demand Dialing. The PortMaster creates a network interface and the appropriate routing information to notify attached networks of the connectivity to the remote site. The PortMaster can perform these tasks whether or not an actual physical connection exists to that site at the time.

When changing a location from manual to on-demand, make sure to close the dial-out connection by resetting the serial port before updating the location table.

Example

```
Command> set location hq on_demand
hq changed to On-Demand Dial
```

See Also

reset dialer - page 2-15

set location idletime - page 8-13

set location chap

This command is used for configuring outbound CHAP authentication for a specified location.

set location *Locname* **chap on|off**

Locname Location name that is in the location table. The username and password entered in the location table are used as the system identifier and MD5 secret in the CHAP authentication. The secret is determined through the use of the Message-Digest Algorithm from RSA Data Security, Inc., as defined in RFC 1321.

on CHAP authentication is negotiated for the specified location.

off CHAP authentication is not supported for an outbound dial. This is the default.

Usage

The username and password entered in the location table are used as the system identifier and MD5 secret in the CHAP authentication. Use of this feature eliminates the need to use the system name and user table configurations for CHAP, unless the device being dialed also dials into the PortMaster.

See Also

set chap - page 3-6

set location password - page 8-22

set pap - page 3-16

set location compression

This command sets the use of Van Jacobson TCP/IP header compression and Stac LZS data compression for the location, improving interactive session performance.

set location *Locname* **compression on|off|stac|vj**

<i>Locname</i>	Location name that is in the location table.
on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3 and 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 Office Router products.
vj	Enables Van Jacobson TCP/IP header compression only.

Usage

Van Jacobson TCP/IP header compression can be used for SLIP and PPP connections. With SLIP, both sides need to be configured identically. For PPP connections, the PortMaster supports both bidirectional and unidirectional 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.

Example

```
Command> set location hq compression on  
hq compression changed from off to on
```

set location destination

This command sets the IP address expected for the system at the remote end of the dial-out connection.

set location *Locname* **destination** *Ipaddress*

Locname Location name that is in the location table.

Ipaddress IP address or hostname of between 1 and 39 characters of the destination.

Usage

For SLIP connections, enter the IP address or a valid hostname of the system at the remote end of the dial-up connection. The IP address or hostname can contain up to 39 characters. For PPP connections, the destination can be specified or negotiated. To negotiate the address, use 255.255.255.255.

Example

```
Command> set location hq destination 192.168.1.1  
hq destination changed from 0.0.0.0 to 192.168.1.1
```

set location group

This command defines which network dial-out ports can be used for a specified location.

set location *Locname* **group** *Group*

Locname Location name that is in the location table.

Group Dial group from 0 to 100. The default is 0.

Usage

Each location has a dial group number. Ports configured with this dial group number are available for dial-out to this location. This command 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.

Example

```
Command> set location hq group 1  
hq group number changed from 0 to 1
```

See Also

set S0 group - page 5-19

set W1 group - page 6-12

set location high_water

This command sets the number of bytes of queued network traffic required to open an additional dial-out line to the remote location.

set location *Locname* **high_water** *Number*

Locname Location name that is in the location table.

Number Number between 0 and 65535. The default is 0.

Usage

This value is used only when **maxports** is greater than 1 and network dial-out ports are available on the PortMaster. The PortMaster can quickly use all available ports for this location dial group if the **high_water** setting is too small.

Generally, interactive terminal traffic has no more than a few hundred bytes queued at any one time, but file transfers (for example, FTP) queue several thousand bytes. Consider size differences when deciding the number to use for **high_water**.

Example

```
Command> set location hq high_water 500  
hq high water level changed from 0 to 500
```

See Also

set location group - page 8-11
set location maxports - page 8-18

set location idletime

This command sets the length of time the line can be idle—in both directions—before the PortMaster disconnects the connection to a specified location.

set location *Locname* **idletime** *Number* [**minutes**|**seconds**]

<i>Locname</i>	Location name that is in the location table.
<i>Number</i>	Timeout value from 0 to 255. The default value is 0.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.

Usage

The idle timeout value is specified in minutes or seconds and can be any value from 0 to 255. It is for manual and on-demand locations.

If the idle timeout value is set to 0, the idle timer is disabled.

If the value is set to 2 seconds or a longer interval, the connection is disconnected after having no traffic for the designated time. RIP packets are not counted as traffic.

Example

```
Command> set location hq idletime 30  
hq idle timeout changed from 0 minutes to 30 minutes
```

set location ifilter

This command sets a packet filter for packets entering the PortMaster from the interface this location establishes.

set location *Locname* **ifilter** [*Filtername*]

Locname Location name that is in the location table.

Filtername Name of the input filter. The maximum is 15 characters.

Usage

When a filter is changed, any ports in use by the location must be reset to have the changes take effect.

You remove the filter by entering the command without a filter name.



Note – If a matching filter name is not in the filter table, this command is not effective and all traffic is permitted.

Example

Command> **set location hq ifilter hq.in**
New input filter set for location hq

See Also

add filter - page 13-4
set location ofilter - page 8-21

set location ipxnet

This command sets the IPX network number for the point-to-point connection.

set location *Locname* **ipxnet** *Ipxnetwork*

Locname Location name that is in the location table.

Ipxnetwork IPX network to be used for a serial link. A 32-bit hexadecimal value.

Usage



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

Specify this number only if you are routing IPX across the link. The number is only used for the serial link itself, and must be different from the IPX network numbers at each end of the Ethernet.

Example

Command> **set location home ipxnet 0x0f012345**
IPX network set to F012345

See Also

set ipx on - page 3-9

set location local-ip-address

This command allows a location to set a local IP address on a PortMaster dial-out asynchronous or ISDN port for numbered IP networks. Use this command only when a unique IP subnet is required for a point-to-point network connection.

set location *Locname* **local-ip-address assigned** | *Ipaddress*

<i>Locname</i>	Location name that is in the location table.
assigned	Local IP address is assigned by the unit that is dialed by this location. When the location <i>Locname</i> is dialed, the unit that answers the call assigns an address from its address pool to this WAN connection.
<i>Ipaddress</i>	IP address or hostname of between 1 and 39 characters.

Usage

This command is not needed for typical PortMaster operation. If this value is not set, the PortMaster uses the IP address of the Ether0 port.

Example

Command> **set location denver local-ip-address 192.168.96.6**
denver local ip address changed from 0.0.0.0 to 192.168.96.6

See Also

set location destination - page 8-10
set reported_ip - page 3-19

set location map

This command sets the PPP asynchronous map for a specified location.

set location *Locname* **map** *Hex*

Locname Location name that is in the location table.

Hex A 32-bit hexadecimal number. The default is 0x00000000.

Usage

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 must be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments must set the asynchronous map to zero to achieve maximum throughput. This command does not apply to the Serial Line Internet Protocol (SLIP).

The command **set location** *Locname* **map 0** disables the asynchronous mapping.

Example

```
Command> set location hq map 0x00000001
hq async character map changed to 0x00000001
```

set location maxports

This command sets the maximum number of network dial-out ports the PortMaster can use for this location.

set location *Locname* **maxports** *Number*

Locname Location name that is in the location table.

Number Number between 0 and 60. The default is 0.

Usage

If 0 is selected, dialing to this location is disabled. If a number greater than 1 is selected, the PortMaster uses the value of **high_water** to decide when to dial out on additional lines. If more than one line is open to the remote location, the PortMaster balances the load among the lines. If multiple lines are open, the idle time is used to decide when to disconnect unused lines.

The maximum number of ports must be the last setting configured for a location. When the number is set to greater than zero, the location is available for use.

Example

Command> **set location hq maxports 4**
hq maximum port count changed from 0 to 4

See Also

set location high_water - page 8-12

set location idletime - page 8-13

set location multilink - page 8-20

set location mtu

This command sets the maximum transmission unit (MTU) for the location.

set location *Locname* **mtu** *MTU*

Locname Location name that is in the location table.

MTU MTU value, from 100 to 1500 bytes.

Usage

The MTU defines the largest frame or packet that can be sent through this port without fragmentation. A packet that exceeds this value is automatically fragmented if IP, or discarded if IPX. PPP connections have a maximum MTU of 1500 bytes, and SLIP connections have a maximum of 1006 bytes.

Example

```
Command> set location denver mtu 1006  
denver mtu changed from 1500 to 1006
```

See Also

set location protocol - page 8-23

set location multilink

This command determines whether the PortMaster uses RFC 1990 Multilink PPP or PortMaster multiline load balancing for dial-out to a specified location through multiple ports.

set location *Locname* **multilink on|off**

<i>Locname</i>	Location name that is in the location table.
on	Enables Multilink PPP—for ISDN and analog connections only.
off	Enables PortMaster multiline load-balancing. This is the default.

Usage

PortMaster multiline load balancing and Multilink PPP provide methods for splitting, recombining, and sequencing packets across multiple logical data links. PortMaster multiline load balancing can be used only for communications between PortMaster products. In contrast, Multilink PPP can be used with an ISDN connection between devices that support the standard described in RFC 1990.

Example

```
Command> set location hq multilink on  
hq multilink changed from off to on
```

See Also

set location high_water - page 8-12
set location maxports - page 8-18

set location netmask

This command sets the IP netmask expected for the host or network at the remote end of the dial-out connection.

set location *Locname* **netmask** *Ipmask*

Locname Location name that is in the location table.

Ipmask IP netmask in dotted decimal notation.

Usage

Enter the netmask number in dotted decimal notation. For more information, see the section on netmasks in the *PortMaster Configuration Guide*.

Example

```
Command> set location hq netmask 255.255.255.0  
hq netmask changed from 0.0.0.0 to 255.255.255.0
```

set location ofilter

This command sets a packet filter for packets exiting the PortMaster to the interface this location establishes.

set location *Locname* **ofilter** [*Filtername*]

Locname Location name that is in the location table.

Filtername Name of the output filter. The maximum is 15 characters.

Usage

When a filter is changed, any ports in use by the location must be reset to have the change take effect.

To remove the filter, enter the command without a filter name.

Example

Command> **set location hq ofilter hq.out**
New output filter set for location hq

See Also

add filter - page 13-4
set location ifilter - page 8-14

set location password

This command sets up a password for automatic location table scripting for dialing to a remote location.

set location *Locname* **password** *Password*

<i>Locname</i>	Location name that is in the location table.
<i>Password</i>	PAP password associated with the username. Alternatively, this password can be used with CHAP if CHAP authentication is set on for the location; see page 8-8. The maximum password length is 64 characters.

Usage

Location table scripting, which uses this command together with the **set location telephone** and **set location username** commands, provides a simple alternative to setting up a V.25bis or chat dial script.

This is the preferred way for PPP users to set up location table scripting when dialing to a remote location.



Note – If you are configuring for dial-out SLIP, you must use the v.25bis script on page 8-24 instead of setting location username, password, and telephone.

Example

```
Command> set location denver password excalcolaur  
New password successfully set for location denver
```

See Also

set location chap - page 8-8
set location script - page 8-24
set location telephone - page 8-26
set location username - page 8-27

set location protocol

This command sets the protocol for encapsulating packets for the specified location.

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

<i>Locname</i>	Location name that is in the location table.
slip	SLIP protocol.
ppp	PPP protocol.
frame_relay	Frame Relay subinterface.
x75-sync	X.75 protocol.

Usage

PPP can be used with either IP or IPX packet routing, or both.

Example

```
Command> set location hq protocol ppp  
hq protocol changed to ppp
```

See Also

add dlci - page 8-33

set location mtu - page 8-19

set location script

This command sets up a dial script for dialing to a remote location.

```
set location Locname script|v25bis RuleNumber "String1" "String2"
```

<i>Locname</i>	Location name that is in the location table.
script	Enables a dial script for dial-out on an asynchronous port. The total length of all strings in the script must not exceed 256 characters.
v25bis	Enables a dial script for synchronous V.25bis protocol dial-out, for switched 56Kbps or ISDN.
<i>RuleNumber</i>	Rule number, from 1 to 98. Use rule number 99 to delete the script.
" <i>String1</i> "	Send string of up to 30 characters, in quotation marks.
" <i>String2</i> "	Expect string of up to 30 characters, in quotation marks.



Note – Alternatively, you can set up automatic location table scripting. This method is much simpler to administer, and is preferred for setting up location table scripting. See the commands **set location telephone**, **set location username**, and **set location password**—starting on page 8-26—for information.

Usage

Each send string is sent from the PortMaster to the modem or remote host. When the expect string is matched against the input from the remote end, the next line in the send string is sent, and so on. When the last line in the script is finished, the PortMaster activates the data link protocol specified for this location. Therefore, the last entry in the dial command script must be an expect string indicating that the remote location is ready to begin receiving network packets.

Any printable ASCII character can be placed in the send or expect strings. In addition, the following special characters are available:

<code>\r</code>	ASCII carriage return. Send strings usually end with the <code>\r</code> character. Do not use <code>\r</code> in the send string for the V.25bis protocol.
<code>\0XX</code>	Replaced by the octal digit in the XX.
<code>\\</code>	Replaced by a single backslash.

When you are connecting to a remote PortMaster, the final expect string to verify must be **SL/IP** for SLIP connections and **PPP** or a tilde (~) for PPP connections. A tilde is always the first character of a PPP frame. For other manufacturer's products, consult their manuals.

The dial script can also be used to implement outbound PAP authentication. If you specify a PAP username and password in the last line of the dial script, the PortMaster can be authenticated by the remote end using PAP. This capability is shown in the final example below.

Examples

```
Command> set location hq script 1 "atdt18005551212\r" "CONNECT"  
New script entry successfully added.
```

```
Command> set location hq script 2 "\r" "ogin:"  
New script entry successfully added.
```

```
Command> set location hq script 3 "my_login\r" "ssword:"  
New script entry successfully added.
```

```
Command> set location hq script 4 "my_password\r" "PPP"
New script entry successfully added.
```

```
Command> set location denver v25bis 1 "CRN7005552227" "=DCD="
New script entry successfully added.
```

```
Command> set location denver v25bis 2 "=PAP=my-login/my-password"
New script entry successfully added.
```

See Also

set location password - page 8-22
set location telephone - page 8-26
set location username - page 8-27

set location telephone

This command sets up a telephone number for automatic location table scripting for dialing to a remote location.

set location *Locname* **telephone** *String*

<i>Locname</i>	Location name that is in the location table.
<i>String</i>	Telephone number to dial. Specify multiple numbers by separating them with ampersands (&). The maximum string length is 64 characters.

Usage

Location table scripting, which uses this command together with the **set location username** and **set location password** commands, provides a simple alternative to setting up a V.25bis or chat dial script.

This is the preferred way for PPP users to set up location table scripting when dialing to a remote location.



Note – If you are configuring for dial-out SLIP, you must use the v.25bis script on page 8-24 instead of setting location username, password, and telephone.

Example

Command> **set location denver telephone 13035551212&13035551313**
New telephone successfully set for location denver

See Also

set location password - page 8-22
set location script - page 8-24
set location username - page 8-27

set location username

This command sets up a PAP or CHAP username for automatic location table scripting for dialing to a remote location.

set location *Locname* **username** *Username*

<i>Locname</i>	Location name that is in the location table.
<i>Username</i>	PAP or CHAP username to use when logging in to the remote location.
	The maximum name length is 64 characters.

Usage

Location table scripting, which uses this command together with the **set location telephone** and **set location password** commands, provides a simple alternative to setting up a V.25bis or chat dial script.

This is the preferred way for PPP users to set up location table scripting when dialing to a remote location.



Note – If you are configuring for dial-out SLIP, you must use the v.25bis script on page 8-24 instead of setting location username, password, and telephone.

Example

```
Command> set location denver username sanjose  
New username successfully set for location denver
```

See Also

set location chap - page 8-8
set location password - page 8-22
set location script - page 8-24
set location telephone - page 8-26

set location voice

This command forces a data-over-voice call on an outbound ISDN connection to a specified location.

set location *Locname* **voice on|off**

<i>Locname</i>	Location name that is in the location table.
on	Forces data-over-voice via 3.1KHz audio service on an outbound ISDN connection.
off	Disables data-over-voice on an outbound ISDN connection. This is the default.

Usage

Data over voice is supported for inbound and outbound ISDN connections. The PortMaster automatically accepts inbound voice calls and treats them as data calls.

Example

```
Command> set location denver voice on  
denver voice dial changed from off to on
```


See Also

add location - page 8-4

set location analog - page 8-6

show location

This command displays configuration information for a specified location.

show location *Locname*

Locname Location name that is in the location table.

Examples

Command> **show location sub1**

Location:	sub1	Type:	Sub-Interface
IP Address:	192.168.3.1	Netmask:	255.255.255.0
Protocol:	Frame Relay	Options:	Routing
Group:	1	Mtu:	1500
IP DLCI's:	DLCI	Address	
	---	-----	
	16	0.0.0.0	
	17	0.0.0.0	

Command> **show loc natloc**

Location:	natloc	Type:	Manual
Destination:	192.168.1.37	Netmask:	255.255.255.0
Local IP:	192.168.1.36		
Protocol:	PPP	Options:	Quiet VJ-Comp Multilink
Group:	1	Max Ports:	2
Idle Timeout:	0 minutes	High Mark:	0 bytes
Mtu:	1500	Async Map:	00000000
Username:	newuser	Password:	nat

Telephone: 94603774
 NAT parameters
SessionTimeOut: TCP: 1440 mins Other: 15 secs
Log Options: SessionFail Console
SessFailAction: drop

Explanation

Location	Location that is in the location table.
Type	Type of connection—on-demand, continuous, or manual. See page 8-7.
Destination	IP address or hostname of the destination.
Netmask	Netmask.
Local IP Address	IP address of the port used to dial to the location.
Protocol	Protocol used for encapsulating packets for this location—SLIP, PPP, Frame Relay, or X.75. See page 8-23.
Options	Enabled optional parameters for this location such as compression, PPP, multiline load balancing, and so on.
Group	Dial group number for this location.
Max Ports	Maximum number of network dial-out ports that the PortMaster can use for this location. See page 8-18.
Idle Timeout	Idle time limit set for this location.
High Mark	Bytes of queued packets required to open an additional dial-out line to the remote location. See page 8-12.
Mtu	Maximum transmission unit—the largest frame or packet that can be sent through this location without fragmentation. See page 8-19.
IP DLCIs	List of DLCIs identifying Frame Relay Subinterfaces and the IP address of each corresponding router.

Async Map	PPP asynchronous map for this location.
Username	User in the user table.
Password	User password.
Telephone	Telephone number for the remote location.
SessionTimeout	Idle time specified before the PortMaster issues a session timeout. See page 14-17.
Log Options	<p>Logging options specified for this location to monitor NAT sessions:</p> <ul style="list-style-type: none">• Log to the console or syslog.• Event logged—successful NAT translation (SessionSuccess) or failed NAT session (SessionFail).
SessFailAction	<p>Shows one of the following actions that the PortMaster takes in the event of a NAT session failure:</p> <p>Drop—Session packets are dropped without notifying the source host.</p> <p>ICMP reject—The PortMaster notifies the source host that packets are rejected.</p> <p>Pass—Packets are permitted to pass through untranslated.</p>

See Also

show all - page 2-22

show S0 - page 2-35

show table location

Network dial-out destinations are configured in the location table. This command shows the current entries in the location table.

show table location

Example

Command> show table location					
Location	Destination	Netmask	Group	Maxconn	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

Explanation

Location	Location name.
Destination	Destination IP address.
Netmask	Netmask.
Group	Group number.
Maxconn	Maximum connections.
Type	Type of connection: <ul style="list-style-type: none">• On demand• Continuous• Manual

DLCI Commands

The DLCI table commands in Table 8-2 configure the DLCI table used to split a Frame Relay interface into primary and secondary subinterfaces according to the data link connection identifier (DLCI).

Table 8-2 DLCI Table Commands

Command Syntax	
add dlci ipdlci ipxdlci <i>Locname Dlci</i> [: <i>Ipaddress</i> : <i>Ipxnode</i>]	- see page 8-33
delete dlci ipdlci ipxdlci <i>Locname Dlci</i>	- see page 8-35
show location <i>Locname</i>	- see page 8-29

add dlci

This command sets the Frame Relay subinterfaces for a specified location that has been configured to use Frame Relay service.

add dlci|ipdlci|ipxdlci *Locname Dlci* [:*Ipaddress*:*Ipxnode*]



Note – **ipdlci** is a synonym for **dlci**.

ipdlci or dlci	Use for IP connections.
ipxdlci	Use for IPX connections.
<i>Locname</i>	Location name that is in the location table.
<i>Dlci</i>	DLCI number, from 1 to 1023.
<i>:Ipaddress</i>	Optional IP address of the router attached to the permanent virtual circuit (PVC) represented by the DLCI.
<i>:Ipxnode</i>	IPX node address of the PortMaster attached to the permanent virtual circuit (PVC) represented by the DLCI. This value is the PortMaster MAC address—a 48-bit number.

Usage

The PortMaster supports a feature called DLCI bundling to allow one synchronous port with multiple DLCIs to be split into up to 32 Frame Relay subinterfaces. Each Frame Relay subinterface can have up to 50 DLCI mappings. Splitting is done through the use of the location table and the DLCI table.

The port to which the Frame Relay is connected must be set for Frame Relay, and must be in the same dial group as the location. Each subinterface must have its own subnet or network number.

The PortMaster can be configured for no more than 512 total active interfaces—or fewer if limited by available memory.

Refer to the *PortMaster Configuration Guide* for more information.

You can change values in the **add dlci** command by repeating the command with new values. You do not need to delete the existing DLCI entries before changing the values.

Example

In this example, port **S1** is configured for Frame Relay and a new location **sub1** is configured as a subinterface. Commands and responses are shown.

```
Command> set s1 protocol frame
Protocol for port S1 changed from slip to frame_relay
```

```
Command> set s1 group 1
Group number for port S1 changed from 0 to 1
```

```
Command> add location sub1
Location sub1 successfully added
```

```
Command> set location sub1 protocol frame
sub1 protocol changed to frame_relay
```

```
Command> set location sub1 group 1
sub1 group number changed from 0 to 1
```

```
Command> set location sub1 address 192.168.3.1
sub1 destination changed from 0.0.0.0 to 192.168.3.1
```

```
Command> set location sub1 netmask 255.255.255.0  
sub1 netmask changed from 0.0.0.0 to 255.255.255.0
```

```
Command> set location sub1 routing on  
sub1 routing changed from off to on (broadcast,listen)
```

```
Command> add dlci sub1 16  
New dlci successfully added
```

```
Command> add dlci sub1 17  
New dlci successfully added
```

```
Command> save all  
Command> reset s1
```

See Also

add dlci - page 6-10

delete dlci

This command deletes entries from the DLCI table.

delete dlci|ipdlci|ipxdlci *Locname* *Dlci*

dlci or **ipdlci** Use for IP connections.

ipxdlci Use for IPX connections.

Locname Specified location name that is in the location table.

Dlci DLCI number, from 1 to 1023. You can delete only one DLCI at a time.

Usage

This procedure is the reverse of adding the DLCI subinterfaces. You can confirm the removal by using the **show location** command.

Examples

Command> **delete dlci sub1 16**
DLCI successfully deleted

Command> **delete dlci sub1 17**
DLCI successfully deleted

See Also

add dlci - page 8-33
delete dlci - page 6-4

This chapter describes how to use the command line interface to configure the parallel port, **p0**, included on some PortMaster products. Detailed command definitions follow a command summary table.

Displaying Parallel Port Information

The following command is available to show the configuration of the parallel port:

- **show p0**—see page 2-35

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of Parallel Port Commands

The parallel port commands in Table 9-1 configure the parallel port P0. See Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1, for the range of ports available on each PortMaster model.

Table 9-1 Parallel Port Configuration

Command Syntax	
reset p0	- see page 2-15
save p0	- see page 2-18
set p0 device <i>Device</i>	- see page 9-2
set p0 disabled	- see page 9-2
set p0 disconnect <i>Seconds</i> infinity	- see page 9-3
set p0 extended on off	- see page 9-4
set p0 host default prompt [1 2 3 4] <i>Ipaddress</i>	- see page 9-4
set p0 service_device netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 9-5

Table 9-1 Parallel Port Configuration (*Continued*)

Command Syntax	
show all	- see page 2-22
show p0	- see page 2-35

Parallel Port Commands

These commands are used to configure the parallel port (P0) of the PortMaster.

set p0 device

This command sets the parallel port to operate as a host-controlled device.

set p0 device *Device*

Device Device designation—for example, **/dev/ttyrf**.

Usage

In the following example, a PortMaster host device **/dev/ttyrd** is shown. To use the PortMaster device service, you must have the PortMaster **in.pmd** daemon installed on the specified host.

Example

Command> **set p0 device /dev/ttyrd**
Port type for port P0 changed from Device to Host Device(/dev/ttyrd)

set p0 disabled

This command disables the parallel port.

set p0 disabled

Usage

To enable the port, set it as a host device—for example, **set p0 device /dev/ttyrd**.

Example

```
Command> set p0 disabled
Port type for port P0 changed from Device to Disabled
```

See Also

set p0 device - page 9-2

set p0 disconnect

This command sets the disconnection timeout for the parallel port.

set p0 disconnect *Seconds* | **infinity**

Seconds Number of seconds. Default is 120.

infinity Infinite timeout. This setting effectively disables a disconnection timeout.

Usage

The timeout feature disconnects a session from the port when the port has been inactive for the designated time. The port is then available for other sessions.

The infinite timeout feature is useful, for example, for printers that go offline when they run out of paper, but that you do not want to disconnect and thereby terminate the print job.

Example

```
Command> set p0 disconnect 240
Disconnect timeout for port P0 changed from 120 to 240
```

set p0 extended

This command sets the extended display mode on or off for the parallel port.

set p0 extended on|off

on	Turns extended mode on.
off	Turns extended off. This is the default.

Usage

When extended mode is on, the **show p0** command provides more detailed output.

Example

```
Command> set p0 extended on  
Extended mode for port P0 changed from off to on
```

set p0 host

This command sets the device host for the parallel port.

set p0 host default|prompt|[1|2|3|4] *Ipaddress*

default	Uses the default host as device host.
prompt	Displays the host prompt before the login prompt. The user is required to enter a valid hostname or Internet address for a host on the network. Entering PPP or SLIP at the prompt returns a login prompt.
<i>Ipaddress</i>	Uses the host with this IP address or hostname of between 1 and 39 characters as the device host.
1 2 3 4	Used to specify alternate hosts, with the primary host being 1. The default is 1.

Usage

The host must have the **in.pmd** daemon installed.

Example

```
Command> set p0 host 192.168.200.2
Host changed from default to 192.168.200.2 for P0
```

See Also

set host - page 5-21

set p0 service_device

This command indicates device service to be used by the parallel port.

```
set p0 service_device netdata|portmaster|rlogin|telnet [Tport]
```

netdata	Allows netdata connections to this port from the network.
portmaster	Used for host device emulation from a host with the in.pmd daemon installed.
rlogin	Allows rlogin connections to this port from the network.
telnet	Allows Telnet connections to this port from the network.
<i>Tport</i>	Specifies the designated TCP port on the host, from 1 to 65535.

Usage

The host device must be set as the port type for any port that is to act as a host-controlled device on a workstation. This capability allows users to connect through the PortMaster to shared devices such as printers.

Example

Command> **set p0 service_device portmaster**
Device Service for port P0 changed from to portmaster

See Also

set p0 device - page 9-2

This chapter describes how to configure the host table in the nonvolatile RAM of the PortMaster.

Each host attached to an IP network has a unique IP address. The PortMaster supports a local host table to map hostnames to IP addresses. Hostnames are for the convenience of the administrator who uses the command line interface, and to record hostnames entered by users at the host prompt. To avoid confusion and reduce administrative overhead, Lucent recommends using the Domain Name Service (DNS) or Network Information Service (NIS) for hostname resolution rather than using the local host table.

Displaying Host Information

To display information about the host table, use the following command:

- **show table host**

For general information about command line interface commands, see Chapter 1, "Introduction."

Summary of Host Commands

For information on setting the NIS or DNS server and domain, refer to Chapter 3, "Global Commands."

The host table commands in Table 10-1 are used to configure the host table.

Table 10-1 Host Table Commands

Command Syntax	
add host <i>Ipaddress String</i>	- see page 10-2
delete host <i>Ipaddress String</i>	- see page 10-2
save hosts	- see page 10-3
show table host	- see page 10-3



Note – The PortMaster always checks the local host table before using DNS or NIS.

Host Commands

These commands are used to maintain the PortMaster host table.

add host

This command adds a host to the host table.

add host *Ipaddress String*

Ipaddress IP address of the host.

String String of printable characters representing the hostname.
Maximum length is 39 characters.



Note – You can add duplicate IP addresses, but hostnames must be unique.

Example

Command> **add host 192.168.200.4 chopin**
New host entry successfully added

delete host

This command deletes a host from the host table.

delete host *Ipaddress|String*

Ipaddress IP address of the host.

String Hostname.



Caution – If you delete a duplicate IP address, the first IP address from the host table is also deleted.

Examples

```
Command> delete host chopin  
Host entry successfully deleted
```

save hosts

This command writes the current host table to the nonvolatile RAM of the PortMaster.

save hosts

Usage

You can also save the current host table using the **save all** command.

Example

```
Command> save hosts  
Hosts table successfully saved  
New configurations successfully saved.
```

show table host

This command displays the host table from the PortMaster.

show table host

Example

```
Command> show table host  
192.168.200.4      chopin  
172.16.200.3       elgar
```

This chapter describes how to use the command line interface to configure ISDN BRI ports. Detailed command definitions follow a command summary table.

Examples in this chapter are from a PortMaster 2ER, which uses the indicator *S10* for the first ISDN BRI port when an ISDN expansion module is present. PortMaster products also use other designations for ISDN BRI ports, depending on the model and configuration. Refer to Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1, for the range of ISDN BRI ports available on PortMaster models.

Displaying ISDN Port Information

To display ISDN debug information on the console, use the following commands:

- **set console**—see page 2-20
- **set debug isdn on**—see page 19-8
- **show isdn**
- **show S10**—see page 2-35

For general information about using the command line interface, refer to Chapter 1, “Introduction.”

Summary of ISDN BRI Commands

ISDN BRI commands allow you to configure the switch provisioning values, including the service profile identifier (SPID) and the directory number (DN). The commands are shown in Table 11-1, where those marked with a leading bullet (•) are specifically for ISDN. Additionally, ISDN BRI ports can be configured similarly to asynchronous and synchronous ports.

Table 11-1 ISDN Port Commands

Command Syntax	
attach <i>S10</i>	- see page 5-6
• reset <i>dNumber</i>	- see page 2-15
reset <i>S10</i>	- see page 2-15
save <i>S10</i>	- see page 2-18
save ports	- see page 2-18
set debug isdn	- see page 19-8
• set isdn-msn on off	- see page 11-4
set isdn-numberauto on off	- see page 11-5
set isdn-numberplan 0 1 2 7 8	- see page 11-6
set isdn-numbertype 0 1 2 4	- see page 11-7
• set isdn-switch net3 net5 vn2 vn4 1tr6 ntt kdd	- see page 11-9
• set isdn-switch ni-1 dms-100 5ess 5ess-ptp	- see page 11-9
set pots on off	- see page 3-18
• set <i>S10</i> address <i>Ipaddress</i>	- see page 5-10
• set <i>S10</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]	- see page 11-10
set <i>S10</i> device <i>Device</i> [network dialin dialout twoway]	- see page 5-16
set <i>S10</i> dialback_delay <i>Seconds</i>	- see page 5-17
• set <i>S10 all</i> directory dn <i>Number</i>	- see page 11-11
set <i>S10 all</i> extended on off	- see page 5-19
set <i>S10</i> group <i>Group</i>	- see page 5-19
set <i>S10</i> hangup on off	- see page 5-20
set <i>S10 all</i> host default prompt [1 2 3 4] <i>Ipaddress</i>	- see page 5-21
set <i>S10 all</i> idletime <i>Number</i> [seconds minutes]	- see page 5-22
set <i>S10 all</i> ifilter [<i>Filtername</i>]	- see page 5-24
set <i>S10 all</i> login [network dialin dialout twoway]	- see page 5-26

Table 11-1 ISDN Port Commands (Continued)

Command Syntax	
set <i>S10</i> all message <i>String</i>	- see page 5-28
set <i>S10</i> all network dialin dialout twoway	- see page 5-32
set <i>S10</i> all network hardwired	- see page 11-12
set <i>S10</i> all ofilter [<i>Filtername</i>]	- see page 5-34
set <i>S10</i> ospf	- see page 17-9
set <i>S10</i> all prompt <i>String</i>	- see page 5-37
set <i>S10</i> all security on off	- see page 5-40
set <i>S10</i> all service device netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 5-41
set <i>S10</i> all service login netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 5-42
set <i>S10</i> speed	- see page 11-13
• set <i>S10</i> all spid <i>Number</i>	- see page 11-14
set <i>S10</i> all termtype <i>String</i>	- see page 5-45
set <i>S10</i> twoway <i>Device</i> [network dialin dialout twoway]	- see page 5-46
set <i>S10</i> username autolog [<i>String</i>]	- see page 5-47
show all	- see page 2-22
show isdn [<i>dNumber</i> <i>S10</i>]	- see page 11-15
show pots	- see page 3-23
show <i>S10</i>	- see page 2-35

ISDN BRI Commands

These commands are used for configuring the ISDN BRI ports of the PortMaster. Table A-1, “Configurable Ports Available for Each PortMaster Model,” on page A-1 lists the range of ISDN ports available on each PortMaster model.

set isdn-msn

This command enables the multiple subscriber network (MSN) feature for countries that support BRI via the ISDN S/T bus interface.

set isdn-msn on|off

on	Enables the MSN feature.
off	Disables the MSN feature. This is the default.

Usage

Countries that use international ISDN standards—for example, Japan and the European countries—support BRI via the S/T interface, which can behave as either point-to-point line or a bus. In contrast, the U interface—used in North America—is a point-to-point interface. Multiple ISDN devices, such as a telephone, fax, computer with ISDN card, or PortMaster, can be attached to an S/T bus at the same time. When an incoming call is switched to the S/T bus, it is broadcast to all the attached devices on the D channel. Each attached device then checks the call, and the device with the matching information elements (IEs) for called party (directory number) and bearer capability accepts the call.

When the MSN feature is enabled, the PortMaster checks the called party IE for a match with its directory number. If the directory number matches the called party IE, the PortMaster checks the bearer capability IE for a call type match. If the call type—for example, unrestricted data—matches, the PortMaster accepts the call. If either or both the called party and bearer capability IEs do not match, the PortMaster does not reject the call, but allows other S/T connected devices to check and accept the call. However, when the MSN feature is disabled, the PortMaster rejects the call if a port is not available and the bearer capability IE does not match that of the PortMaster. In this case other S/T connected devices are not given an opportunity to check or accept the call.



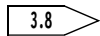
Note – The current MSN feature setting is displayed in the output to the **show global** command.

See Also

show global - page 2-28

set isdn-numberauto

This command enables the PortMaster to automatically determine the ISDN number plan and number type for a received call.



set isdn-numberauto on|off

- | | |
|------------|--|
| on | Enables automatic ISDN number plan and type determination. |
| off | Disables automatic ISDN number plan and type determination. This is the default. |

Usage

When this feature is set to **on**, the **show global** command output displays an added line to indicate that it is enabled.

Any ISDN number type or number plan automatically determined by the PortMaster when this feature is on overrides entries specified with the **set isdn-numbertype** and **set isdn-numberplan** commands.

Example

```
Command>set isdn-numberauto on
numberauto now on
```

See Also

set isdn-numberplan - page 11-6
set isdn-numbertype - page 11-7
show global - page 2-28
show isdn d0 - page 11-15

set isdn-numberplan

This command changes the existing ISDN number plan.

3.8

set isdn-numberplan 0|1|2|7|8

- | | |
|----------|----------------------------------|
| 0 | Unknown. |
| 1 | ISDN E.164. This is the default. |
| 2 | Telephony E.163. |
| 7 | National. |
| 8 | Private. |

Usage

The ISDN number plan and type informs the switch what kind of call is being placed and where the call is to be routed. The PortMaster learns the ISDN number plan automatically when the **set isdn-numberauto on** command is used, unless a specific number plan is entered with the **set isdn-numberplan** command.

To display all the number plan attribute values available and the current setting, enter **set isdn-numberplan** without any arguments. You can also view the current ISDN number plan and number type by displaying the **show global** command.



Note – Although the change in number plan takes place immediately after you enter the command, you must use the **save all** command to save changes to nonvolatile RAM.

Examples

```
Command> set isdn-numberplan  
set isdn-numberplan <plan>  
plans:  
0      unknown  
1      ISDN E.164  
2      Telephony E.163  
7      National  
8      Private  
current type - 1, ISDN E.164  
Command>
```

```
Command> set isdn-numberplan 7  
numberplan now National
```

See Also

set isdn-numberauto - page 11-5
set isdn-numbertype - page 11-7
show global - page 2-28
show isdn d0 - page 11-15

set isdn-numbertype

This command changes the existing ISDN number type.

3.8

```
set isdn-numbertype 0|1|2|4
```

0	Unknown.
1	International.
2	National.
4	Local.

Usage

The ISDN number plan and type informs the switch what kind of call is being placed and where the call is to be routed. The PortMaster learns the ISDN number plan automatically when the **set isdn-numberauto on** command is used, unless a specific number plan is entered with the **set isdn-numbertype** command.

To display all the number type attribute values available and the current setting, enter **set isdn-numbertype** without any arguments. You can also view the current ISDN number plan and number type by displaying the **show global** command.



Note – Although the change in number type takes place immediately after you enter the command, you must use the **save all** command to save changes to nonvolatile RAM.

Examples

```
Command> set isdn-numbertype
set isdn-numberplan <type>
types:
0      unknown
1      International
2      National
4      Local
current type - 4, Local
Command>
```

```
Command> set isdn-numbertype 4
numbertype now Local
```

See Also

set isdn-numberauto - page 11-5
set isdn-numberplan - page 11-6
show global - page 2-28
show isdn d0 - page 11-15

set isdn-switch

This command sets the switch provisioning for ISDN connections to the PortMaster ISDN BRI ports.

```
set isdn-switch ni-1|dms-100|5ess|5ess-ptp
```

```
set isdn-switch net3|net5|vn2|vn4|1tr6|ntt|kdd
```

ni-1	National ISDN-1 (NI-1) compliant. This is the default.
dms-100	Northern Telecom DMS-100 Custom.
5ess	AT&T 5ESS Custom Multi-Point.
5ess-ptp	AT&T 5ESS Custom Point-to-Point.
net3	European ISDN standard (includes Swiss extensions).
net5	Australia.
vn2	France.
vn4	France—current National switch.
1tr6	Germany—older switch.
ntt	Japan.
kdd	Japan.

Usage

The switch provisioning information is available from your ISDN telephone service provider. DMS-100 and 5ESS switches can operate with either switch-specific software, or the more universal NI-1 software. When your ISDN telephone switch has NI-1 software, you must use the NI-1 value. Any change you make in the switch provisioning setting does not take effect until the PortMaster is rebooted.

Examples

For an AT&T 5ESS switch with switch-specific software:

```
Command> set isdn-switch 5ess  
ISDN switch type set to ATT-5ESS  
Command> save all  
Command> reboot
```

For an AT&T 5ESS switch with NI-1 software:

```
Command> set isdn-switch ni-1  
ISDN switch type set to NI-1  
Command> save all  
Command> reboot
```

See Also

set S10 directory - page 11-11
set S10 spid - page 11-14

set S10 destination

This command sets the IP address and the netmask of the remote router for a network hardwired BRI port connection.

set S10 destination *Ipaddress* [*Ipmask*]

Ipaddress IP address or 39-character hostname of the remote router in dotted decimal notation.

Ipmask IP mask in dotted decimal notation.

Usage

If the remote destination is set to 255.255.255.255 for PPP connections, the PortMaster attempts to learn the remote IP address. If set to 0.0.0.0, the port is disabled.



Note – This command is used only for network hardwired BRI ports.

Example

Command> **set S10 destination 255.255.255.255**
Port S10 destination changed from 0.0.0.0 to 255.255.255.255

See Also

set S0 destination - page 5-15
set W1 destination - page 6-9

set S10|all directory

This command sets the directory number (DN) for a port so that an incoming call that matches the number uses this port.

set S10|all directory|dn *Number*

<i>S10</i>	The ISDN port.
<i>Number</i>	The access telephone number provided by your ISDN telephone service provider—from 0 to 15 characters.

Usage

The directory numbers for the two bearer (B) channels are normally different, and both of the corresponding PortMaster ports need to be configured with the correct directory number.

You can simultaneously set all ISDN ports to the same directory number by using the **set all dn** command.

3.8

BACP and BAP Support. ComOS 3.8 and later releases support the Bandwidth Allocation Control Protocol (BACP), according to RFC 2125. Because BACP and the Bandwidth Allocation Protocol (BAP) are both negotiated protocols, no commands are

necessary to turn them on. The only requirement for the use of BAP and BACP is setting directory numbers on the serial ports so the PortMaster can offer a second number to the client dialing in.

BACP supports local exchange telephone numbers. If a long-distance BACP user is configured to dial a local exchange telephone number, the PortMaster checks the Called-Station-Id when the second channel is requested. To implement this configuration, do not set the directory numbers.

Examples

```
Command> set s10 directory 5551212  
Directory No for port S10 changed from    to 5551212
```

```
Command> set s11 dn 5551213  
Directory No for port S11 changed from    to 5551213
```

See Also

set isdn-switch - page 11-9

set S10|all network hardwired

This command sets a single BRI line or both BRI lines for a permanent network connection that requires no dialing or authentication.

set S10|all network hardwired

Usage

ComOS 3.7 and later releases support European leased line ISDN facility—no ISDN signaling is involved.

You can set the port type to **network hardwired** for one BRI, or all ports simultaneously, by using the **set all network hardwired** command.

You must also set the address of the other end of the network hardwired connection with the **set S10 destination** command.

Use this command for ports used in a dedicated or hardwired network connection between two sites. The port immediately begins running the specified protocol.



Note – You must use the **save all** and **reboot** commands for the changes to take effect.

Example

Command> **set s10 network hardwired**

Port type for port S10 changed from Login to Network(hardwired)

See Also

set S10 destination - page 11-10

show isdn d0 - page 11-15

set S10 speed

This command sets the baud rate for a single BRI line.

```
set S10 speed [1|2|3] 300|600|1200|2400|4800|9600|19200|  
38400|57600|76800|115200|128000
```

<i>S10</i>	ISDN port.
1 2 3	Indicates which of the three baud rates is being set: 1, 2, or 3. Default is 1.
300 600 , and so on	Indicates the data terminal equipment (DTE) rate. Default is 9600bps.

Usage

ComOS 3.7 and later releases support a line speed of 128Kbps for BRI ports. Only one BRI line can be configured for 128Kbps, and when it is configured for this rate, the second line is placed into a NO-SERVICE state.

Examples

Command> **set s1 speed 128000**

Speed for port S10 (1) changed from 9600 to 128000

set S10|all spid

This command sets the service profile identifier (SPID) numbers for the bearer (B) channels of the ISDN connection.

set S10|all spid *Number*

S10 ISDN port.

Number Integer—between 7 and 14 digits long—provided by the ISDN service provider.

Usage

The SPID numbers for each of the two B channels are provided by your ISDN service provider. The SPID numbers for the two B channels are normally different, and both of the corresponding PortMaster ports need to be configured with the correct SPID number.

You can simultaneously set all the B channels on all ISDN ports to the same SPID number by using the **set all spid** command. Although the **set all spid** command is not typically used in a BRI configuration, it can be useful for diagnosing a BRI problem.



Note – SPID numbers can vary by service provider.

Example

Command> **set s10 spid 700555111100**

SPID for port S10 changed from to 700555111100

See Also

set isdn-switch - page 11-9
set S10 dn - page 11-11

show isdn

Shows the status of the ISDN ports.

show isdn [*dNumber*|*S10*]

- dNumber* D channel number.
- S0* Serial port number associated with the BRI port.

Usage

To display comprehensive information about a BRI port, enter the command with the active D channel number or the serial port number associated with the BRI port.

For information on using this command to diagnose BRI problems, refer to the *PortMaster Troubleshooting Guide*.

Example 1

For all ISDN ports on a PortMaster:

Command> show isdn											
D	Ports	State	Change	Start	Up	Down	Time	Sess	In	Out	Err
--	-----	-----	-----	---	---	----	----	---	-----	-----	--
0	S0/S1	Active	12days	2	2	0	0	7	232435	242617	0
1	S2/S3	Active	23:59	4	4	0	0	84	234492	243629	2
2	S4/S5	Active	12days	2	2	0	0	32	225771	236417	0
3	S6/S7	Active	12days	2	2	0	0	10	215027	224158	0

Explanation 1

D	D channel associated with an active session.
Ports	ISDN port numbers on the PortMaster.
State	Line status.
Change	Time since the last change in status.
Start	Number of times a network termination 1 device (NT1) has attempted to bring up a link.
Up	Number of times a link has gone to up status.
Down	Number of times a link has gone to down status.
Time	Number of times a D channel has timed out attempting to bring up the link.
Sess	Number of times the PortMaster has received a connect message from the switch.
In	Number of ISDN frames input on a B channel.
Out	Number of ISDN frames output on a B channel.
Err	Number of cyclic redundancy check (CRC), abnormal termination, overrun, bad byte count (bbc), and lost frame errors.

Example 2

For the ports associated with the D channel d0:

```
Command> show isdn d0
D00 status ----- BRI_NI1
Interface state:      F7- active
Init count: 1         uptime: 4days      last state change: 4days
recv count:  75159    xmit:   79418      errors:         0
numberplan          type:   Local    plan: ISDN E.164
S1 -----
Ces state: Connected  last change: 4days  Port state: ESTABLISHED
Directory: 5105557770 SPID:   510555777000  regs:         1
Called:      7771 Caller:                Flags: 0x00
```

```

Connects:      1          last connect: 4days   b channel: 1
Setup: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
S2 -----
Ces state: Connected      last change: 4days   Port state: ESTABLISHED
Directory:                SPID:   510555777101  regs:      1
Called: 5557771          Caller:                Flags: 0x00
Connects:      1          last connect: 4days   b channel: 2
Setup: 04 03 08 00 10 18 02 01 02 34 01 4f 70 09 04 01
35 35 35 37 37 37 31 04 02 88 90 18 01 8a 34 01
271: msg 19 SPID Register ERROR, cause 1 Unassigned Number

```

Explanation 2

D	Active D channel number.
BRI	Active switch type.
Interface State	Interface state:
	F0 Inactive.
	F3 Deactivated.
	F4 Awaiting signal.
	F5 Identifying input.
	F6 Synchronized.
	F7 Active.
	F8 Temporary framing lost.
Init Count	Number of Layer 1 activations.
uptime	Current Layer 1 uptime.
last state change	Time since last Layer 1 uptime.
recv count	Number of input D channel packets.
xmit	Number of output D channel packets.
errors	Number of D channel errors.
type	ISDN number type.
plan	ISDN number plan.
S0	Serial port number.

Ces state	Status of the BRI line or leased line configuration if the port is configured as a leased line network hardwired port: <ul style="list-style-type: none">• Idle.• Registering—transition state—SPID registration is in progress.• Registered.• Connecting—transition state—call is in the process of being connected.• Connected—connected BRI line.• Hangup—transition state—call is being terminated.• Leased line—port is configured as network hardwired.
Port state	Line status—established or idle.
Directory	Directory number.
SPID	Service profile identifier.
regs	Number of SPID registration attempts.
Called	Called directory number.
Caller	Caller telephone number.
Flags	Call attributes.
Connects	Number of successful calls.
last connect	Duration of the last call.
b channel	B channel number.
Setup	Image of caller information for this session.

This chapter describes how to use the command line interface to configure the ISDN Primary Rate Interface (PRI) **line0** and **line1**, the optional T1 expansion card for the PortMaster 3, and the digital modems on the PortMaster for the following kinds of services:

T1 Line0 through Line3	E1 Line0 through Line2
Full T1	Full E1
Fractional T1	Fractional E1
Channelized T1	Multifrequency R2 (MFR2) signaling for channelized E1
ISDN Primary Rate Interface (PRI)	ISDN PRI
	Fractional PRI



Caution – The T1 card is hot-swappable. After removing the card from the PortMaster 3 slot, you must wait for a few seconds before re-inserting it. If you remove the T1 card and re-insert it immediately, the PortMaster 3 locks up and you must turn it off and on again to restart.

This chapter also describes commands for configuring non-facility associated signaling (NFAS) for a T1 line on the PortMaster.

See the *PortMaster Configuration Guide* for more information about configuring T1, E1, and ISDN PRI lines, digital modems, and NFAS.



Note – After making any configuration changes to Line0 or Line1 or to the T1 expansion card, you must use the **save all** and **reboot** commands for the changes to take effect.

Displaying T1, E1, and PRI Diagnostic Information

To display T1, E1, or PRI ISDN debug information on the console, use the following commands:

- **set console**—see page 2-20
- **set debug isdn**—see page 19-8
- **set debug mdp-status**—see page 19-11
- **set debug nfas**—see page 19-13

When finished, use the following commands:

- **set debug off**—see page 19-6
- **reset console**—see page 2-15

To display line configuration or status, use the following commands:

- **show global**—see page 2-28
- **show Line0**
- **show mcppp**
- **show modems**
- **show nfas**
- **show nfas history**
- **show nfas stat**
- **show sessions**—see page 2-39
- **show MO**

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of T1, E1, and PRI Commands

T1, E1, and PRI configuration commands are shown in Table 12-1.

Table 12-1 T1, E1, and PRI Configuration Commands

Command Syntax	
attach <i>S0</i>	- see page 5-6
reset <i>M0</i>	- see page 12-5
reset <i>V0</i>	- see page 12-5
save all	- see page 2-18
set call-check on off	- see page 3-4
set debug isdn isdn-dframes isdn-d0 isdn-l1 D0 termination isdn-v120 on off	- see page 19-8
set debug mdp-events mdp-max mdp-status on off	- see page 19-11
set debug nfas on off	- see page 19-13
set endpoint <i>Hex</i>	- see page 12-6
set isdn-switch net5 vn2 vn3 ltr6 ntt kdd ts014	- see page 12-7
set isdn-switch ni-2 dms-100 4ess att-5ess	- see page 12-7
set <i>Line0 line2</i> encoding b8zs ami hdb3	- see page 12-8
set <i>Line0 line2</i> framing esf d4 crc4 fas	- see page 12-9
set <i>Line0 line2</i> group <i>Cgroup</i> 56k 64k	- see page 12-9
set <i>Line0 line2</i> group <i>Cgroup none</i> channels <i>Channel-list</i>	- see page 12-10
set <i>Line0</i> isdn t1 e1 fractional isdn-fractional inband	- see page 12-11
set line2 t1 fractional	- see page 12-11
set <i>Line0 line2</i> loopback on off	- see page 12-13

Table 12-1 T1, E1, and PRI Configuration Commands (Continued)

Command Syntax	
set <i>Line0</i> nfas pri sec sla dis <i>Identifier Group</i>	- see page 12-14
set <i>Line0</i> pcm u-law a-law	- see page 12-16
set <i>Line0</i> signaling wink immediate fxs	- see page 12-17
set <i>Line0</i> signaling r2generic mfr2 <i>Profile</i>	- see page 12-18
set <i>Line0 line2</i> clock internal external	- see page 12-19
set location <i>Locname</i> analog on off	- see page 12-20
set <i>MO</i> on off	- see page 12-20
set <i>MO</i> lastcall	- see page 12-21
set <i>SO</i> directory <i>Number</i>	- see page 12-22
show all	- see page 2-22
show <i>Line0 line2</i>	- see page 12-23
show <i>MO</i>	- see page 12-27
show mcppp	- see page 12-29
show modems	- see page 12-30
show nfas	- see page 12-31
show nfas history	- see page 12-33
show nfas stat	- see page 12-34

T1, E1, and PRI Commands

These commands are used for displaying the status of and configuring the ISDN PRI E1 or T1 lines, the T1 expansion card, digital modems, and Multichassis PPP connections of the PortMaster 3.

reset M0

This command resets an internal digital modem and reloads its digital signal processor (DSP) code.



reset M0

M0 Digital modem number **m0** through **m59**.

Example

```
Command> reset m0
M0: Modem Resetting
Command> reset m1
M1: Modem Resetting
```

See Also

set M0 - page 12-20

reset V0

When you are using Multichassis PPP, this command resets a virtual port on the master unit and the corresponding physical port on the slave unit.

reset V0

V0 Virtual port number, 0, 1, and so on.

Usage

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.

See Also

set endpoint - page 12-6

set endpoint

This command enables Multichassis PPP, which supports RFC 1990 Multilink PPP across multiple PortMaster products sharing an Ethernet.

set endpoint *Hex*

Hex End point discriminator—a 1 to 12-digit hexadecimal number. ComOS appends zeros if you specify fewer than 12 digits.

Usage

Multichassis PPP allows the use of Multilink PPP across multiple PortMaster products on the same Ethernet.

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 products on that hunt group, but any 12-digit hexadecimal number will serve.



Note – You must use the **save all** and **reboot** commands after issuing the **set endpoint** command for the end point discriminator to take effect.

Example

```
Command> set endpoint 00C005123456  
Endpoint Discriminator set to 00C005123456
```

See Also

reset V0 - page 12-5

set isdn switch

This command sets the switch type for ISDN connections to the PortMaster ISDN PRI ports.

```
set isdn-switch ni-2|dms-100|4ess|att-5ess
```

```
set isdn-switch net5|vn2|vn3|1tr6|ntt|kdd|ts014
```

ni-2	National ISDN-2 (NI-2) compliant. This is the default.
dms-100	Northern Telecom DMS-100.
4ess	AT&T 4ESS.
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.

Usage

The switch type information is available from your ISDN PRI telephone service provider. To activate any change you make to the switch type setting, you must first reboot the PortMaster.

Example

Command> **set isdn-switch att-5ess**
ISDN switch type set to ATT-5ESS

set Line0|line2 encoding

This command sets the encoding method used with T1 or E1 lines or the T1 expansion card.

set Line0|line2 encoding b8zs|ami|hdb3

3.8

<i>Line0</i>	line0 or line1 .
line2	T1 expansion card.
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.

Example

Command> **set line0 encoding b8zs**
line0 encoding successfully changed

set Line0|line2 framing

This command sets the framing format used for the E1 or T1 line or the T1 expansion card.

set Line0|line2 framing esf|d4|crc4|fas

Line0 **line0** or **line1**.

3.8

line2 T1 expansion card.

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.

Example

Command> **set line0 framing esf**
line0 framing successfully changed

set Line0|line2 group

This command allows you to set the channel rate for a group on a fractional T1 or E1 line or on a T1 expansion card to 56Kbps or 64Kbps.

set Line0|line2 group Cgroup 56k|64k

Line0 **line0** or **line1**.

3.8

line2 T1 expansion card.

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.

Usage

Before setting the channel rate, you must first set the line type to **fractional** with the **set Line0 fractional** command, and create channel groups with the **set Line0 group channels** command.

See Also

set Line0 fractional - page 12-11
set Line0 group channels - page 12-10

set Line0|line2 group channels

This command allows you to divide an ISDN PRI line, each of the T1 or E1 lines, or the T1 expansion card into groups that function as synchronous ports.

set Line0|line2 group Cgroup channels Channel-list



<i>Line0</i>	line0 or line1 .
line2	T1 expansion card.
<i>Cgroup</i>	Group number from 1 to 63 that designates a port number on each ISDN line, T1 or E1 line, or T1 card.
<i>Channel-list</i>	Space-separated list of one or more channel numbers, from 1 through 24 for T1, or 1 through 30 for E1. The channel numbers do not have to be contiguous.

Usage

To use channel groups, you must first set the line type to **fractional** or **isdn-fractional** with the **set Line0** command.

When set to **fractional**, the T1 expansion card supports only one line group, and the first line group found is used for configuration.

To remove a group number from a line, enter the command **set Line0 group** without any arguments.

Example

To allocate channels 1 through 4 of Line0 to group 2 to function as 256Kbps synchronous port 2, and to set the lines to a channel rate of 64Kbps, use the following commands:

```
Command> set line0 fractional
Command> set line0 group 2 channels 1 2 3 4
Command> set line0 group 2 64k
Command> save all
Command> reboot
```

Now configure the channel group 2 as you would any PortMaster synchronous port.

See Also

set Line0 fractional - page 12-11

set Line0 group 64k - page 12-9

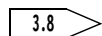
set Line0|line2

This command allows you to use a line as a single E1 or T1 line; as PRI B channels; as a fractional ISDN, E1, or T1 line divided into channel groups; or for inband signaling for channelized T1 and E1.



Note – T1 and E1 settings are mutually exclusive and are dependent on the PortMaster model.


set Line0 isdn|t1|e1|fractional|isdn-fractional|inband



set line2 t1|fractional

Line0 **line0** or **line1**.

line2 T1 expansion card.

isdn	Uses the line as PRI B channels. This is the default.
t1	Uses the entire line as a T1 line.
e1	Use the entire line as an E1 line.
 isdn-fractional	Divides an ISDN line into groups specified by the set Line0 line2 group command (see page 12-10).
fractional	Divides a T1 or E1 line into groups specified by the set Line0 line2 group command (see page 12-10).
inband	Sets the line for inband signaling, used for channelized T1 and E1. The signaling protocol for channelized T1 is specified by the set Line0 signaling command (see page 12-17). For channelized E1, use the set Line0 signaling mfr2 command (see page 12-18).

Usage

ComOS 3.8 and later releases support the use of the T1 expansion card *PM3-SYNC-T1* in any available modem slot of a PortMaster 3. Only one T1 card can be installed in a PortMaster 3, and any additional T1 card installed is ignored.

When the T1 expansion card is installed, a new port—W24 for a single PRI or W48 for two PRIs—is added to the list of active ports.

When set to **isdn**, Line2 defaults to T1 operation. When set to **fractional**, the T1 card supports only one line group and the first line group found is used for configuration.



Caution – If you configure a line for fractional T1 and reboot the PortMaster 3 before configuring the group and channels, you will no longer be able to access and configure the line. You must erase your entire configuration and reboot to access the line again.



Note – T1 and E1 lines require an external clock signal provided by the device that the PortMaster is connected to, or by the telephone company network.

Examples

Command> **set line1 isdn-fractional**
line1 changed to isdn-fractional T1

set Line0|line2 loopback

This command sets a T1 or E1 line for local network loopback.

3.8

set Line0|line2 loopback on|off

<i>Line0</i>	line0 or line1 .
line2	T1 expansion card.
on	Turns on local network loopback.
off	Turns off local network loopback.

Usage

This command is used for telephone line testing purposes.

Example

Command> **set line0 loopback on**
Loopback set ON for Line0

set Line0 nfas

This command sets non-facility associated signaling (NFAS) parameters for a T1 line.

 **set Line0 nfas pri|sec|sla|dis Identifier Group**

- | | |
|-------------------|--|
| <i>Line0</i> | line0 or line1 . |
| pri | Sets the primary D channel on <i>Line0</i> . |
| sec | Sets the backup D channel on <i>Line0</i> . |
| sla | Sets the line as a slave interface—all channels on the line are B channels. |
| dis | Disables NFAS on the interface. |
| <i>Identifier</i> | Identifier number—an integer between 0 and 19 that uniquely identifies a T1 interface in an NFAS group. |
| <i>Group</i> | Group number—a common number assigned to all the T1 lines belonging to the same NFAS group. <i>Group</i> is an integer between 1 and 99. |

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.



Caution – Setting multiple pairs of primary and backup D channels from different PortMaster 3s in the same group causes NFAS to stop working.

ComOS 3.9 implementation of NFAS allows up to 20 T1 interfaces to be grouped together to share a primary D channel and a backup D channel.

The two T1 interfaces of any single PortMaster 3 must belong to the same NFAS group. Once NFAS is enabled on a PortMaster 3, a T1 line can no longer run in the standard PRI configuration of 23 B channels plus one D channel. If only one T1 interface exists or is available, it can belong to an NFAS group by itself.

If the active D channel fails, the backup D channel is enabled, but the active calls on the lines serviced by the failed D channel are terminated. No calls are saved during the switch to the backup D channel.

NFAS is serviced by UDP port 1650.

For more information about configuring your PortMaster for NFAS, refer to the *PortMaster Configuration Guide*.

You must use the **save all** and **reboot** commands after using the command **set Line0 nfas** for the settings to take effect.

Examples

The following examples are from two PortMaster 3 units in the same NFAS group **4**. The first PortMaster 3 with T1 interface **0** is set with the primary D channel, and its second T1 interface **2** is set with the backup D channel.

The third PortMaster 3 with T1 interface **1** is set as a slave interface.

Command> **set line0 nfas pri 0 4**

New NFAS parameters will be effective after next reboot

Command> **set line1 nfas sec 2 4**

New NFAS parameters will be effective after next reboot

Command> **set line0 nfas sla 1 4**

New NFAS parameters will be effective after next reboot

See Also

set debug nfas on|off - page 19-13

show Line0 - page 12-23

show nfas - page 12-31

show nfas stat - page 12-34

set Line0 pcm

This command sets the method for compressing and expanding, or **companding**, digitized audio signals.

set Line0 pcm u-law|a-law

Line0 **line0** or **line1**.

u-law Default method of companding the amplitude of audio signals over T1 PRI lines.

a-law Default method of companding the amplitude of audio signals over E1 PRI lines.

Usage

This command is needed only when you are using digital modems in the PortMaster 3. The default settings must not be changed unless your PRI service provider instructs you otherwise.

3.8

ComOS 3.8 and later releases support the V.90 modem protocol for Lucent and 3Com chipsets for dial-in modems on T1 PRI lines.

Example

```
Command> set line0 pcm u-law
line0 PCM encoding changed to u-law
```

set Line0 signaling

This command sets the inband signaling protocol and the inband call options used with channelized T1.

set Line0 signaling wink|immediate|fxs

<i>Line0</i>	line0 or line1 .
wink	E & M wink start protocol, an option for use with channelized T1 lines. This is the default.
immediate	E & M immediate start protocol.
fxs	Foreign exchange station (FXS) loop start protocol.



Note – You must first set the line to inband signaling using the command **set Line0 inband** before using the command **set Line0 signaling**.

Example

```
Command> set line0 signaling wink  
line0 changed to inband signaling wink
```

See Also

set Line0 inband - page 12-11

set Line0 signaling r2generic|mfr2

This command sets inband signaling to multifrequency R2 signaling (MFR2) for a channelized E1 line.



set Line0 signaling r2generic|mfr2 Profile

<i>Line0</i>	line0 or line1 .
r2generic	Generic R2, the default when Line0 is set for inband signaling. Sets inband signaling to MFR2 but without tone signaling.
mfr2 Profile	One of the following channelized E1 inband signaling profiles: <ul style="list-style-type: none"> 0 ITU-T standard: Argentina and other countries. 1 Mexico. 2 Brazil and Tunisia. 3 Venezuela. 4 Mexico. Profile 4 is a subset of profile 1 and is used with switches that do not support caller ID. This profile can be used in Mexico wherever profile 1 is used, but the reverse is not true.

Usage

A number profile can apply to different countries, and a country can have more than one MFR2 profile available.

MFR2 signaling is supported by ComOS 3.8 and later releases for incoming calls on E1 lines and requires the use of Lucent True Digital K56flex modem cards.

Use the **show line0** command to display the type of inband signaling used and the MFR2 profile selected.

For more information on configuring MFR2 signaling, refer to the *PortMaster Configuration Guide*.



Note – You must first set the line to inband signaling using the command **set Line0 inband** before setting the line to MFR2 signaling.

Examples

Command> **set line0 signaling mfr2 0**
line0 changed to inband signaling, MFR2

Command> **set line1 signaling r2gen**
line1 changed to inband signaling, R2MF generic

See Also

set Line0 inband - page 12-11
show Line0 - page 12-23

set Line0|line2 clock

This command sets the source for the clock signal for the T1 expansion card.



set Line0|line2 clock internal|external

<i>Line0</i>	line0 or line1 .
line2	T1 expansion card.
internal	Selects the built-in 1.544Mhz crystal to drive the line. This setting is used for dry wire configurations or back-to-back connections.
external	Built-in channel service unit/digital service unit(CSU/DSU) extracts the clock signal from the line. This is the default.

Examples

Command> **set line2 clock external**
line2 clocking changed to external
Command> **set line2 clock internal**
line2 clocking changed to internal

See Also

set Line0|line2 - page 12-11

set location analog

This command sets the digital modems of a PortMaster 3 to analog modem service when dialing out to the specified location.

set location *Locname* **analog on|off**

<i>Locname</i>	Location name that is in the location table.
on	Enables analog modem service on dial-out.
off	Disables analog modem service on dial-out, and causes the service to revert to ISDN.

Usage

Use this command when analog rather than digital modem service is required for dial-out network connections.

Example

Command> **set location hq analog on**
hq voice dial changed from off to on

set M0

This command makes the digital modems on the PortMaster 3 available or unavailable.

set M0 on|off

<i>M0</i>	Any digital 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.

Usage

The digital modems on the PortMaster 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.

Any user on a modem that is busied is disconnected.



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

Example

```
Command> set m0 off
Modem M0 changed from on to off
```

See Also

set location analog - page 12-20

set M0 lastcall

This command forces an active modem into ADMIN mode as soon as a user logs off.

set M0 lastcall

M0 Any digital modem number from **m0** to **m59**. Changes to the default setting must be made to individual modems.

Usage

ComOS 3.7.2c and later releases support this command to enable you to hot-swap a modem card without disconnecting a user.

To return the modem to its normal operation, reboot or use the command **set M0 on**.

The modem status displayed by the **show M0** and **show modems** commands is ACT(LC) instead of ACTIVE, to show that the modem status is Active (Last Call).



Note – When circuits are available to the PortMaster but no modems are available, the PortMaster replies to another incoming call with a user busy signal to the telephone company, giving the user a busy signal, instead of forwarding the call to the next line in the hunt group. To remedy this situation, the telephone company might be able to configure the line for “forward when busy” to prevent this behavior.

Example

```
Command> set m20 lastcall
Modem M20 changed from on to lastcall
```

See Also

set line2 t1 - page 12-11
set M0 on|off - page 12-20
show M0 - page 12-27

set S0 directory

This command sets a telephone number for an individual port when the line is configured as ISDN B channels.

set S0 directory *Number*

<i>S0</i>	One of the ISDN ports.
<i>Number</i>	Access telephone number.

Usage

Normally a PRI line has a single telephone number. However, when the line is set up as ISDN B channels, this optional command can be used to set a telephone number for an individual port. If set, it allows you to identify the circuit telephone number associated with a specific ISDN port.

3.8

BACP and BAP Supports. ComOS 3.8 and later releases support the Bandwidth Allocation Control Protocol (BACP), according to RFC 2125. Because BACP and the Bandwidth Allocation Protocol (BAP) are both negotiated protocols, no commands are necessary to turn them on. The only requirement for the use of BAP and BACP is setting directory numbers on the serial ports so the PortMaster can offer a second number to the client dialing in.

BACP supports local exchange telephone numbers. If a long-distance BACP user is configured to dial a local exchange telephone number, the PortMaster checks the Called-Station-Id when the second channel is requested. To implement this configuration, do not set the directory numbers.

Example

```
Command> set s0 directory 5105551212  
Directory No for port S0 changed from      to 5105551212
```

show Line0

This command shows the status of an E1 or T1 line on a PortMaster 3.

```
show Line0|line2
```

<i>Line0</i>	line0 or line1 .
line2	T1 expansion card.

E1 Example

Line1 is configured as a PRI ISDN line.

```
Command> show line1
----- line1 - E1 Primary Rate ISDN -----
Status: DOWN F3      Framing: FAS      Encoding: HDB3      PCM: a-law
Violations
-----
Bipolar              1209159
CRC4                  0
E-bit                 0
FAS
```

T1 Examples

Line0 is configured as a PRI ISDN line.

```
Command> show line0
----- line0 - T1 Primary Rate ISDN -----
Status: UP           Framing: ESF      Encoding: B8ZS      PCM: u-law
Receive Level:       +2dB to -7.5dB
Alarms
-----
Blue                  0
Yellow                0
Receive Carrier Loss  0
Loss of Sync          0
Bipolar              102
CRC Errors            1
Multiframe Sync       9
```

Line0 is configured for inband signaling—channelized T1.

```
Command> show line0
----- line0 - T1 Inband DS0 -----
Status: UP           Framing: ESF      Encoding: B8ZS      PCM: u-law
Signaling: Trunk E&M wink start      Options: inbound calls only
Receive Level:       +2dB to -7.5dB
Alarms
-----
Violations
```

Blue	0	Bipolar	5
Yellow	0	CRC Errors	0
Receive Carrier Loss	0	Multiframe Sync	2
Loss of Sync	0		

ISDN Example

Line0 is configured as a fractional ISDN line with one group of seven channels.

```
Command> show line0
----- line0 - T1 ISDN-Fractional -----
Status: UP           Framing: ESF      Encoding: B8ZS      PCM: u-law
Channel
Group              Speed              Channels
-----
1                  ISDN              1 2 3 4 5 6 7
Receive Level:      +2dB to -7.5dB
Alarms              Violations
-----
Blue                0                Bipolar           0
Yellow              0                CRC Errors        0
Receive Carrier Loss 0                Multiframe Sync   0
Loss of Sync         0
```

Explanation

Status	Status of T1, E1, or ISDN line.
F State—E1 only (F3 in example)	PRI Layer 1 state at the user side of the interface. Range: F0 to F6.
	F0—Power off, no signal.
	F1—Operational.
	F2 to F5—Failure conditions FC1 to FC4.
	F6—Power on, no signal.

Framing	Framing format in use.	See page 12-9.
Encoding	Encoding method in use.	See page 12-8.
PCM	Pulse code modulation method in use.	See page 12-16.
Channel Group	Channel number.	See page 12-10
Speed	Connect speed.	
Channels	Channel list numbers.	See page 12-10.
Signaling	Type of inband signaling in use.	See page 12-17 and page 12-18.
Options	Inband signaling options in use.	
Receive Level	Signal strength on the line.	
E1 Alarms	Remote Alarm—Remote is in alarm state.	
	Receive Carrier Loss—Loss of carrier signal.	
	Loss of Sync—Device loss of synchronization signal.	
	Loss of Sync—Device loss of synchronization signal.	
T1 and ISDN Alarms	Blue—Unframed all ones (1s) signal.	
	Yellow—D4 bit2, D4 12th F-bit, or extended superframe (ESF) mode (framing) signal.	
	Receive Carrier Loss—Loss of carrier signal.	
	Loss of Sync—Device loss of synchronization signal.	
E1 Violations	Bipolar—Consecutive bipolar violations of same polarity.	
	CRC4—Errors in the CRC4 code words (CRC4 framing).	
	E-bit—CRC4 error bits.	
	FAS bit—Errors in the frame alignment signal (FAS) code words (FAS framing).	
T1 Violations	Bipolar—Consecutive bipolar violations of the same polarity.	
	CRC Errors—Errors in CRC6 code words (ESF framing), or in the Ft framing bit position (D4 framing).	
	Multiframe Sync—Multiframes received out of synchronization.	

show M0

This command shows the status of a digital modem on a PortMaster 3.

show M0

M0 Digital modem number from **m0** to **m59**.

Example

```
Command> show m0
State                ACTIVE
Active Port          S2
Transmit Rate        28800
Receive Rate         28800
Connection Type      LAPM/V42BIS
Chars Sent           19001366
Chars Received       3177827
Retrains             0
Renegotiations       3
Total Calls          63
Modem Detects        58
Good Connects        56
Connection Failures
No Modulation        1
No Protocol          1
Total Failed         2
Session Terminations
Lost Carrier         0
Normal Disconnect    56
```

Explanation

State	Modem status—one of the following:	
	ACTIVE	The modem is in use.
	ACT(LC)	The modem is in use but will go into ADMIN mode as soon as user logs off.
	READY	The modem is available for use.
	ADMIN	The modem has been busied out.
	TEST	The modem is under test.
	DOWN	The modem is not available.
Active Port	Digital modem port assignment.	
Transmit Rate	Modem transmission speed in bits per second.	
Receive Rate	Modem reception speed in bits per second.	
Connection Type	Data link-layer protocol/compression standard used.	
	The following status information is measured since the PortMaster was last rebooted:	
Chars Sent	Number of characters transmitted.	
Chars Received	Number of characters received.	
Retrains	Number of times the modem changed speed (retrained) due to a change in line quality since the last reboot.	
Renegotiations	Number of modem handshake renegotiation events.	
Total Calls	Total calls attempted.	
Modem Detects	Total calls in which a remote modem was detected.	
Good Connects	Number of detected calls that made valid connections.	
Connection Failures	Reason and number of modem connection failures, as follows:	
	No Modulation:	No signal modulation detected.
	No Protocol:	No link-layer protocol detected.
	Total Failed:	Total failed connections.
Session Terminations	Reason and number of modem session terminations, as follows:	

Lost Carrier: DCD was lost, with consequent session termination.

Normal Disconnect: Normal session termination.

show mcppp

This command displays the addresses of the neighboring PortMaster devices in the same Multichassis PPP group, and a list of connections to virtual and physical ports on the PortMaster.

show mcppp

Example

Command> **show mcppp**

Neighbors:

pm3-02-e0 (172.16.137.14)pm3-03-e0 (172.16.137.12)

pm3-01-e0 (172.16.137.11)

Port	User	Host/Inet/Dest	Type	Peer
----	-----	-----	-----	-----
S11	misha	192.168.96.2	SLAVE	pm3-02-e0
S39	neil	172.16.200.4	SLAVE	pm3-03-e0
V0	bsmith	192.168.200.1	VIRTUAL	pm3-01-e0

Explanation

Port	Physical port number (for example S11) used as a slave port for a Multichassis PPP connection, or a virtual port number (for example, V0) established to complete a Multichassis PPP connection with another PortMaster in the same Multichassis PPP group.
User	Username of the user logged in to the port.
Host/Inet/Dest	Hostname, or IP address of login user.
Type	Port type, as follows: SLAVE Physical port used as a slave for a corresponding virtual port on another PortMaster in the same Multichassis PPP group. VIRTUAL Virtual port created for a corresponding physical port on another PortMaster in the same Multichassis PPP group.
Peer	Name or IP address of the PortMaster in the same Multichassis PPP group that is connected to the login user via a corresponding physical or virtual port.

show modems

Shows the status of the digital modems on a PortMaster 3.

show modems

Example

Command> show modems								
Mdm	Port	Status	Speed	Compression	Protocol	Calls	Retrain	Disconnect
----	----	-----	-----	-----	-----	-----	-----	-----
M0	S2	ACTIVE	28800	V42BIS	LAPM	12	0	NORMAL
M1	S3	ACTIVE	28800	V42BIS	LAPM	5	0	NORMAL
M2	S4	ACTIVE	28800	V42BIS	LAPM	7	0	NORMAL
M3	S11	READY	UNKWN	NONE	NONE	0	0	NORMAL

Explanation

Mdm	Digital modem number.	
Port	PortMaster port assignment.	
Status	ACTIVE	The modem is in use.
	INITALIZE	The modem is in transition state—modem has just been reseated.
	READY	The modem is available for use.
	ADMIN	The modem has been busied out.
	TEST	The modem is under test.
	DOWN	The modem is not available.
Speed	The connect speed in bits per second.	
Compression	Compression standard used.	
Protocol	Data-link layer protocol used.	
Calls	Number of calls since the last PortMaster reboot.	
Retrain	Number of times the modem changes speed (retrains) due to a change in line quality since the last PortMaster reboot.	
Disconnect	Type of modem disconnection, normal or lost carrier.	

show nfas

This command displays NFAS information for this PortMaster and neighboring PortMaster products in the same NFAS group.



show nfas

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Example

```
Command> show nfas
NFAS GROUP 4

Neighbor          line0 ifc    line1 ifc    line0 state  line1 state
-----
149.198.96.70     X           2(SEC)       STANDBY
149.198.96.68     1(SLA)      X
This chassis      0(PRI)      X           IN-SERVICE
```

Explanation

Neighbor	IP address of a PortMaster in an NFAS group.
line0 ifc or line1 ifc	Interface number of the T1 line and the type: PRI Line set with the primary D channel servicing all interfaces in the NFAS group. SEC Line set with the backup D channel interface. SLA Slave interface.
line0 state or line1 state	Displays status of the D channels.

See Also

set Line0 nfas - page 12-14
show nfas stat - page 12-34

show nfas history

This command shows the last 40 messages exchanged between this PortMaster and other PortMaster products in the same NFAS group.

3.9

show nfas history

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command can be used to diagnose Multichassis PPP problems.

Example

Command> **show nfas history**

```
SND: 95c66045 4 53 PKG 5 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 9
RCV: 95c66045 4 32 PKG 10 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 10
RCV: 95c66045 4 127 PKG 11 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 6 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 11
RCV: 95c66045 4 32 PKG 12 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 12
RCV: 95c66045 4 127 PKG 13 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 7 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 13
RCV: 95c66045 4 32 PKG 14 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 14
RCV: 95c66045 4 127 PKG 15 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 8 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 15
RCV: 95c66045 4 32 PKG 16 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 16
```

```

RCV: 95c66045 4 127 PKG 17 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 9 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 17
RCV: 95c66045 4 32 PKG 18 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 18
RCV: 95c66045 4 127 PKG 19 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 10 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 19
RCV: 95c66045 4 32 PKG 20 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 20
RCV: 95c66045 4 127 PKG 21 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 11 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 21
RCV: 95c66045 4 32 PKG 22 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 22
RCV: 95c66045 4 127 PKG 23 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 53 PKG 12 0 2 1 0 -1 2 - 1280 1024 19793 45
SND: 95c66045 4 127 ACK 23
SND: 95c66045 4 53 PKG 12 0 2 1 0 -1 2 - 1280 1024 19793 45
RCV: 95c66045 4 32 PKG 24 0 2 1 0 0 -1 - 1024 1280 19793 45
SND: 95c66045 4 32 ACK 24

```

show nfas stat

This command displays the status of calls in an NFAS group.

3.9

show nfas stat

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command can be used to diagnose connection problems in an NFAS group.

This command is useful when comparing the output from the PortMaster 3 with the active D channel against the output from the PortMaster 3 receiving the call.

Examples

On the PortMaster with the active D channel:

Command> **show nfas stat**

XMT_DROP RCV_DROP

 0 0

Reference Table:

ADDR/DSL	ID	IFC	F	ADDR/DSL	ID	IFC	F
-----	---	---	-	-----	----	---	-
C0c66046	1d8f	2	1				
C0c66046	1d8e	2	1				
1	27	1	1	1	812e	1	1
1	26	1	1	1	25	1	1
1	812c	1	1	1	24	1	1
1	812b	1	1	1	23	1	1
1	8129	1	1	1	22	1	1
1	8127	1	1	1	21	1	1
1	8124	1	1	1	20	1	1
1	8123	1	1	1	1f	1	1
1	8120	1	1	1	1e	1	1
1	811f	1	1	1	1d	1	1
1	811d	1	1	1	1c	1	1
1	811b	1	1	1	1b	1	1
95c66046	1a	2	1	1	8119	1	1
95c66046	19	2	1	95c66046	18	2	1
95c66046	17	2	1	95c66046	16	2	1
95c66046	15	2	1	95c66046	14	2	1
95c66046	13	2	1	95c66046	12	2	1
95c66046	11	2	1	95c66046	10	2	1
95c66046	f	2	1	95c66046	e	2	1

95c66046	d	2	1	95c66046	c	2	1
95c66046	b	2	1	95c66046	a	2	1
95c66046	9	2	1	95c66046	8	2	1
95c66046	7	2	1	95c66046	6	2	1
95c66046	5	2	1	95c66046	4	2	1

On the PortMaster in the NFAS group receiving the call:

Command> **show nfas stat**

XMT_DROP RCV_DROP

 0 0

Reference Table:

ADDR/DSL	ID	IFC	F	ADDR/DSL	ID	IFC	F
-----	---	---	-	-----	----	---	-
0	1a	2	1	0	19	2	1
0	18	2	1	0	17	2	1
0	16	2	1	0	15	2	1
0	14	2	1	0	13	2	1
0	12	2	1	0	11	2	1
0	10	2	1	0	f	2	1
0	e	2	1	0	d	2	1
0	c	2	1	0	b	2	1
0	a	2	1	0	9	2	1
0	8	2	1	0	7	2	1
0	6	2	1	0	5	2	1
0	4	2	1				

Explanation

ADDR/DSL	One of the following: <ul style="list-style-type: none">• IP address in hexadecimal notation—when this command is used on the PortMaster 3 with the active D channel.• Digital signaling line—0 or 1—when this command is used on the PortMaster 3 receiving the call.
ID	Message ID number.
IFC	Interface number.
F	Flag—status of the call. <ol style="list-style-type: none">1 Active—active call.2 Transition—call has been terminated and the identification number will be deleted in the next few seconds.3 Deleting—message identification number is deleted.

This chapter describes how to use the command line interface to create, edit, and delete filters. Detailed command definitions follow a command summary table.

System administrators can use the command line interface to create appropriate packet filters to control access to specific hosts, networks, and network services.

Once a filter is defined, it can be used with the **ptrace** command or attached to an Ethernet interface, network hardwired port, user, or location. If used for route propagation, the filter is assigned to a specified protocol. Filters for network hardwired ports and Ethernet interfaces are set for the port or interface. Filters for dial-in users are set in the user table, or can be referred to by RADIUS. Filters for dial-out locations are set in the location table.

For more information about designing packet filters, refer to the *PortMaster Configuration Guide*.

Displaying Filter Information

To display information about your filters, use the following filter-specific commands:

- **show table filter**
- **show filter**
- **ifconfig**—see page 2-9



Note – Filter names have a maximum of 15 characters. If longer names are used, they are truncated to 15 characters.

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of Filter Commands

The commands in Table 13-1 configure the filter table. Filters can be applied to Ethernet interfaces, users, locations, network hardwired ports, protocols, or security profiles and can be used for debugging with the **ptrace** command.



Note – Enter each command on one line, without any breaks. Line breaks shown here are due to the limited space available.

Table 13-1 Filter Table Configuration

Command Syntax	
add filter <i>Filtername</i>	- see page 13-4
delete filter <i>Filtername</i>	- see page 13-4
save filter	- see page 13-5
set filter <i>Filtername</i> blank	- see page 13-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM Ipaddress(dest)/NM</i>] [esp ah ipip ospf] [log] [notify]	- see page 13-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM Ipaddress(dest)/NM</i>] [protocol <i>Number</i>] [log] [notify]	- see page 13-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>=ListName Ipaddress(dest)/NM</i> [esp ah ipip ospf] [log] [notify]	- see page 13-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>=ListName Ipaddress(dest)/NM</i> [protocol <i>Number</i>] [log] [notify]	- see page 13-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM =ListName</i> [esp ah ipip ospf] [log] [notify]	- see page 13-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM =ListName</i> [protocol <i>Number</i>] [log] [notify]	- see page 13-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM Ipaddress(dest)/NM</i>] tcp [src eq lt gt <i>Tport</i>] [dst eq lt gt <i>Tport</i>] [established] [log] [notify]	- see page 13-10

Table 13-1 Filter Table Configuration (Continued)

Command Syntax	
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny = <i>ListName</i> <i>Ipaddress(dest)/NM</i> tcp [src eq lt gt <i>Tport</i>] [dst eq lt gt <i>Tport</i>] [established] [log] [notify]	- see page 13-10
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM</i> = <i>ListName</i> tcp [src eq lt gt <i>Tport</i>] [dst eq lt gt <i>Tport</i>] [established] [log] [notify]	- see page 13-10
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress(dest)/NM</i>] udp [src eq lt gt <i>Uport</i>] [dst eq lt gt <i>Uport</i>] [log] [notify]	- see page 13-13
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny = <i>ListName</i> <i>Ipaddress(dest)/NM</i> udp [src eq lt gt <i>Uport</i>] [dst eq lt gt <i>Uport</i>] [log] [notify]	- see page 13-13
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM</i> = <i>ListName</i> udp [src eq lt gt <i>Uport</i>] [dst eq lt gt <i>Uport</i>] [log] [notify]	- see page 13-13
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress(dest)/NM</i>] icmp [type <i>Itype</i>] [log] [notify]	- see page 13-16
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny = <i>ListName</i> <i>Ipaddress(dest)/NM</i> icmp [type <i>Itype</i>] [log] [notify]	- see page 13-16
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM</i> = <i>ListName</i> icmp [type <i>Itype</i>] [log] [notify]	- see page 13-16
set ipxfilter <i>Filtername</i> <i>RuleNumber</i> permit deny [srcnet <i>Ipxnetwork</i>] [srchost <i>Ipxnode</i>] [srcsocket eq gt lt <i>Ipxsock</i>] [dstnet <i>Ipxnetwork</i>] [dsthost <i>Ipxnode</i>] [dstsocket eq gt lt <i>Ipxsock</i>]	- see page 13-19
set sapfilter <i>Filtername</i> <i>RuleNumber</i> permit deny [server <i>String</i>] [network <i>Ipxnetwork</i>] [host <i>Ipxnode</i>] [socket eq gt lt <i>Ipxsock</i>]	- see page 13-22
show filter ipxfilter sapfilter <i>Filtername</i>	- see page 13-24
show table filter	- see page 13-25

Filter Commands

The following commands create, delete, and modify, and display filters.



Note – If a filter rule is set with no arguments, the rule is removed. If a filter rule is set with arguments without specifying **permit** or **deny**, **permit** is chosen by default.

add filter

This command creates a new filter name and adds it to the filter table.

add filter *Filtername*

Filtername Name for a filter—up to 15 characters.

Usage

If the filter is to be used by RADIUS, it must end in **.in** if it is an input filter and **.out** if it is an output filter. Consider using the same convention to distinguish all input and output filters.

Example

```
Command> add filter s1.in  
New Filter successfully added
```

delete filter

This command deletes an existing filter from the filter table.

delete filter *Filtername*

Filtername Name of a filter in the filter table.

Usage

Use caution when removing filters from the filter table. Make sure that they are no longer needed for any packet filtering.

Example

Command> **delete filter s1.in**

ComOS provides no automatic response to this command, but you can use the **show table filter** command to confirm that the filter has been removed from the filter table.

See Also

add filter - page 13-4

set filter blank - page 13-6

show table filter - page 13-25

save filter

This command saves any changes in the filter table to the nonvolatile RAM of the PortMaster.

save filter

Usage

The **save all** command can also be used.

Example

Command> **save filter**

Filter table successfully saved

New configurations successfully saved.

set filter blank

This command empties the contents of a filter.

set filter *Filtername* **blank**

Filtername Name of a filter in the filter table.

blank Removes all the rules from a filter.

Example

Command> **set filter test blank**

See Also

delete filter - page 13-4

set filter (IP)

These commands configure a filter that controls passage of an IP packet through an interface.



Note – Enter each command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
set filter Filtername RuleNumber permit|deny  
[Ipaddress/NM Ipaddress(dest)/NM] [esp|ah|ipip|ospf] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny  
[Ipaddress/NM Ipaddress(dest)/NM] [protocol Number] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny  
=ListName Ipaddress(dest)/NM [esp|ah|ospf] [log] [notify]
```



```
set filter Filtername RuleNumber permit|deny  
=ListName Ipaddress(dest)/NM [protocol Number] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny  
Ipaddress/NM =ListName [esp|ah|ipip] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny  
Ipaddress/NM =ListName [protocol Number] [log] [notify]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits a packet that matches the filter to pass through the interface. This is the default.
deny	Stops a packet that matches the filter from passing through the interface. The packet is dropped, and an ICMP “Host Unreachable” message is sent to the source address.
<i>Ipaddress</i>	IP address expressed in dotted decimal notation or as a hostname of up to 39 characters, to compare with the source IP address of the packet.
<i>/NM</i>	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are /0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
<i>Ipaddress(dest)</i>	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.

esp	Matches packets using the Encapsulating Security Payload (ESP) protocol. See RFC 1827 for more information on this protocol.
ah	Matches packets using the 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.
ospf	Matches packets using OSPF protocol.
log	Packets matching the rule are logged by syslog to the loghost.
notify	Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword causes a notification pop-up to appear on your computer.
protocol <i>Number</i>	Matches packets using the specified Internet Protocol. <i>Number</i> is a specified protocol number, as listed in RFC 1700, <i>Assigned Numbers</i> .
=ListName	Specifies a list of sites in the /etc/choicenet/lists directory on the ChoiceNet server. The equal sign (=) must immediately precede the value.

Usage

You construct filters by first creating the filter using the command **add filter**, and then adding rules to permit or deny packets that match the criteria in the rules. You can update an existing filter by setting additional rules with new rule numbers and new filter criteria, or you can edit the existing rules.

You can delete a rule by specifying only the rule number—for example **set filter s0.in 4**. You cannot use the command line interface to insert a rule between other rules, although you can do so with the PMVision GUI and the FilterEditor application.

Zero-length filters are treated as permit filters. That is, if a filter has no rules at all it permits everything through. If a filter has one or more rules, anything not explicitly permitted by a rule is denied at the end of the filter.



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

Example

The following example denies any incoming IP packet to the subnet 192.168.1.0/24 from the Internet claiming to be from—or spoofing—your own network (192.168.1.0), preventing spoofing attacks. This rule also logs the header information in the spoofing packets to **syslog**.

```
Command> set filter w1.in 1 deny 192.168.1.0/24 0.0.0.0/0 log
Filter w1.in updated
```

See Also

add filter - page 13-4
set choicenets - page 3-33
set loghost - page 3-11

set filter (TCP)

These commands set filtering rules for TCP packets.



Note – Enter each command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
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]
```

```
set filter Filtername RuleNumber permit|deny
=ListName Ipaddress(dest)/NM tcp [src eq|lt|gt Tport]
[dst eq|lt|gt Tport] [established] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny
Ipaddress/NM =ListName tcp [src eq|lt|gt Tport]
[dst eq|lt|gt Tport] [established] [log] [notify]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits a packet that matches the filter to pass through the interface. This is the default.
deny	Stops a packet that matches the filter from passing through the interface. The packet is dropped, and an ICMP “Host Unreachable” message is sent to the source address.
<i>Ipaddress</i>	IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the source IP address of the packet.

<i>/NM</i>	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are /0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
<i>Ipaddress(dest)</i>	An IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the destination IP address of the packet.
src	Specifies that the packet source port number be tested; see “Usage” for test criteria.
eq, lt, or gt	Mode of comparison of port numbers; equal to (eq), less than (lt), or greater than (gt).
<i>Tport</i>	Number of the designated TCP port. See Table D, “TCP and UDP Ports and Services,” on page D-1 for a list of the port numbers 20 through 1701 commonly assigned to TCP and UDP services.
dst	Specifies that the packet destination port number be tested; see “Usage” for test criteria.
established	Accepts only packets being sent to an established TCP network connection, and denies packets sent to establish new TCP connections.
log	Packets matching the rule are logged by syslog to the loghost.
notify	Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword causes a notification pop-up to appear on your computer.
<i>=ListName</i>	Specifies a list of source or destination sites in the /etc/choicenet/lists directory on the ChoiceNet server. The equal sign (=) must immediately precede the value.

Usage

The filtering rules are based on source and destination port numbers, and the established state of a connection.

The order of rules in a filter is important because the PortMaster evaluates the rules in the order that they are numbered. Refer to the *PortMaster Configuration Guide* for more information.

The **src** and **dst** keywords allow you to test the source or destination port number in the packet to determine whether it does the following:

- | | |
|---------------------|--|
| [src dst eq] | Equals the port number in the filter. |
| [src dst gt] | Is greater than the port number in the filter. |
| [src dst lt] | Is less than the port number in the filter. |



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

Examples

```
Command> set filter w1.in 1 deny 192.168.1.0/24 0.0.0.0./0 log
Filter w1.in updated
```

```
Command> set filter w1.in 2 permit tcp estab
Filter w1.in updated
```

```
Command> set filter w1.in 3 permit tcp dst eq 80
Filter w1.in updated
```

```
Command> set filter w1.in 4 permit tcp dst eq 25
Filter w1.in updated
```

At any point, you can see the updates made to the filter by using the following command (shown with response):

```
Command> show filter w1.in
1 deny 192.168.1.0/24 0.0.0.0/0 ip log
2 permit 0.0.0.0/0 0.0.0.0/0 tcp estab
3 permit 0.0.0.0/0 0.0.0.0/0 tcp dst eq 80
4 permit 0.0.0.0/0 0.0.0.0/0 tcp dst eq 25
```

See Also

add filter - page 13-4
set loghost - page 3-11

set filter (UDP)

These commands set filtering rules for User Datagram Protocol (UDP) packets.



Note – Enter each command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress(dest)/NM] udp [src eq|lt|gt Uport]
[dst eq|lt|gt Uport] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny
=ListName Ipaddress(dest)/NM udp [src eq|lt|gt Uport]
[dst eq|lt|gt Uport] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny
Ipaddress/NM =ListName udp [src eq|lt|gt Uport]
[dst eq|lt|gt Uport] [log] [notify]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits a packet that matches the filter to pass through the interface. This is the default.

deny	Stops a packet that matches the filter from passing through the interface. The packet is dropped, and an ICMP “Host Unreachable” message is sent to the source address.
<i>Ipaddress</i>	IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the source IP address of the packet.
<i>/NM</i>	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are /0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
<i>Ipaddress(dest)</i>	IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the destination IP address of the packet.
src	Specifies that the packet source port number be tested; see “Usage” for test criteria.
eq, lt, or gt	Mode of comparison of port numbers; equal (eq), less than (lt), or greater than (gt).
<i>Uport</i>	Designated UDP port. See Table D, “TCP and UDP Ports and Services,” on page D-1 for a list of the port numbers 20 through 1701 commonly assigned to TCP and UDP services.
dst	Specifies that the packet destination UDP port number be tested; see “Usage” for test criteria.
log	Packets matching the rule are logged by syslog to the loghost.
notify	Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword causes a notification pop-up to appear on your computer.

=ListName Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory on the ChoiceNet server. The equal sign (=) must immediately precede the value.

Usage

The filtering rules are very similar to those used for TCP packets, except that there is no **established** keyword for UDP. The order of rules in a filter is important because the PortMaster evaluates the rules in the order that they are numbered. Refer to the *PortMaster Configuration Guide* for more information.

The **src** and **dst** keywords allow you to test the source or destination port number in the packet to determine whether it does the following:

- [src|dst eq]** Equals the port number in the filter.
- [src|dst gt]** Is greater than the port number in the filter.
- [src|dst lt]** Is less than the port number in the filter.



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

Examples

The following rule permits UDP packets from port 53—DNS replies—into your network.

```
Command> set filter w1.in 5 permit udp src eq 53
Filter w1.in updated
```

The following rule permits UDP packets destined for port 53—allowing DNS requests to leave your network.

```
Command> set filter w1.in 6 permit udp dst eq 53
Filter w1.in updated
```

See Also

add filter - page 13-4
set loghost - page 3-11

set filter (ICMP)

These commands set filtering rules for Internet Control Message Protocol (ICMP) packets.



Note – Enter each command on one line, without any breaks. The line breaks shown here are due to the limited space available.



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

```
set filter Filtername RuleNumber permit|deny
[Ipaddress/NM Ipaddress(dest)/NM] icmp [type Itype] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny
=ListName Ipaddress(dest)/NM icmp [type Itype] [log] [notify]
```

```
set filter Filtername RuleNumber permit|deny
Ipaddress/NM =ListName icmp [type Itype] [log] [notify]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits a packet that matches the filter to pass through the interface. This is the default.
deny	Stops the packet from passing through the interface. The packet is dropped, and an ICMP “Host Unreachable” message is sent to the source address.
<i>Ipaddress</i>	IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the source IP address of the packet.

/NM Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are

/0—To match all packets with any address.

/16—Looks at high-order 16 bits of the address.

/24—Looks at high-order 24 bits of the address.

/32—Looks at the entire IP address.

Ipaddress(dest) IP address expressed in dotted decimal notation or as a hostname, up to 39 characters, to compare with the destination IP address of the packet.

type Itype ICMP message type to compare against the ICMP message type contained in the packet. ICMP message types are defined in RFC 1700, *Assigned Numbers*. Common ICMP types are the following:

- 0** Echo Reply
- 3** Destination Unreachable
- 4** Source Quench
- 5** Redirect
- 6** Alternate Host Address
- 8** Echo
- 9** Router Advertisement
- 10** Router Selection
- 11** Time Exceeded
- 12** Parameter Problem
- 13** Timestamp
- 14** Timestamp Reply
- 15** Information Request

16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reserved (for Security)
30	Traceroute
31	Datagram Conversion Error
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
log	Packets matching the rule are logged by syslog to the loghost.
notify	Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword causes a notification pop-up to appear on your computer.
=ListName	Specifies a list of source or destination sites in the /etc/choicenet/lists directory on the ChoiceNet server. The equal sign (=) must immediately precede the value.

Example

The following rule permits incoming ICMP packets.

```
Command> set filter w1.in 1 permit icmp
Filter w1.in updated
```

See Also

add filter - page 13-4
set loghost - page 3-11

set ipxfilter

This command sets filtering rules for IPX packets.



Note – Enter this command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
set ipxfilter Filtername RuleNumber permit|deny
[srcnet Ipxnetwork] [srchost Ipxnode] [srcsocket eq|gt|lt Ipxsock]
[dstnet Ipxnetwork] [dsthost Ipxnode] [dstsocket eq|gt|lt Ipxsock]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits a packet that matches the filter to pass through the interface. This is the default.
deny	Stops a packet that matches the filter from passing through the interface.
srcnet	Specifies the comparison with the source IPX network number contained in the packet, a 32-bit hexadecimal value.
<i>Ipxnetwork</i>	IPX network number, a 32-bit hexadecimal value.
srchost	Specifies the comparison with the source IPX node address contained in the packet, a 48-bit hexadecimal value—usually the MAC address of the host.
<i>Ipxnode</i>	IPX node address, a 48-bit hexadecimal value—usually the MAC address of the host.
srcsocket	Specifies that the source IPX socket number contained in the packet must be compared with the IPX socket number specified in the filter. A second keyword— eq , lt , or gt —must be used to indicate the mode of comparison, an integer from 0 to 65535.

eq, lt, or gt	Mode of comparison of socket numbers; equal (eq), less than (lt), or greater than (gt).
<i>Ipxsock</i>	A socket number specified for the comparison, an integer from 1 to 65535.
dstnet	Specifies the comparison with the destination IPX network number contained in the packet. A 32-bit hexadecimal number.
dsthost	Specifies the comparison with the destination IPX node address contained in the packet. A 32-bit hexadecimal number.
dstsocket	Specifies that the destination IPX socket number contained in the packet must be compared with the IPX socket number specified in the filter. A second keyword— eq , lt , or gt —must be used to indicate the mode of comparison, an integer from 0 to 65535.

Usage

The filtering rules are based on source or destination host, network, or socket.

The **eq**, **gt** and **lt** keywords allow you to test the source or destination socket number in the packet to determine whether it does the following:

eq	Equals the socket number in the filter.
gt	Is greater than the socket number in the filter.
lt	Is less than the socket number in the filter.



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

Examples

```
Command> set ipxfilter e0.in 1 permit dstnet 0XC009C901
```

```
Filter e0.in updated
```

```
Command> set ipxfilter e0.in 2 permit srcnet 0XC009C905
```

```
Filter e0.in updated
```

```
Command> set ipxfilter e0.in 3 permit srchost 0XA0B1C2D3
```

```
Filter e0.in updated
```

```
Command> set ipxfilter e0.in 4 permit dsthost 0XA1B2C3D4
```

```
Filter e0.in updated
```

```
Command> set ipxfilter e0.in 5 deny dstsocket eq 451
```

```
Filter e0.in updated
```

```
Command> set ipxfilter e0.in 6 permit srcsocket gt 455
```

```
Filter e0.in updated
```

```
Command> show ipxfilter e0.in
```

```
- IPX Rules -
```

```
1 permit dstnet C009C901
```

```
2 permit srcnet C009C905
```

```
3 permit srchost A0B1C2D3
```

```
4 permit dsthost A1B2C3D4
```

```
5 deny dstsocket eq 0451
```

```
6 permit srcsocket gt 0455
```

See Also

add filter - page 13-4

set sapfilter

This command sets filtering rules for IPX Service Advertising Protocol (SAP) packets.



Note – Enter this command on one line, without any breaks. The line breaks shown here are due to the limited space available.

```
set sapfilter Filtername RuleNumber permit|deny [server String]
[network Ipxnetwork] [host Ipxnode] [socket eq|gt|lt Ipxsock]
```

<i>Filtername</i>	Name of an existing filter that is in the filter table.
<i>RuleNumber</i>	Filter rule number—between 1 and 256 for the PortMaster 3 and IRX, and between 1 and 100 for other PortMaster products.
permit	Permits an SAP packet that matches the filter to pass through the interface. This is the default.
deny	Stops an SAP packet that matches the filter from passing through the interface.
server	Specifies the comparison with the name of the server that is advertising its service.
<i>String</i>	SAP server name.
network	Specifies the comparison with the server's IPX network number.
<i>Ipxnetwork</i>	IPX network number, a 32-bit hexadecimal value.
host	Specifies the comparison with the server's IPX node address.
<i>Ipxnode</i>	IPX node address, a 48-bit hexadecimal value—usually the MAC address of the host.

socket	Specifies that the server's IPX socket number must be compared with the IPX socket number specified in the filter. A second keyword— eq , lt , or gt —must be used to indicate the mode of comparison.
eq, lt, or gt	Mode of comparison of socket numbers; equal (eq), less than (lt), or greater than (gt).
<i>Ipxsock</i>	Socket number specified for the comparison, an integer from 1 to 65535.

Usage

The filtering rules are based on server, network, host, or socket. SAP packets can be filtered only on output, not on input. SAP filter rules used as inbound packet filters are ignored.

The **eq**, **gt** and **lt** keywords allow you to test the destination socket number in the packet to determine whether it does the following:

eq	Equals the socket number in the filter.
gt	Is greater than the socket number in the filter.
lt	Is less than the socket number in the filter.



Note – Entering the command **set filter** *Filtername* without any arguments removes all filter rules from the filter.

Examples

```
Command> set sapfilter e0.out 1 permit network C009C901
Filter e0.out updated
```

```
Command> set sapfilter e0.out 2 permit host A0B1C2D3E4F5
Filter e0.out updated
```

```
Command> set sapfilter e0.out 3 deny socket eq 452
Filter e0.out updated
```

```
Command> show sapfilter e0.out  
1 permit network C009C901  
2 permit host A0B1C2D3E4F5  
3 deny    socket eq 0452
```

See Also

add filter - page 13-4

show filter

This command shows the configuration of a specified filter.

show filter|ipxfilter|sapfilter *Filtername*

filter	Displays IP and IPX rules.
ipxfilter	Displays IPX rules only.
sapfilter	Displays SAP rules only.
<i>Filtername</i>	Name of a filter that is in the filter table.

Example

The following example denies all IP packets to the subnet 192.168.200.0/24 and permits all inbound and outbound TCP, UDP, and ICMP packets. All other services are denied.

```
Command> show filter internet.in  
1 deny    192.168.200.0/24 0.0.0.0/0 ip  
2 permit  0.0.0.0/0 0.0.0.0/0 tcp estab  
3 permit  0.0.0.0/0 0.0.0.0/0 udp dst eq 53  
4 permit  0.0.0.0/0 0.0.0.0/0 tcp dst eq 53  
5 permit  0.0.0.0/0 0.0.0.0/0 tcp dst eq 25  
6 permit  0.0.0.0/0 0.0.0.0/0 icmp
```

show table filter

This command shows a list of the filters in the filter table.

show table filter

Example

```
Command> show table filter
internet.in      ether0.in      check.in      pingtr.in
internet.out     ether.out
```

See Also

show filter - page 13-24

This chapter describes the command line interface commands used to configure the network address translator (NAT) features on a PortMaster. ComOS implementation of NAT is based on RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

ComOS supports the following NAT features for both inbound and outbound sessions:

- **Basic NAT** for translating, or mapping, private IP addresses to global IP addresses. Private IP addresses are unregistered IP addresses, which are considered internal to the PortMaster running NAT. Global IP addresses are registered, unique IP addresses, which are valid on the Internet.
- **Network address port translation (NAPT)** for translating many network addresses and TCP and/or UDP (TCP/UDP) ports into a single global network address with translated TCP/UDP ports.
- **NAT outsource**, a proprietary function that enables a PortMaster to process and manage NAT for a connected network interface that cannot run NAT.

For a detailed explanation of NAT on the PortMaster and detailed information on how to configure NAT for a specific application, refer to the *PortMaster Configuration Guide*.



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

Displaying NAT Information

To display NAT information on the console, use the following commands:

- **ifconfig**—see page 2-9
- **show location**—see page 8-29
- **show map**

- **show nat mapusage**
- **show nat sessions**
- **show nat statistics**
- **show S0**—see page 2-35
- **show table map**
- **show syslog**—see page 2-40
- **show user**—see page 7-25

For general information about using the command line interface, refer to Chapter 1, “Introduction.”

Summary of NAT Commands

The commands in Table 14-1 enable you to configure the PortMaster to use NAT, NAPT, and NAT outsource.

Table 14-1 NAT Commands

Command Syntax	
add map <i>Mapname</i>	- see page 14-3
delete map <i>Mapname</i>	- see page 14-4
delete nat session <i>Sessionid</i>	- see page 14-5
reset nat [<i>Ether0</i> <i>S0</i> <i>W1</i>]	- see page 14-6
save map	- see page 14-7
set debug nat-ftp nat-icmp-err nat-rt-interface nat-max on off	- see page 19-12
set <i>Ether0</i> <i>S0</i> <i>W1</i> location <i>Locname</i> user <i>Username</i> nat inmap outmap defaultnapt Mapname blank [outsource]	- see page 14-14
set <i>Ether0</i> <i>S0</i> <i>W1</i> location <i>Locname</i> user <i>Username</i> nat log sessionfail sessionsuccess syslog console on off	- see page 14-16
set <i>Ether0</i> <i>S0</i> <i>W1</i> location <i>Locname</i> user <i>Username</i> nat sessiontimeout tcp other <i>Number</i> [minutes seconds]	- see page 14-17

Table 14-1 NAT Commands (Continued)

Command Syntax	
set <i>Ether0 S0 W1 location Locname user Username nat</i>	- see page 14-19
session-direction-fail-action <i>drop icmproject passthrough</i>	
set map <i>Mapname RuleNumber blank</i>	- see page 14-11
set map <i>Mapname RuleNumber addressmap staticaddressmap</i>	- see page 14-8
<i>Ipaddrxfrom Ipaddrxto @ipaddr [log]</i>	
set map <i>Mapname Rulenumber static-tcp-udp-portmap</i>	- see page 14-12
<i>Ipaddrxfrom:{Tport1 Portname} Ipaddrxto:{Tport2 Portname}</i>	
set syslog nat	- see page 3-20
show map <i>Mapname</i>	- see page 14-20
show nat mapusage	- see page 14-21
show nat sessions [<i>tcp udp ftp Sessionid</i>]	- see page 14-22
show nat statistics	- see page 14-24
show table map	- see page 14-26

NAT Commands

The following commands are used to configure and maintain basic NAT, NAPT, and NAT outsource on any PortMaster.

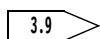


Note – Only stub border routers can be configured for NAT.

For information on how to use these commands to configure your PortMaster for a specific application, refer to the *PortMaster Configuration Guide*.

add map

This command creates a new address map and adds it to the map table.



add map *Mapname*

Mapname

Address map name—up to 15 characters.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

You must reset an active interface to add, delete, or change a NAT map.

Example

```
Command> add map bnat.inmap
NAT Map bnat successfully added
```

See Also

delete map - page 14-4
set map addressmap - page 14-8
set map staticaddressmap - page 14-8
set map static-tcp-udp-portmap - page 14-12

delete map

This command deletes an address map from the map table.



delete map *Mapname*

Mapname Address map name in the map table.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

If you delete an address map name that is configured for a user, location, or interface, NAT is disabled on that interface the next time you reset the interface, reset NAT on the interface, or use the **reset all** command.

You must reset an active interface to delete, add, or change a NAT map.



Caution – Resetting NAT when connections are active can cause improper disconnections, leaving client and server connections open.

Example

```
Command> delete map bnat  
NAT Map bnat successfully deleted
```

See Also

add map - page 14-3

delete nat session

This command deletes an active NAT session from the map table.

 **delete nat session** [*Sessionid*]

Sessionid Number identifying a NAT session.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Use the command **show nat sessions** to view the identification numbers of current NAT sessions. To delete all NAT sessions, use the **reset nat** command.

Example

```
Command> delete nat session 5408  
NAT Session deleted successfully.
```

See Also

reset nat - page 14-6

show nat sessions - page 14-22

reset nat

This command resets active NAT sessions on an interface or all interfaces on the PortMaster.



reset nat [*Ether0*|*S0*|*W1*]



Caution – Resetting NAT when connections are active can cause improper disconnections, leaving client and server connections open.

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Asynchronous port.
<i>W1</i>	Synchronous port.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command resets active NAT sessions on the specified interface. If no interface is specified, this command resets all existing NAT sessions for the PortMaster, like the **reset all** command.



Note – If you modify the NAT configuration on any active port, you must reset the port to activate the new NAT settings.

To delete a specific NAT session, use the command **delete nat session** *Sessionid*.

On-Demand Locations. The **reset nat** command does not work for locations configured for on-demand service. To reset NAT for a location configured for on-demand service, you must use the **reset dialer** command as follows:

1. Enter the following commands in order:

```
Command> set location Locname maxports 0
Command> reset dialer
```

2. Enter the necessary NAT changes to the location:

```
Command> set location Locname nat inmap|outmap  
Command> set location Locname nat log  
Command> set location Locname nat sessiontimeout  
Command> set location Locname nat session-direction-fail-action
```

3. Reconfigure the maximum number of network dial-out ports for this location:

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

Replace *Number* with the original **maxport** setting for the location.

Example

```
Command> reset nat  
NAT reset on all router interfaces.
```

See Also

delete nat session - page 14-5
reset dialer - page 2-15
reset S0|W1 - page 2-15
set location maxports - page 8-18

save map

This command saves NAT address map contents into nonvolatile RAM.

**save map***Usage*

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Example

Command> **save map**
NAT Map table successfully saved
New configurations successfully saved.

See Also

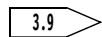
reset nat - page 14-6

set map addressmap

This command creates a static or dynamic IP address map entry and numbers the entry.



Note – This command must be entered on one line without any breaks.



set map *Mapname RuleNumber* **addressmap|staticaddressmap** *Ipaddrxfrom*
Ipaddrxto **@ipaddr [log]**

<i>Mapname</i>	Address map name that is in the map table.
<i>RuleNumber</i>	Integer between 1 and 20.
addressmap	Sets dynamic address mapping. The keyword addressmap can be abbreviated to am .
staticaddressmap	Sets static IP address mapping for multiple address lists. The keyword staticaddressmap can be abbreviated to sam .
<i>Ipaddrxfrom</i>	IP address or range or list of IP addresses to be translated.
<i>Ipaddrxto</i>	IP address or range or list of IP addresses to translate to, as described in the “Usage” section.

@ipaddr	IP address of the port being configured as the destination address. This keyword can be used only for outbound or outbound NAT outsource addresses.
log	Selectively logs events for this map entry. For example, when an outbound map is specified, a message is sent to the console whenever successful translation of this map entry occurs.



Note – You must first set logging settings before using the **set nat log** command.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Private Addresses. Lucent recommends using one of the private IP address ranges specified in RFC 1918 to number your private networks, which are currently 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 (172.168.0.0/16)

Address Format. IP addresses entered as *Ipaddxto* and *Ipaddxfrom* values must have one of the following formats or a combination of the following:

<i>Ipaddress/NM</i>	IP address in dotted decimal notation plus a netmask as a number from 1 to 32, preceded by a slash (/)—for example, /24 .
<i>Ipaddress-IPaddress</i>	Range of IP addresses in dotted decimal notation, separated by a hyphen (-)—for example, 192.162.7.1-192.162.7.5 .
<i>Ipaddress</i> <i>Ipaddress1,Ipaddress2,...</i>	A single address or a list in dotted decimal notation. Separate a list of IP addresses with commas (,).

Rule Removal. Enter the command without a rule number to remove the rule from the address map. Use the command **set map Mapname blank** to empty the contents of a map.

Mapping. Address mapping is applied to the first packet of the NAT session. When an inbound address map is defined for a port with this option, the translation succeeds only when the destination IP address of the first packet of the session matches the *Ipaddrxfrom* address.

For example, if you have an outmap with the rule **1 am 192.168.1.32 10.1.70.32**, and an outbound packet with a source IP address of 192.168.1.32 arrives at the interface, the source IP address is translated to 10.1.70.32.

Outsource NAT. To use outsource mode with **defaultnapt** or any address map containing **@ipaddr**, you must set the IP address of the specified port to the IP address of the interface you are outsourcing for to create a dial-out point-to-point network connection. Use the **set user local-ip-address** command to do so.

Examples

The following command dynamically maps a private IP address pool 10.0.0.0/8 to the single global IP address 192.168.1.36.

```
Command> set map newmap 1 addressmap 10.0.0.0/8 192.168.1.36
NAT Map newmap has rule 1 successfully updated.
```

The following command always statically maps private IP address 10.0.0.2 to global IP address 192.168.1.36, and private IP address 10.0.0.5 to global IP address 192.168.1.36.

```
Command> set map statmap 1 staticaddressmap 10.0.0.2, 10.0.0.5 192.168.1.36,
192.168.1.37
NAT Map statmap has rule 1 successfully updated.
```

The following command maps the address pool to **@ipaddr**, the IP address assigned to the port.

```
Command> set map mymap 1 addressmap 10.0.0.0/8 @ipaddr
NAT Map mymap has rule 1 successfully updated.
```

The following command removes a rule from an address map.

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

See Also

set nat inmap|outmap - page 14-14
set nat log - page 14-16
set user local-ip-address - page 7-15
show map - page 14-20

set map blank

This command removes the contents from an address map.

3.9

set map *Mapname RuleNumber* | **blank**

<i>Mapname</i>	Address map name that is in the map table.
<i>Rulenummer</i>	Deletes the specified rule from the map.
blank	Deletes all the contents from an address map.

Examples

Command> **set map testmap1 blank**
NAT Map testmap1 is empty.

Command> **set map testmap2 1**
NAT Map testmap2 has rule 1 Removed.

set map static-tcp-udp-portmap

This command defines a static map entry for a TCP/UDP port address range map entry and numbers the rule for the entry.



Note – This command must be entered on one line without any breaks.



```
set map Mapname RuleNumber static-tcp-udp-portmap
Ipaddrxfrom:{Tport1|Portname} Ipaddrxto:{Tport2|Portname} log
```

Mapname	Address map name that is in the map table.												
static-tcp-udp-portmap	Sets TCP/UDP port mapping. This keyword can be abbreviated to stupm .												
RuleNumber	Integer between 1 and 20.												
Ipaddrxfrom	IP address to be translated.												
Ipaddrxto	IP address to translate to.												
Portname	One of the following services: <table><tr><td>telnet</td><td>TCP port 23.</td></tr><tr><td>ftp</td><td>TCP ports 20 and 21.</td></tr><tr><td>tftp</td><td>UDP port 69.</td></tr><tr><td>http</td><td>TCP port 80.</td></tr><tr><td>dns</td><td>TCP/UDP port 53</td></tr><tr><td>smtp</td><td>TCP port 25</td></tr></table>	telnet	TCP port 23.	ftp	TCP ports 20 and 21.	tftp	UDP port 69.	http	TCP port 80.	dns	TCP/UDP port 53	smtp	TCP port 25
telnet	TCP port 23.												
ftp	TCP ports 20 and 21.												
tftp	UDP port 69.												
http	TCP port 80.												
dns	TCP/UDP port 53												
smtp	TCP port 25												

Tport

Number between 1 and 65535—TCP or UDP port number or range of port numbers.

See Table D-1, “TCP and UDP Ports and Services,” on page D-1 for a list of TCP and UDP ports.

log

Selectively logs the map entry.



Note – You must first enable logging settings before using the command **set nat log**.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Private Addresses. Lucent recommends using one of the private IP address ranges specified in RFC 1918 to number your private networks, which are currently the following:

- 10.0.0.0 through 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 through 172.31.255.25 (172.16.0.0/12)
- 192.168.0.0 through 192.168.255.255 (192.168.0.0/16)

Mapping. The PortMaster evaluates address and port mapping from left to right, with the source and destination addresses relative to the direction of session.

Address mapping is applied to the first packet of the NAT session. When an inbound address map is defined for a port with this option, the translation succeeds only when the destination IP address of the first packet of the session matches the *Ipaddrxfrom* address.



Note – Some port-dependent applications cannot work with NATP.

Example

In the following example, when an inbound HTTP packet with a destination address of 192.168.7.1 arrives at the interface to which this map is applied for inbound sessions, the destination address is translated to 10.1.1.0.

Command> **set map w24.inmap 1 statictcpudpportmap 192.168.7.1:http 10.1.1.10:http**
NAT Map w24.inmap has rule 1 successfully updated.

See Also

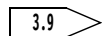
add map - page 14-3
set map addressmap - page 14-8

set nat inmap|outmap

This command specifies the direction of an address map as inbound or outbound; associates it with an interface, user, or location; and optionally enables the NAT outsource function.



Note – This command must be entered on one line without any breaks.



**set Ether0|S0|W1|location Locname|user Username nat inmap|outmap
defaultnapt|Mapname|blank [outsource]**

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Asynchronous port.
<i>W1</i>	Synchronous port.
location	Remote dial-out location.
<i>Locname</i>	Location name in the location table.
user	Network user.
<i>Username</i>	Username in the user table.
inmap	Sets the address map for inbound sessions.
outmap	Sets the address map for outbound sessions.

defaultnapt	Name of the following reserved map: 1. AddressMap 0.0.0.0/0 @ipaddr log.
<i>Mapname</i>	Map name that is in the map table.
blank	Dissociates the map from the specified interface, location, or user.
outsource	Sets an address map to be used in an outsource mode.



Note – You must reset an active port for changes to its NAT configuration to take effect.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

If you are using **defaultnapt**, the specified interface must have at least one valid global IP address—even if it is dynamically assigned. If you are using **defaultnapt** in the outsource mode or with any map using **@ipaddr**, you must set a local IP address to a user.

Effects of using **defaultnapt**:

- **defaultnapt** set to **outmap** without the **outsource** option—all outbound IP sessions from the specified port are subject to NAPT, using the IP address assigned to the port.
- **defaultnapt** set to **outmap** with the **outsource** option—the specified port is subject to outbound outsource NAPT, using the IP address assigned to the port.

This command also sets the NAT outsource function that enables a PortMaster to process and maintain NAT for a connected network interface that is unable to run NAT. For example, the PortMaster can perform address translation for a remote client that is dialed in to a WAN port but cannot run NAT on the local router. For more information on configuring a PortMaster for NAT outsource mode, see the *PortMaster Configuration Guide*.

Examples

```
Command> set location natloc nat outmap newmap  
NAT Outmap for Location natloc set to newmap
```

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

NAT Outmap for Location natloc set to defaultnapt

Command> **set user natuser nat outmap defaultnapt outsource**
NAT Outsource Outmap for user natuser set to defaultnapt

See Also

- set location local-ip-address** - page 8-16
- set map addressmap** - page 14-8
- set map staticaddressmap** - page 14-8
- set map statictcpudpport** - page 14-12
- set user local-ip-address** - page 7-15

set nat log

This command sets logging options for a NAT session on an interface.



set *Ether0|S0|W1* **location** *Locname* **user** *Username* **nat log**
sessionfail|sessionsuccess|syslog|console on|off

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Asynchronous port.
<i>W1</i>	Synchronous port.
location	Remote dial-out location.
<i>Locname</i>	Location name in the location table.
user	Network user.
<i>Username</i>	Username in the user table.
sessionfail	Logs failed NAT sessions. This is the default.
sessionsuccess	Logs successful NAT sessions.
syslog	Logs selected events to syslog .

console Displays selected events on the console. This is the default.

on Enables the settings specified.

off Disables the settings specified.



Note – You must reset a port for changes to its NAT configuration to take effect.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Example

Command> **set location or nat log sessionfail on**
 NAT Log option for Location or set to SessionFail, Console

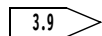
Command> **set location or nat log syslog on**
 NAT Log option for Location or set to SessionFail, SysLog, Console

See Also

reset *S0|W1* - page 2-15

set nat sessiontimeout

This command sets the maximum idle time for a NAT session.



set *Ether0|S0|W1|location Locname|user Username nat sessiontimeout*
tcp|other *Number[minutes|seconds]*

Ether0 Ethernet interface.

S0 Asynchronous port.

W1 Synchronous port.

location	Remote dial-out location.
<i>Locname</i>	Location in the location table.
user	Network user.
<i>Username</i>	User in the user table.
tcp	Sets the session timeout value for TCP sessions. By default, TCP session timeout is set at 1440 minutes (24 hours).
other	Sets the session timeout value for all types of sessions other than a TCP session, such as UDP and ICMP. The default setting for other is 15 seconds.
<i>Number</i>	Number of minutes or seconds, an integer between 0 and 99999.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.



Note – You must reset an active port for changes to its NAT configuration to take effect.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Example

Command> **set location or nat sessiontimeout other 30 seconds**
 NAT SessionTimeOut for or is set to: TCP: 1440 mins, Other: 30 secs

set nat session-direction-fail-action

This command sets the default action that the PortMaster takes in the event that a request for a NAT session is refused because of an invalid map configuration or because no mapping exists for the NAT request.

3.9

```
set Ether0|S0|W1 location Locname|user Username nat  
session-direction-fail-action drop|icmpreject|passthrough
```

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Asynchronous port.
<i>W1</i>	Synchronous port.
location	Remote dial-out location.
<i>Locname</i>	Location in the location table.
user	Network user.
<i>Username</i>	User in the user table.
session-direction-fail-action	Identifies the action that a PortMaster takes if a NAT session fails. This keyword can be abbreviated to sdfa .
drop	If a request for a NAT session fails, the PortMaster drops session packets without notifying the source host. This is the default.
icmpreject	If a request for a NAT session fails, the PortMaster notifies the source host that packets are rejected.
passthrough	If a request for a NAT session request fails, packets are permitted to pass through untranslated.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

See Also

show nat sessions - page 14-22

show map

This command displays the contents of an address map.



show map *Mapname*

Mapname Address map name that is in the map table.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command displays the configuration of a specific map, including the source IP address or subnet, and the destination IP address.

Example

```
Command> show map net1  
1. addressmap        10.0.0.2, 10.0.0.5 192.168.1.36, 192.168.1.37  
2. addressmap        10.0.0.0/8 192.168.1.38, 192.168.1.39, 192.168.1.40
```

Explanation

The example displays the entries for address map **net1**. The first rule reserves global addresses 192.168.1.36 and 192.168.1.37 for the private addresses 10.0.0.2 and 10.0.0.5. The second rule dynamically maps any three devices from the subnet 10.0.0.0/8 to the global addresses 192.168.1.38, 192.168.1.39, and 192.168.1.40.

See Also

set map addressmap - page 14-8

show nat mapusage

This command shows available TCP or UDP ports for currently active NAT interfaces.



show nat mapusage

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command shows source utilization and can be used for debugging. Use this command to display available TCP/UDP resources for a port, the IP address of the port, and port bindings.

Example

```
Command> show nat mapusage
Router-Port Dir Bind-Type      Original-Parameters    Xlation-parameters    #Sess
-----
No resource BINDings to display

Router-Port Dir Resource-Type  Resources-Available-for-use
-----
ether0      Out NAPT TU ports 192.162.7.3: 29179-53551, 53553-55075,
                                     55077-61062, 61064-61083, 61085-63899,
                                     63901-63913, 63915-64160, 64162-64166, 64171,
                                     64173-64174, 64177-64178, 64180, 64183,
                                     64186-64188, 64194-64195, 64198, 64201,
                                     64204-64207, 64209-64210, 64213, 64215-64218,
                                     64222, 64227-64229, 64234-64235, 64237-64238,
                                     64240, 64244-64246, 64249, 64252, 64256-64257,
                                     64853-64854, 64856, 64858-64859, 64862-64863,
```

Explanation

Router Port	Interface on the PortMaster—Ether0 or Ether1, asynchronous or synchronous port.
Dir	Direction of the session: Out—packets are originating from the host specified. In—packets are destined for the port specified.
Original Parameters	IP addresses translated from and ports.
Xlation-parameters	Translation parameters.
Resource Type	Type of NAT address mapping used—NAPT, static, dynamic, or pool—and the type of port used.
Resources-Available for-use	Contains the range of available TCP/UDP port numbers.

See Also

show nat session - page 14-22

show nat sessions

This command displays information about active NAT sessions.



show nat sessions tcp|udp|ftp|*Sessionid*

tcp	Displays information about all NAT TCP sessions.
udp	Displays information about all NAT UDP sessions.
ftp	Displays information about all NAT FTP sessions.
<i>Sessionid</i>	Number identifying a NAT session.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

To view information about a specific NAT session, append the session identification number at the end of the command line.

Example

```
Command> show nat session
Total no. of sessions: 588
ID      Router Sess Dir  Original-Session-Params  Translated-Sess-Params  Idle
      Port   Type
-----
138773 ether0 FTP  Out  (192.168.7.0,1118)->    (192.168.8.12,55076)->  1426
      (172.16.6.1,21)
      DATA In   (172.16.6.1,20)->      (172.16.6.1,20)->
      (192.168.7.0,1118)    (192.168.8.12,55076)
5408   ether0 FTP  Out  (192.168.7.0,2486)->    (192.168.8.12,26679)->  8552
      (172.16.6.1,21)      (172.16.6.1,21)
```

Explanation

- Total no. of sessions Active NAT sessions.
- ID Session identification number.
- Router Port Type of interface—*Ether0*, or *Ether1*, *S0*, *W1*, user, or location.
- Sess Type Session type—such as FTP, Telnet, or HTTP.
- Dir Direction of session:
- Out—packets are originating from the host specified.
 - In—packets are destined for the port specified.

Original-Session-Params	IP address or range of addresses. For NAT configurations, this column also displays the TCP/UDP port number or port range.
Translated-Session-Params	Translated IP address or range of addresses. For NAT configurations, this column also displays the TCP/UDP port number or port range.
Idle Secs	Idle time in seconds.

See Also

delete nat session - page 14-5
set nat session-direction-fail-action - page 14-19

show nat statistics

This command displays the status of all NAT sessions for a PortMaster configured for NAT.



show nat statistics

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

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

This command can be useful for tracking failed translations due to incorrect session flow or incomplete maps.

Example

Command> **show nat statistics**

```
Router  Dir    Good    ==== Translation failed due to: ====
Port                               Xlated   Internal  Address/  SessDir   ICMP     Session   Session   Misc
                               Packets  failures  TU port   Invalid   Rejects   timed-    type not
                                                             shortage Dropped   Sent      out      allowed
ptp5    In                               4         0         0         0         0         0         0
        Out   4         0         0         0         0         0         0         0
```

Explanation

Router Port	Name of the port.
Dir	Direction of the active NAT session on the port—inbound or outbound.
Good Xlated Packets	Number of translated packets.
Internal failures	Number of failed NAT sessions due to internal failures.
Address/TU port shortage	Number of failed NAT sessions due to an insufficient number of global addresses or TCP/UDP ports.
Sessdir Invalid Dropped	Number of unsuccessful translation attempts due to incomplete or invalid map entries.
ICMP Rejects Sent	Number of ICMP rejects sent due to session-direction-failure-action.
Session timed-out	Number of failed NAT sessions due to exceeded idle times.
Session type not allowed	Number of unsuccessful NAT sessions due to invalid sessions types.
Misc	Number of failed NAT sessions or unsuccessful translation attempts due to reasons not specified elsewhere in the output.

See Also

set nat session-direction-fail-action - page 14-19

show nat sessions - page 14-22

show table map

This command shows current address maps in the map table.

3.9

show table map

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

To delete an address map from the map table, use the command **delete map** *Mapname*.

Example

```
Command> show table map  
m-napt          cubie          i-map          bnat
```

Explanation

The output displays the map names in the map table.

This chapter describes the commands you use to configure the Layer 2 Tunneling Protocol (L2TP) on the PortMaster. L2TP allows the PortMaster to tunnel PPP frames from an incoming call across an IP network from one PortMaster that answers the call—an L2TP access concentrator (LAC)—to another PortMaster that processes the PPP frames—an L2TP network server (LNS).

ComOS releases 3.9 and later relevant releases support LAC and LNS features on the PortMaster.

L2TP can be implemented on the PortMaster with or without the RADIUS call-check feature. A LAC and the LNS can use the same RADIUS server. To use L2TP, you must add the appropriate attributes to the RADIUS dictionary. See the *PortMaster Configuration Guide* for these attributes and for additional information about configuring L2TP on the PortMaster.

Displaying L2TP Diagnostic Information

To display L2TP debug information on the console, use the following commands:

- **set console**—see page 2-20
- **set debug l2tp**—see page 19-9

When finished, use the following commands:

- **set debug off**—see page 19-6
- **reset console**—see page 2-15

To display L2TP session information or line status, use the following commands:

- **show l2tp**
- **show global**—see page 2-28
- **show S0**—see page 2-35

Summary of L2TP Commands

Table 15-1 shows the L2TP configuration commands.

Table 15-1 L2TP Commands

Command Syntax	
create 12tp tunnel udp <i>Ipaddress</i> [<i>Password</i> none]	- see page 15-2
reset 12tp [stats tunnel <i>Number</i>]	- see page 15-3
set call-check on off	- see page 3-4
set debug 12tp max packets [<i>Bytes</i>] setup stats on off	- see page 19-9
set 12tp authenticate-remote on off	- see page 15-6
set 12tp choose-random-tunnel-endpoint on off	- see page 15-7
set 12tp disable enable {lac lns}	- see page 15-4
set 12tp secret [<i>Password</i> none]	- see page 15-8
show 12tp global sessions stats tunnels	- see page 15-9

L2TP Commands

The commands in this section are used to configure and maintain L2TP on a PortMaster.

create 12tp tunnel

This command manually establishes an L2TP tunnel for the PortMaster for testing and troubleshooting.



create 12tp tunnel udp *Ipaddress* [*Password*|none]

- Ipaddress*
- IP address of the L2TP tunnel end point expressed in dotted decimal notation.
- Password*
- Optional password that the PortMaster uses to authenticate itself when responding to a tunnel request from the L2TP end point.

none Sets the PortMaster to use the L2TP secret configured for it with the **set l2tp secret** command. This is the default.

Usage

The PortMaster supports this command on ComOS 3.9 and later relevant releases.
Use this command for testing and troubleshooting L2TP. It is global for the PortMaster.

Example

Command> **create l2tp tunnel udp 192.168.60.8**
OK

See Also

set l2tp - page 15-4
set l2tp secret - page 15-8

reset l2tp

This command resets active L2TP tunnels and sessions or resets the L2TP statistics counter for the entire PortMaster.



reset l2tp [**stats**|**tunnel** *Number*]

stats Resets L2TP counters displayed by the **show l2tp stats** command to zero. This command does not reset active L2TP sessions.

tunnel *Number* Resets the specified tunnel. To view L2TP tunnel numbers, use the **show l2tp tunnels** command.

Number is an integer between 1 and 100. If no tunnel number is specified, all L2TP tunnels are reset.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

To reset all L2TP tunnels and terminate all PPP sessions, enter **reset l2tp** with no arguments.

Example

```
Command> reset l2tp stats  
Command>
```

See Also

show l2tp - page 15-9

set l2tp

This command enables and disables L2TP features on the PortMaster.



set l2tp disable|enable {lac|lns}

disable Disables L2TP on the PortMaster

enable lac Enables the PortMaster as a LAC.

enable lns Enables the PortMaster as an LNS. On an LNS, any line ports are automatically set as T1 or E1 ports and can no longer be used for dial-in. The virtual *S0* ports become *WI* ports.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

To activate the new configuration, you must use the **save all** command.

L2TP and RADIUS Accounting. Both the LAC and LNS log any user sessions to RADIUS accounting. If you are using the RADIUS call-check feature to establish the L2TP tunnel, the LAC's accounting data contains only the calling line ID (CLID) information, not the username, because that information has not yet been passed on the link. The LNS accounting data shows both the CLID and username in its accounting data along with the assigned IP address.

If partial authentication instead of call-check is taking place on the LAC, then the username might be available to it. In that case, the username appears in the RADIUS accounting logs for both the LNS and the LAC.

In both cases, the LNS displays NAS-Port-Type as **virtual**, while the LAC displays the NAS-Port-Type set to the actual physical interfaces connection type—the normal behavior of the network access server.

Examples

```
Command> set 12tp disable
```

```
Command> save all
```

```
Command> set 12tp enable lac
```

```
L2TP lac will be enabled after next reboot
```

```
Command> save all
```

See Also

set call-check - page 3-4

set 12tp-authenticate remote - page 15-6

show 12tp - page 15-9

set 12tp authenticate-remote

This command sets the PortMaster to initiate L2TP tunnel authentication.



set 12tp authenticate-remote on|off

on Sets the PortMaster to initiate authentication with the other side of the L2TP connection before it creates the tunnel.

off Disables the PortMaster 4 from initiating authentication.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command configures the PortMaster—set either as a LAC or an LNS—to initiate authentication before establishing a tunnel, but does not determine how the PortMaster responds to an authentication request.

Example

```
Command> set 12tp authenticate-remote on  
OK
```

See Also

set 12tp - see page 15-4

set 12tp choose-random-tunnel-endpoint

This command determines the order in which the PortMaster chooses a tunnel end point when multiple tunnel end points are set for a user.

3.9

set 12tp choose-random-tunnel-endpoint on|off

- | | |
|------------|--|
| on | Sets the PortMaster to choose the tunnel end point randomly from the list of tunnel end points returned by RADIUS. |
| off | Sets the PortMaster to select a tunnel end point serially. |

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

This command changes the way the PortMaster selects a tunnel end point when multiple end points are set for a user. By default, the PortMaster selects the tunnel end point serially.

You can configure a RADIUS user profile to support up to three L2TP redundant end points—the LAC discards any additional end points. See the *PortMaster Configuration Guide* for additional information.



Note – The PortMaster supports up to three L2TP end points.

Example

```
Command> set 12tp choose-random-tunnel-endpoint on
OK
```

See Also

set 12tp - see page 15-4

set 12tp secret

This command sets the password used by the PortMaster to respond to L2TP tunnel authentication requests.



set 12tp secret [*Password*|**none**]

<i>Password</i>	Sets the password that the PortMaster uses to respond to L2TP tunnel authentication requests. <i>Password</i> is a string of up to 15 ASCII characters.
none	Disables the L2TP password on the PortMaster. This is the default.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

When a PortMaster configured as a LAC receives a tunnel authentication request, it uses the Tunnel-Password value from the RADIUS access-accept, if present, instead of the global L2TP secret. See the *PortMaster Configuration Guide* for additional information.

Example

```
Command> set 12tp secret isotopes
New secret: isotopes
```

See Also

set 12tp - page 15-4

show l2tp

This command displays information about active L2TP sessions for the PortMaster.

3.9

show l2tp global|sessions|stats|tunnels

global	Displays L2TP settings.
sessions	Displays information about active L2TP sessions.
stats	Displays L2TP statistics.
tunnels	Displays information about L2TP tunnels such as the tunnel identification number, assigned ID, tunnel ID, and port name.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Examples

```
Command> show l2tp global
debug packets debug stats debug setup Tunnel Authentication Enabled
Initiation of Authentication Remote Tunnel Disabled
Default Board configuration
```

```
Command> show l2tp sessions
  Id      Assign-Id  Tunnel-Id  Portname
  2305      1           1          S0
```

Command> **show 12tp stats**

NEW_SESSION	1
NEW_TUNNEL	4
TUNNEL_CLOSED	3
HANDLE_CLOSED	3
L2TP_STATS_MEDIUM_HANDLE	3
INTERNAL_ERROR	14
CTL_SEND	9
CTL_REXMIT	1
CTL_RCV	10
MSG_CHANGE_STATE	4
WRONG_AVP_VALUE	3
EVENT_CHANGE_STATE	3

Command> **show 12tp tunnels**

Id	Assign-Id	Hnd	State	Server-Endpoint	Client-Endpoint
1	1	24	L2T_ESTABLISHED	192.168.6.13	192.168.10.28

This chapter describes the commands you use to configure the PortMaster for static and default routing, the Routing Information Protocol (RIP), route propagation, and subnet masks—including variable-length subnet masks (VLSMs). See the *PortMaster Routing Guide* for configuration instructions and examples.

To configure the PortMaster for advanced routing protocols, see Chapter 17, “OSPF Routing,” and Chapter 18, “BGP Routing.”

Displaying Routing Information

To display routing information on the console, use the following commands:

- **show routes**
- **show route to-dest**
- **show ipxroutes**
- **show propagation**
- **show table netmask**

For general information about using the command line interface, refer to Chapter 1, “Introduction.”

Summary of Routing Commands

The commands shown in Table 16-1 are used for displaying route information and configuring the PortMaster for the following:

- Default and static routes
- Subnet masks, including variable-length subnet masks (VLSMs)
- Routing Information Protocol (RIP)
- Route filters

- Route propagation from one routing protocol into another
- Netmask tables

Table 16-1 Routing Commands

Command Syntax	
add ipxroute <i>Ipxnetwork Ipxaddress Metric Ticks</i>	- see page 16-14
add netmask <i>Ipaddress Ipmask</i>	- see page 16-23
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 16-3
add route <i>Ipaddress[/NM] Ipaddress(gw) Metric</i>	- see page 16-15
delete ipxroute <i>ipxnetwork ipxaddress</i>	- see page 16-16
delete netmask <i>Ipaddress</i>	- see page 16-24
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 16-3
delete route <i>Ipaddress Ipaddress(gw)</i>	- see page 16-17
reset propagation	- see page 16-6
save netmask	- see page 16-24
save route	- see page 16-17
set default <i>on off broadcast listen</i>	- see page 16-18
set <i>Ether0 S0 W1 netmask Ipmask</i>	- see page 16-7
set <i>Ether0 S0 W1 rip on off broadcast listen</i>	- see page 16-19
set <i>Ether0 S0 W1 user Username location Locname route-filter incoming outgoing Filtername</i>	- see page 16-8
set gateway <i>Ipaddress [Metric]</i>	- see page 16-12
set ipxgateway <i>Network Node Metric</i>	- see page 3-10
set location <i>Locname rip on off broadcast listen</i>	- see page 16-20

Table 16-1 Routing Commands (Continued)

Command Syntax	
set user <i>Username</i> rip on off broadcast listen	- see page 16-21
set user-netmask on off	- see page 16-13
show ipxroutes	- see page 16-25
show propagation	- see page 16-26
show routes [<i>String</i> <i>Prefix/NM</i>]	- see page 16-27
show route to-dest <i>Ipaddress</i>	- see page 16-29
show table netmask	- see page 16-31

General Routing Commands

The following commands set the default route gateway address, user and IP netmasks, route filters, and route propagation.

add|delete propagation

These commands create, modify, or delete a propagation rule that defines how routes coming from one routing protocol are translated and advertised by the PortMaster into another routing protocol.



Note – These commands are available only on the PortMaster 3 and IRX products.

add propagation *Protocol(src) Protocol(dest) Metric Filtername*

delete propagation *Protocol(src) Protocol(dest)*

<i>Protocol(src)</i>	Designates the source protocol of the route. Use one of the following keywords: <ul style="list-style-type: none">• rip• static• ospf• bgp
<i>Protocol(dest)</i>	Designates the destination routing protocol for the route propagation. Use one of the following keywords: <ul style="list-style-type: none">• rip• static• ospf• bgp
<i>Metric</i>	Common metric used to translate from one protocol to the other. A metric of 0 indicates that the automatic rules in use in the PortMaster attempt to build a metric automatically. By default, all routes propagate and the common metric is 0.
<i>Filtername</i>	IP access filter added to the filter table with the add filter command and configured with the set filter command for use in the propagation rule.



Caution – If you plan to use a constant metric instead of the automatically generated metric provided by the ComOS, then you run the risk of creating routing loops if you do not provide for filters or policies to screen the route information that the PortMaster accepts from each routing protocol.

Usage

Use the **add propagation** command to create or modify an entry. See “Modifying a Propagation Rule” later in this section for modification instructions. Use the **delete propagation** command to delete an entry.

The **add propagation** command allows routes coming from one protocol to be advertised into another, based on the filter specified in the rule. The filter is a familiar IP access filter that uses the source address(es) specified in the filter to indicate the routes.

BGP-to-OSPF or BGP-to-RIP Propagation. You must explicitly configure the **add propagation** command to enable BGP routes to be propagated into OSPF or RIP.

Static-to-BGP Propagation. When static routes are the source protocol and BGP is the destination protocol, you need no other routing protocol. This combination allows the automatic, immediate advertisement into BGP of any configured static routes or static routes learned via RADIUS. This type of configuration is useful for points of presence (POPs) with a single LAN and an attachment to a BGP-routed backbone. Configuring static routes as the source protocol and BGP as the destination protocol eliminates the overhead of using a routing protocol other than BGP just to advertise static routes learned via RADIUS.

RIP-to-OSPF Propagation. To propagate RIP routes from an Ethernet interface into OSPF, you must first use the **set ether0 ospf accept-rip on** command.

Modifying a Propagation Rule. The recommended sequence for changing a propagation rule is as follows:

1. **Delete your propagation rule with** delete propagation.
2. **Add the revised propagation rule with** add propagation.
3. **Enter the command** reset propagation.

The output of the **reset propagation** command prompts you to enter the **reset ospf** or **reset bgp** command, if necessary.

4. **Follow any instructions for entering the** reset ospf **or** reset bgp **command.**

Example

To propagate BGP routes into OSPF, you can use a set of commands similar to the following:

```
Command> add filter fullprop  
New Filter successfully added
```

```
Command> set filter fullprop 1 permit 0.0.0.0/0 0.0.0.0/0  
Filter fullprop updated
```

```
Command> set propagation static bgp 1 fullprop  
Propagation rule successfully defined
```

See Also

add filter - page 13-4
set Ether0 ospf accept-rip on - page 17-7
set filter - page 13-6

reset propagation

This command resets the propagation rules system.

reset propagation

Usage

This command must be used each time the propagation filters are changed. If the propagation affects OSPF or BGP, use the commands **reset ospf** or **reset bgp**, respectively.

Example

```
Command> reset propagation  
Propagation rules reset
```

See Also

reset bgp - page 18-10

reset ospf - page 17-6

set Ether0|S0|W1 netmask

This command sets the IP netmask for a specified interface.

set Ether0|S0|W1 netmask Ipmask

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Network hardwired asynchronous port.
<i>W1</i>	Network hardwired synchronous port.
<i>Ipmask</i>	IP netmask in dotted decimal notation.

Example

Command> **set s0 netmask 255.255.255.0**

S0 netmask changed from 0.0.0.0 to 255.255.255.0

See Also

set Ether0 address - page 4-3

set location netmask - page 8-21

set user netmask - page 7-19

set Ether0|S0|W1|user|location route-filter

This command applies an input or output filter to a specified interface on the PortMaster or to a specified remote location (destination) or user. The filters determine which RIP or OSPF routes are injected into the routing table or advertised to other routers.



Note – These filters are ignored for BGP routes. Use BGP policies instead of filters to determine how BGP routes are accepted, injected, and advertised by the PortMaster. See Chapter 18, “BGP Routing,” for details on the **add bgp policy** and **set bgp policy** commands.

**set Ether0|S0|W1|user Username|location Locname route-filter
incoming|outgoing Filtername**



Note – This command is available only on the PortMaster 3 and IRX products.

<i>Ether0</i>	Ethernet interface that the route filter is applied to.
<i>S0</i>	Asynchronous port that the route filter is applied to.
<i>W1</i>	Synchronous port that the route filter is applied to.
<i>Username</i>	User from the user table.
<i>Locname</i>	Location from the location table.
incoming	Inbound filter.
outgoing	Outbound filter.
<i>Filtername</i>	IP access filter that has been created in the filter table with the add filter command and configured with the set filter command. Using the command without <i>Filtername</i> removes the filter.

Usage

The filters used are standard packet filters, with the source and destination addresses significant on input filters, and only the destination address significant on output filters.

The effects of a route filter depend on the protocol being filtered and on whether the filter is for inbound or outbound routes. Table 16-2 describes the effects.

To disable a filter, enter the command with no *Filtername* value.

To change a filter, enter the command with the new *Filtername* value.

After applying a route filter to be used with OSPF to an interface or making changes to it, use the **reset ospf** command.

Table 16-2 Effects of PortMaster Route Filters on RIP and OSPF Routes

Protocol	Inbound Route Filter—Route Injection	Outbound Route Filter—Route Advertisement
RIP	<div>The filter permit/deny rule applies and determines which routes are placed into the PortMaster routing table when</div> <ul style="list-style-type: none">• The address of the advertiser of the route matches the source address in the filter.• The destination address in the route being advertised matches the destination address in the filter. <div>For RIP, the advertiser is the next-hop (direct) advertiser of the information.</div>	<div>The destination addresses in the filter determine which routes are advertised out of this interface.</div>

Table 16-2 Effects of PortMaster Route Filters on RIP and OSPF Routes (Continued)

Protocol	Inbound Route Filter—Route Injection	Outbound Route Filter—Route Advertisement
OSPF	<p>The filter permit/deny rule applies and determines which routes are placed into the routing table when</p> <ul style="list-style-type: none">• The address of the advertiser of the route matches the source address in the filter.• The destination address in the route being advertised matches the destination address in the filter. <p>For OSPF, the advertiser is the ultimate advertiser of the information, not the next-hop OSPF router. Also, the filter specifies only the information that is in the routing table.</p> <p>Because OSPF area flooding rules make filtering inbound or outbound information on a per-interface basis impractical, applying the same inbound filter to all interfaces running OSPF within the same area is generally good practice.</p>	<p>The filter is ignored. OSPF area flooding rules make the definition of outbound route filters impractical on a per-interface basis.</p> <p>Use propagation filters to translate routing information from RIP, static, or BGP routes so that they do not enter OSPF as external Type 2 routes. See the add propagation command on page 16-3 for details.</p>

Examples

The following example disables an outbound route filter on the S1 interface:

```
Command> set s1 route-filter outgoing
Outgoing route filter on S1 disabled
```

The following example changes the inbound route filter on the S0 interface:

```
Command> set s0 route-filter incoming inb
Incoming route filter for port S0 changed from ina to inb
```

The following examples apply inbound and outbound route filters to user *zephyr*:

```
Command> set user zephyr route-filter incoming routes.in
Username: zephyr                               Type: Dial-in Network User
Address: Negotiated                             Netmask: 255.255.255.255
```

```

Protocol: PPP
MTU: 1500
OSPF: on
OSPF accept-rip: off
OSPF cost: 1
OSPF Hello Int: 10
OSPF Dead Time: 40
OSPF(WAN Type): nbma
route-filter
incoming: routes.in
outgoing:
Options: Quiet, Compression
Async Map: 00000000

```

```
Command> set user zephyr route-filter outgoing routes.out
```

```

Username: zephyr
Address: Negotiated
Protocol: PPP
MTU: 1500
OSPF: on
OSPF accept-rip: off
OSPF cost: 1
OSPF Hello Int: 10
OSPF Dead Time: 40
OSPF(WAN Type): nbma
route-filter
incoming: routes.in
outgoing: routes.out
Type: Dial-in Network User
Netmask: 255.255.255.255
Options: Quiet Compression
Async Map: 00000000

```

See Also

add filter - page 13-4

reset ospf - page 17-6

set bgp policy (advertisement) - page 18-33

set bgp policy (injection) - page 18-29

set gateway

This command sets the default route gateway address.

set gateway *Ipaddress* [*Metric*]

Ipaddress IP address. The default is 0.0.0.0.

Metric Metric for the default route, between 1 and 15. Default is 1.

Usage

The 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 gateway must not be the address of any interface on the PortMaster itself, but must be an address on a network attached to the PortMaster.

Example

```
Command> set gateway 172.16.200.1 1  
Gateway changed from 0.0.0.0 to 172.16.200.1, metric = 1
```

See Also

show routes - page 16-27

set user-netmask

This command sets the PortMaster behavior for the treatment of user netmasks.



Caution – Be careful when using this command because it affects both routing and Proxy ARP on the PortMaster.

set user-netmask on|off

- | | |
|------------|--|
| on | The PortMaster adds routes for dial-in users based on the specified netmask. |
| off | The PortMaster treats all netmasks specified in the user table or RADIUS as though they were 255.255.255.255. This is the default. |

Usage

ComOS 3.5 and later releases, support variable-length subnet masks (VLSMs). In contrast, previous releases of ComOS required the same netmask to be used for all subnets of a network.

With the command **set user-netmask off**, the PortMaster behaves in the same way as ComOS releases prior to 3.5, and treats all netmasks specified in the user table or RADIUS as if they were 255.255.255.255. The command **set user-netmask on** adds routes based on the specified netmask, and the PortMaster uses the actual value of the Framed-IP-Netmask RADIUS reply item to update the routing table when a user logs in.



Note – Always use a netmask of 255.255.255.255—or the default **set user-netmask off**—when using the PortMaster assigned address pool.

Example

```
Command> set user-netmask on
Accept User Netmask changed from off to on
```

See Also

add route - page 16-15

Static Routing Commands

Static routes are used to provide routing information instead of or in addition to that provided by RIP or other routing protocols. The static routes are stored in the PortMaster route table.

add ipxroute

This command adds a static route to the PortMaster IPX route table.

add ipxroute *Ipxnetwork Ipxaddress Metric Ticks*

<i>Ipxnetwork</i>	Destination IPX network number. A 32-bit hexadecimal number.
<i>Ipxaddress</i>	Gateway IPX address in the following format: IPX network number and IPX node address separated by a colon (:).
<i>Metric</i>	Hop count to the remote destination. An integer from 1 to 15.
<i>Ticks</i>	Time required to send the packet to the destination network in 50ms increments. An integer from 1 to 15.

Usage

The destination is the IPX network that the PortMaster is sending packets to. The gateway is the address of a router where packets are sent for forwarding to the destination.



Note – The gateway must not be set to an address on the PortMaster itself. The IPX node address is usually the MAC address on PortMaster products.

Example

```
Command> add ipxroute C009C901 00000002:A0B1C2D3E4F5 2 4
New route successfully added
```

See Also

delete ipxroute - page 16-16

show ipxroutes - page 16-25

add route

This command adds a static route to the IP route table on the PortMaster.



Caution – If you plan to use a static netmask, add it before setting any static routes that will be affected. However, Lucent recommends using the OSPF routing protocol instead of a netmask table for most routing configurations.

add route *Ipaddress*[/*NM*] *Ipaddress(gw)* *Metric*

<i>Ipaddress</i>	Destination address or network.
<i>/NM</i>	Netmask—a number from 1 to 32 preceded by a slash (/)—for example, /24.
<i>Ipaddress(gw)</i>	Gateway IP address.
<i>Metric</i>	Hop count to the remote destination. An integer from 1 to 15.

Usage

The destination is the IP address of the host or network for which the PortMaster is routing. The gateway is the address of a router where packets must be sent for forwarding to the destination.

Static routes support VLSM by means of this command, as shown in the example.



Note – The gateway IP address must not be set to an address on the PortMaster itself.

Example

The following example adds a route to the 192.168.1.32/27 subnet through gateway 192.168.1.1 with metric 2:

Command> **add route 192.168.1.32/27 192.168.1.1 2**

See Also

add netmask - page 16-23
set user-netmask - page 16-13
delete route - page 16-17
show ipxroutes - page 16-25

delete ipxroute

This command deletes a static route from the PortMaster IPX route table.

delete ipxroute *Ipxnetwork*

Ipxnetwork Destination IPX network number.

Usage

Only static routes can be deleted.

Example

Command> **delete ipxroute 192.168.1.32/27**
Route successfully deleted

See Also

add ipxroute - page 16-14
show ipxroutes - page 16-25

delete route

This command deletes a static route from the PortMaster IP static route table.

delete route *Ipaddress*[/*NM*] [*Ipaddress(gw)*]

<i>Ipaddress</i>	Destination IP address.
<i>/NM</i>	Netmask—a number from 1 to 32 preceded by a slash (/)—for example, /24.
<i>Ipaddress(gw)</i>	Gateway IP address.

Usage

Only static routes can be deleted.

Examples

Command> **delete route 192.168.7.0 192.168.7.1**
Route successfully deleted

See Also

add route - page 16-15

save route

This command writes the current PortMaster static IP and IPX route table to the nonvolatile memory of the PortMaster.

save route

Usage

save all can also be used.

Example

Command> **save route**
Static route table successfully saved
New configurations successfully saved.

RIP Commands



Unlike advanced routing protocols such as OSPF, RIP does not support VLSMs. RIP fails to propagate netmask information along with the IP addresses in its route information.

set default

When you are using RIP, this command sets all PortMaster interfaces to send and listen for default route information.

set default on|off|broadcast|listen

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

Usage

With this command set **on**, the PortMaster listens for default route information in RIP and OSPF messages, and if the PortMaster has a default route it is advertised to RIP and OSPF.

Example

Command> **set default on**

Default routing changed from off (no_broadcast,no_listen) to on (broadcast,listen)

See Also

set gateway - page 16-12

show global - page 2-28

set Ether0|S0|W1 rip

This command enables RIP on a specified interface.

set Ether0|S0|W1|all rip on|off|broadcast|listen

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Network hardwired asynchronous port.
<i>W1</i>	Network hardwired synchronous port.
all	All ports on the PortMaster.
on	The PortMaster sends and listens for RIP packets on this interface. This is the default.
off	The PortMaster neither sends nor listens for RIP packets on this interface.
broadcast	The PortMaster sends RIP packets on this interface.
listen	The PortMaster listens for RIP packets on this interface.

Usage

This command sets the PortMaster to send and listen for RIP packets—and IPX RIP packets if IPX is enabled—on the specified interface.

Using this command without specifying any interface or port sets *Ether0* by default.



Note – The command keyword **rip** replaces the keyword **routing** in ComOS release 3.6 and later. The keyword **routing** is still supported, but Lucent recommends that you use the keyword **rip**.

Example

Command> **set s0 rip on**
Routing for port S0 changed from listen to on (broadcast,listen)

See Also

set location rip - page 16-20
set user rip - page 16-21

set location rip

This command enables RIP for the selected location.

set location *Locname* rip on|off|broadcast|listen

<i>Locname</i>	Location name that is in the location table.
on	The PortMaster sends and listens for RIP packets from this network interface when it is established.
off	The PortMaster neither sends nor listens for RIP packets from this network interface when it is established. This is the default.
broadcast	The PortMaster sends 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.

Usage

Locations can have routing associated with them—for example, a dial-on-demand connection where the remote router is defined as a location on the local PortMaster. If routing is not set to **off** in an on-demand location, the PortMaster dials out to the location at boot time to perform routing, and hangs up when the idle timer expires. RIP packets do not affect the idle timer.



Note – The command keyword **rip** replaces the keyword **routing** in ComOS release 3.6 and later. The keyword **routing** is still supported, but Lucent recommends that you use the keyword **rip**.

Example

```
Command> set location hq rip on
hq routing changed from off to on (broadcast,listen)
```

See Also

set default - page 16-18

set user rip

This command enables RIP for a network user.

set user *Username* **rip** **on|off|broadcast|listen**

<i>Username</i>	Name of a network user.
on	The PortMaster sends and listens for RIP packets to the interface established when this user logs in.
off	The PortMaster neither sends nor listens for RIP packets on the interface established when this user logs in. This is the default.
broadcast	The PortMaster sends RIP packets to the interface established when this user logs in.
listen	The PortMaster listens for RIP packets from the interface established when this user logs in.

Usage

This command enables the PortMaster to send and listen for RIP packets to and from the remote host.



Note – The command keyword **rip** replaces the keyword **routing** in ComOS release 3.6 and later. The keyword **routing** is still supported, but Lucent recommends that you use the keyword **rip**.

Example

Command> **set user josey rip on**

Username: josey

Type: Dial-in Network User

Address: Negotiated

Netmask: 255.255.255.255

Protocol: PPP

Options: Broadcast, Listen,
Compression

MTU: 1500

Async Map: 00000000

See Also

add netuser - page 7-4

set default - page 16-18

Netmask Commands

The netmask commands configure a table of static netmasks that are used for routing over noncontiguous subnets in RIP. Read the information on setting static routes in the *PortMaster Configuration Guide*.



Caution – 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 overuse 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).

add netmask

This command adds a static netmask to the netmask table. Use caution with the static netmask table. Refer to the *PortMaster Configuration Guide* for more information.

add netmask *Ipaddress Ipmask*

Ipaddress IP address of the network.

Ipmask IP netmask used for the network.

Usage

You can have only one netmask per network when using RIP. The example shows the propagation of host routes for all dial-in clients with 192.168.8 addresses, instead of sending out a summarized network route for 192.168.8.0.



Caution – Be sure to add the netmask before setting any static routes that will be affected. If you change a static netmask, you must delete and then re-enter any affected static routes; otherwise these static routes are not valid.

Example

```
Command> add netmask 192.168.8.0 255.255.255.224  
New netmask successfully added
```

See Also

delete netmask - page 16-24

save netmask - page 16-24

show table netmask - page 16-31

delete netmask

This command deletes a static netmask from the netmask table.

delete netmask *Ipaddress*

Ipaddress IP address of the network.

Example

Command> **delete netmask 192.168.8.0**
Netmask successfully deleted

See Also

add netmask - page 16-23
save netmask - page 16-24
show table netmask - page 16-31

save netmask

This command saves the netmask table.

save netmask

Usage

After changing the netmask table, use this command to save the new netmask table to the nonvolatile memory of the PortMaster. The command **save all** can also be used.

Example

Command> **save netmask**
New configurations successfully saved.

See Also

add netmask - page 16-23
delete netmask - page 16-24
show table netmask - page 16-31

Routing Information Commands

The following commands display routing information on the console.

show ipxroutes

This command shows the IPX routing table.

show ipxroutes

Example

Command> show ipxroutes					
Network	Gateway	Flag	Met	Ticks	Interface
-----	-----	----	----	-----	-----
00001701	95C60100:0080AD06A39A	ND	2	2	ether0
95C60100	95C60100:00C005010923	NL	1	1	ether0

Explanation

Network	Destination IPX network.
Gateway	Gateway IPX address.
Flag	<ul style="list-style-type: none">• H—A host route.• N—A network route.• S—A static route that is either configured (permanent) or learned via a RADIUS Framed-Route (temporary).

- L—A route attached to an interface on the PortMaster.
 - D—A route dynamically learned via RIP or OSPF.
 - C—A changed route that has yet to be advertised to all interfaces.
 - O—An obsolete route scheduled for deletion.
- Met Metric—Hop count to the remote destination.
- Ticks The time required to send the packet to the destination network in 50ms increments.
- Interface The interface used to reach the gateway for this destination.

show propagation

This command shows any route propagation rule set with the **add propagation** command.

show propagation



Note – This command is available only on the PortMaster 3 and IRX products.

Example

Command> show propagation			
From Protocol	To Protocol	Metric	Propagation Filter
-----	-----	-----	-----
RIP	OSPF	0	filterone

Explanation

From Protocol	Source protocol of the routes to be propagated.
To Protocol	Destination routing protocol for route propagation.
Metric	Common metric used to translate from one protocol to the other. A metric of 0 indicates that the automatic rules in use in the PortMaster attempt to build a metric automatically. By default, all routes propagate, and the common metric is 0.
Propagation Filter	Name of the IP access filter added to the filter table with the add filter command and configured with the set filter command for use in the propagation rule.

show routes

This command shows the IP routing table. See the information on routing in the *PortMaster Configuration Guide* for a description of a routing table.

show routes [*String*|*Prefix/NM*]

<i>String</i>	Displays only routes that contain the matching <i>String</i> . For example, show routes local shows only routes that contain the matching <i>String</i> local in a search of the route database.
<i>Prefix/NM</i>	Displays routes only to the destination indicated by this IP address prefix <i>Prefix</i> and netmask <i>NM</i> . The netmask indicates the number of high-order bits in the IP prefix. <ul style="list-style-type: none"> Specify <i>Prefix</i> in dotted decimal notation. Specify <i>NM</i> as number from 1 to 32, preceded by a slash (/)—for example, /24.

Examples

Command> show routes local						
Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	-----	-----	-----	-----	-----	-----
0.0.0.0	0	192.168.96.2	local	NS	1	ether0
192.168.96.0	24	192.168.96.225	local	NL	1	ether0
10.2.5.0	24	192.168.96.2	local	NS	1	ether0

Command> show routes 192.168.1.0/24						
Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	-----	-----	-----	-----	-----	-----
192.168.1.0	24	192.168.2.31	rip	ND	2	ether0

Explanation

Destination	IP address of the host or network to which packets are sent.					
Mask	Netmask in use for the destination. Expressed in bits.					
Gateway	IP address of the directly connected host through which packets are forwarded to the destination.					
Source	Source of the route information:					
	local	Route learned from an interface on the PortMaster.				
	rip	RIP route learned from a connected network.				
	ospf	OSPF route learned from an internal neighbor.				
	ospf/E1	OSPF route learned from Type 1 external or Type 2 external routes.				
	ospf/E2					
	ospf/N1	OSPF route learned as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).				
	ospf/N2					
	ospf/IA	OSPF route originating from another area and learned via an area border router.				
	bgp/D	BGP route for the default network (network 0).				

	bgp/E	BGP route learned from an external neighbor.
	bgp/I	BGP route learned from an internal neighbor.
Flag		<ul style="list-style-type: none">• H—A host route.• N—A network route.• S—A static route that is either configured (permanent) or learned via a RADIUS Framed-Route (temporary).• L—A route attached to an interface on the PortMaster.• D—A route dynamically learned via a routing protocol.• C—A changed route that has yet to be advertised to all interfaces.• O—An obsolete route scheduled for deletion.
Met	Metric	Hop count to the remote destination.
Interface	Interface	used for forwarding packets to the gateway for the destination.
temp	Route learned from RADIUS.	Removed from the routing table when the user logs off.

show route to-dest

This command displays the route in the routing table that the PortMaster uses to forward an IP packet to the address *Ipaddress*.



show route to-dest *Ipaddress*

Ipaddress IP address of the remote destination.

Usage

This command can be useful for debugging routing problems.

Example

Compare the output of **show routes**, which displays the entire routing table for the PortMaster, with the more specific output of **show route to-dest**:

Command> **show routes**

Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	----	-----	-----	----	---	-----
0.0.0.0	0	192.198.110.2	local	NS	1	ether0
192.198.110.64	27	192.198.110.4	rip	ND	2	ether0
192.198.0.0	27	192.198.110.9	rip	ND	3	ether0
192.198.110.0	27	192.198.110.3	local	NL	1	ether0
192.168.32.0	24	192.198.110.9	rip	ND	2	ether0
10.0.0.0	8	192.198.110.9	rip	ND	3	ether0

Command> **show route to-dest 192.198.110.68**

Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	----	-----	-----	----	---	-----
192.198.110.64	27	192.198.110.4	rip	ND	2	ether0

Explanation

The displayed route in the example is a network route with a 27-bit netmask. The route covers IP addresses .65 through .94, where .64 is the network address and .95 is the broadcast address. The PortMaster displays this route because .68 is a member of this subnet.

See Also

show routes - page 16-27

show table netmask

This command shows the status of active and static special netmasks.

show table netmask

Usage

The netmask table also supports special netmasks that override the consolidation of hosts into subnets and subnets into networks in RIP broadcasts.

Example

Command> **show table netmask**

Active Netmasks:

Network	Netmask	Type
-----	-----	-----
172.17.0.0	255.255.255.0	Static
172.16.0.0	255.255.255.0	Dynamic

Stored Netmasks:

Network	Netmask
-----	-----
172.17.0.0	255.255.255.0

See Also

add netmask - page 16-23

delete netmask - page 16-24

save netmask - page 16-24

set user-netmask - page 16-13

show routes - page 16-27

This chapter describes the commands you use to configure the PortMaster when using the Open Shortest Path First (OSPF) routing protocol.

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

Large OSPF routing tables might require the PortMaster to be upgraded to 4MB or 16MB of memory. See your hardware installation guide for more information.



Note – After making changes to an OSPF configuration, you must use the **save all** and **reset ospf** commands to ensure that the changes take effect and are retained after PortMaster reboots.

Displaying OSPF Information

To display OSPF information on the console, use the following commands:

- **show global**—see page 2-28
- **show memory**—see page 2-31
- **show propagation**—see page 16-26
- **ifconfig**—see page 2-9, and this chapter
- **show ospf areas**
- **show ospf links**
- **show ospf neighbor**
- **show routes**
- **show table ospf**

For general information about using the command line interface, refer to Chapter 1, “Introduction.”

Summary of OSPF Commands

The OSPF commands in Table 17-1 allow you to configure the PortMaster to use the OSPF IP routing protocol.

Table 17-1 OSPF Commands

Command Syntax	
add ospf area <i>Area</i>	- see page 17-4
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 16-3
add route <i>Ipaddress/[NM] IPaddress(gw) Metric</i>	- see page 16-15
delete ospf area <i>Area</i>	- see page 17-5
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 16-3
ifconfig	- see page 2-9 and page 17-5
reset ospf	- see page 17-6
reset propagation	- see page 16-6
save ospf	- see page 17-7
set debug ospf-hello ospf-event ospf-spfcalc ospf-lsu ospf-lsa ospf-dbdesc ospf-error ospf-routing ospf-max on off	- see page 19-14
set default on off broadcast listen	- see page 16-18
set Ether0 ospf accept-rip on off	- see page 17-7
set Ether0 ospf on off [cost Number] [hello-interval Seconds] [dead-time Seconds]	- see page 17-8
set Ether0 S0 W0 user Username location Locname route-filter incoming outgoing Filtername	- see page 16-8

Table 17-1 OSPF Commands (Continued)

Command Syntax	
set location <i>Locname</i> <i>S0</i> <i>S10</i> <i>W1</i> user <i>Username</i> ospf on off [cost <i>Number</i>] [hello-interval <i>Seconds</i>] [dead-time <i>Seconds</i>]- see page 17-9 [nbma point-to-multipoint wan-as-stub-ptmp]	
set ospf area <i>Area</i> external on off	- see page 17-12
set ospf area <i>Area</i> md5 <i>Number</i> <i>String</i>	- see page 17-13
set ospf area <i>Area</i> nssa on off	- see page 17-14
set ospf area <i>Area</i> password <i>String</i>	- see page 17-15
set ospf area <i>Area</i> range <i>Prefix/NM</i> [advertise quiet off]	- see page 17-16
set ospf area <i>Area</i> stub-default-cost <i>Number</i>	- see page 17-17
set ospf enable disable	- see page 17-18
set ospf priority <i>Number</i>	- see page 17-19
set ospf router-id <i>Ipaddress</i> <i>Number</i>	- see page 17-20
show ospf areas	- see page 17-21
show ospf links [router network summary external nssa]	- see page 17-24
show ospf neighbor	- see page 17-27
show propagation	- see page 16-26
show routes [<i>String</i> <i>Prefix/NM</i>]	- see page 17-29
show table ospf	- see page 17-21

OSPF Commands

These commands are used for configuring OSPF routing protocol on the PortMaster.



Note – The order of OSPF configuration is very important. First enable the use of OSPF on the PortMaster, then set priority (and router ID if desired), then set areas and ranges, and finally enable OSPF for the interfaces. See the *PortMaster Routing Guide* for more information.

add ospf area

This command adds an area to the area tables of the router.

add ospf area *Area*

<i>Area</i>	The area specified in decimal or dotted decimal notation. A 32-bit number.
-------------	--

Usage

An OSPF area is a contiguous set of routers sharing network segments between them. Routers can be in more than one area, in which case they are area border routers. All routers must have at least one interface in area 0.0.0.0, known as the backbone area. Choose 0.0.0.0 if you have only one OSPF area.



Note – Lucent does not currently support the use of virtual links either to create a noncontiguous area or to allow an area border router to be indirectly attached to the backbone.

Example

```
Command> add ospf area 0.0.0.0  
New Area successfully added
```

delete ospf area

This command deletes an area from the area table of the router.

delete ospf area *Area*

Area The area specified in decimal or dotted decimal notation.
A 32-bit number.

Example

```
Command> delete ospf area 0.0.0.0  
Area successfully deleted
```

ifconfig

This command displays configuration values for all interfaces, and is described more fully on page 2-9. Examples of output are given here to illustrate how **ifconfig** shows OSPF state parameters for the interface, with the identity of the designated router (DR), backup designated router (BACKUP), and other (OTHER) routers on the network.

ifconfig

Examples

In the following example, this router is the designated router.

```
Command> ifconfig  
ether0: flags=40106<IP_UP,IPX_DOWN,BROADCAST,PRIVATE,OSPF>  
inet 192.168.200.131 netmask ffffffff broadcast 192.168.200.0  
area 192.168.200.0 ospf-state DR mtu 1500
```

In the following example, this router is the backup designated router.

```
Command> ifconfig  
ether0: flags=40016<IP_UP,IPX_DOWN,BROADCAST,OSPF>  
inet 192.168.200.130 netmask ffffffff broadcast 192.168.200.0  
area 192.168.200.0 ospf-state BACKUP mtu 1500
```

In the following example, this router is neither the designated router nor the backup designated router.

```
Command> ifconfig  
ether0: flags=40106<IP_UP,IPX_DOWN,BROADCAST,PRIVATE,OSPF>  
inet 192.168.200.129 netmask ffffffff broadcast 192.168.200.0  
area 192.168.200.0 ospf-state DROTHER mtu 1500
```

reset ospf

This command recreates startup conditions with OSPF.



Caution – Resetting OSPF can cause connections to be lost.

reset ospf

Usage

Use this command to remove the old MD5 authentication key numbers and secrets, and reset all active neighbors to use the new key numbers and secrets. You can also use this command to restart OSPF routing, allowing any configuration changes to take effect without a reboot of the PortMaster.

Example

```
Command> reset ospf  
Resetting OSPF
```

save ospf

This command writes any changes in the OSPF area table configuration to the nonvolatile memory of the PortMaster.

save ospf

Usage

The **save all** command can also be used, and is required if you want to save global OSPF information, such as the OSPF ID or the OSPF priority.

Example

```
Command> save ospf  
New configurations successfully saved.
```

set Ether0 ospf accept-rip

This command allows the propagation of RIP routes learned on this Ethernet interface into OSPF as Type 2 external routes.

set Ether0 ospf accept-rip on|off

<i>Ether0</i>	Ethernet interface.
on	Enables the propagation of RIP routes into OSPF.
off	Disables the propagation of RIP routes into OSPF. This is the default.

Usage

When routers run both RIP and OSPF on a network, the RIP routes learned from non-OSPF routers on a network can be translated into OSPF Type 2 external routes. Use this command when you need to enable the propagation of the learned RIP routes into OSPF areas.

However, if the RIP routes learned from the Ethernet interface come from routers that are always running OSPF as well as RIP, leave this command set to the **off** default to avoid duplicating the route information.

Example

```
Command> set ether0 ospf accept-rip on
Ether0 OSPF accept-rip changed from off to on
```

set Ether0 ospf on|off

This command enables or disables the OSPF protocol and allows optional settings on an Ethernet interface.

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

<i>Ether0</i>	Ethernet interface.
on	Enables OSPF on the Ethernet interface.
off	Disables OSPF on the Ethernet interface.
cost	Cost of sending a packet on the interface—also known as the link state metric.
<i>Number</i>	Assigned cost for the interface—a 16-bit number between 1 and 65535. The default is 1.
hello-interval <i>Seconds</i>	Interval that must elapse between the transmission of hello packets on the interface. The range is 10 to 120 seconds; the default is 10 seconds.
dead-time <i>Seconds</i>	Number of seconds the PortMaster waits after ceasing to receive a neighbor router's hello packets and before identifying the remote router as unreachable. The range is 40 to 1200 seconds; the default is 40 seconds.

Usage

The order of OSPF configuration is important. First set priority (and router ID if desired), then set areas and ranges, and finally enable OSPF for the interfaces.



Note – Make sure you set the same **cost** value, **hello-interval** value, and **dead-time** value for all routers attached to a common network.

Example

Command> **set ether0 ospf on cost 2 hello-interval 30 dead-time 90**
Ether0 ospf state changed from off to on.

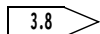
set location|S0|S10|W1|user ospf on|off

This command enables or disables the OSPF protocol and allows optional settings on any network hardwired port, location, or user.

set location *Locname*|*S0*|*S10*|*W1*|**user** *Username* **ospf on|off** [**cost** *Number*]
[**hello-interval** *Seconds*] [**dead-time** *Seconds*] [**nbma|point-to-**
multipoint|wan-as-stub-ptmp]



Note – Enter this command on one line, without any breaks. The line breaks shown here are due to the limited space available.



<i>Locname</i>	Location in the location table.
<i>S0</i>	Asynchronous port—configured as a network hardwired port.
<i>S10</i>	ISDN port—configured as a network hardwired port.
<i>W1</i>	Asynchronous port—configured as a network hardwired port.
<i>Username</i>	Login or network user in the user table.
on	Enables OSPF on the interface or for the location or user.
off	Disables OSPF on the interface or for the location or user.
cost	Cost of sending a packet on the interface—also known as the link state metric.
<i>Number</i>	Assigned cost for the interface—a 16-bit number between 1 and 65535. The default is 1.

hello-interval <i>Seconds</i>	Interval that must elapse between the transmission of hello packets on the interface. The range is 10 to 120 seconds; the default is 10 seconds.
dead-time <i>Seconds</i>	Number of seconds the PortMaster waits after ceasing to receive a neighbor router's hello packets and before identifying the remote router as unreachable. The range is 40 to 1200 seconds; the default is 40 seconds.
nbma	<p>Optionally sets the port as the interface to a nonbroadcast multiaccess (NBMA) Frame Relay network that has full mesh connectivity and all routers on the Frame Relay running OSPF.</p> <p>If you set the port to this value, a designated router is elected on the Frame Relay network, and overall OSPF traffic overhead is reduced.</p> <p>This is the default behavior.</p>
point-to-multipoint	<p>Optionally sets the port as the interface to a point-to-multipoint Frame Relay network. Use this setting when the Frame Relay network has partial mesh connectivity, or when all OSPF speakers on the network cannot communicate with each other.</p> <p>If you set the port to this value, the partially meshed Frame Relay network is modeled as a series of point-to-point interfaces.</p>
wan-as-stub-ptmp	<p>Optionally sets the port as the interface to a point-to-multipoint WAN-as-stub Frame Relay network. This setting works similarly to point-to-multipoint, but is used in cases when the PortMaster must interoperate with other-vendor equipment that implements a variant of point-to-multipoint.</p> <p>If you set the port to this value, the Frame Relay network is advertised as a stub network in the router link state advertisement (LSA), as opposed to the standard host route.</p>

Usage

The order of OSPF configuration is very important. First set priority (and router ID if desired), then set areas and ranges, and finally enable OSPF for the interfaces.

To determine whether to set the port as **point-to-multipoint** instead of **nbma**, use the **show routes** command and the **show ospf links** command. If **show routes** displays no routes learned over the Frame Relay interface, and **show ospf links** displays a large number of routes that might be available, configure the interface as **point-to-multipoint**.

To determine whether to set the port as **point-to-multipoint** or **wan-as-stub-ptmp**, use the **show ospf links** command to check the router LSAs of your neighbors on the Frame Relay network:

- If the LSAs show stub network link entries for the Frame Relay network, with the netmask for that network, configure the interface as **wan-as-stub-ptmp**.
- If the LSAs show the Frame Relay network as a host address, with a netmask of 255.255.255.255, configure the interface as **point-to-multipoint**.



Note – The values for each interface-specific setting must be the same on all routers attached to a common network.

Example

```
Command> set w1 ospf on cost 2 hello-interval 30 dead-time 120 wan-as-stub-ptmp
W1 ospf state changed from off to on.
```

See Also

show ospf links - page 17-24

show routes - page 17-29

set ospf area external

This command allows the propagation of external routes into the OSPF area.

set ospf area *Area* **external on|off**

<i>Area</i>	OSPF area address, specified in decimal or dotted decimal notation.
on	Designates this area as a transit area.
off	Designates this area as a stub area.

Usage

This command lets you define an area as a transit or stub area. Typically, the backbone area (0.0.0.0) is always defined as a transit area.

In contrast, a stub area does not attach to any area except the backbone, and has no exit other than to the backbone area. As a result, external routes are not propagated to stub areas, which must be given a default route to reach external destinations. Use the **set ospf area stub-default-cost** command to enable an area border router to create and inject default routes to stub areas.

Example

```
Command> set area 0.0.0.0 external off  
Area successfully updated
```

See Also

set area nssa - page 17-14
set ospf area stub-default-cost - page 17-17

set ospf area md5

This command sets the MD5 secret for the OSPF area.



Caution – Do not overwrite the current key number with the same number; doing so causes the secret to be lost immediately.

set ospf area *Area md5 Number String*

<i>Area</i>	OSPF area address, specified in decimal or dotted decimal notation.
<i>Number</i>	Key ID number associated with the MD5 secret. An integer from 1 to 255.
<i>String</i>	MD5 secret; an ASCII string of 1 to 16 characters.

Usage

All routers in the area must have the same key number that is associated with the MD5 secret.

When an MD5 key number and secret are changed, both the old and the new key numbers and secrets remain valid until a PortMaster **reboot** or a **reset ospf** command is issued. This feature facilitates the updating of area router information.

Example

```
Command> set ospf area 10.0.0.0 md5 6 kjtrewhut
Area successfully updated
```

set ospf area nssa

This command sets an OSPF area as a not-so-stubby area (NSSA), defined in RFC 1587.

set ospf area *Area* **nssa on|off**

<i>Area</i>	Address of the OSPF area being configured, specified in decimal or dotted decimal notation.
on	Sets the OSPF area as an NSSA.
off	Disables the area as an NSSA.

Usage

NSSAs are very similar to stub areas, except that Type 1 and Type 2 external routes can be learned from them. 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, default costs can be set for NSSAs, and external routes are not advertised into NSSAs.

Example

```
Command> set area 0.0.0.0 nssa on  
Area successfully updated
```

See Also

set area stub-default-cost - page 17-17

set ospf area password

This command sets the password for the OSPF area.

set ospf area *Area* **password** *String*

Area OSPF area address, specified in decimal or dotted decimal notation.

String Password; an ASCII string of from 1 to 8 characters.

Usage

This command sets a password or key to use when you are communicating to other routers in the area. Not specifying a password indicates that no password is set for the area.

Example

```
Command> set area 0.0.0.0 password gwKGft5%  
Area successfully updated
```

set ospf area range

This command sets the ranges of network addresses that define an OSPF area and, optionally, the type of route propagation.

set ospf area *Area* **range** *Prefix/NM* [**advertise**|**quiet**|**off**]

<i>Area</i>	OSPF area address, specified in decimal or dotted decimal notation.
<i>Prefix</i>	IP prefix shared by all IP addresses within the range.
<i>/NM</i>	Netmask that indicates the number of high-order bits in an IP address that must match those in <i>Prefix</i> for the address to belong within the area. The netmask value is a number from 1 to 30—for example, /24.
advertise	Summarizes routes to the networks within the range and propagates them to other areas. This is the default.
quiet	Does not summarize or propagate routes to the networks within the range.
off	Removes this range from the area.

Usage

This command is used on an area border router. When you use the **advertise** keyword, a summary link is propagated for that range. If you use the **quiet** keyword, the summary link is not propagated. You can add multiple ranges for an area by including them in a single command, as shown in the example.

A maximum of eight ranges can be given to a single area.



Note – Make sure that the ranges set with this command include the addresses for all PortMaster interfaces within this OSPF area.

Example

```
Command> set ospf area 0.0.0.0 range 192.168.1.0/24 range 192.168.200.0/24
Area successfully updated
```

set ospf area stub-default-cost

This command enables an area border router to create and advertise the default route (0.0.0.0) in a stub area or a not-so-stubby area (NSSA).

set ospf area *Area* **stub-default-cost** *Number*

<i>Area</i>	Address of the OSPF area being configured—specified in decimal or dotted decimal notation.
<i>Number</i>	Cost given to the default stub or NSSA route. This value is an integer from 0 to 15. Lower-cost routes are preferred. Setting <i>Number</i> to 0 disables the command.

Usage

Stub areas of an autonomous system can be defined with the **set ospf area external off** command. NSSAs can be defined with the **set ospf area nssa on** command. External advertisements are not injected into stub areas or NSSAs, and routing to external destinations is based on a default route for each stub area or NSSA. This command enables area border routers to inject the required default route into a stub area or NSSA, but no further.

Example

```
Command> set area 0.0.0.0 stub-default-cost 4
Area successfully updated
```

See Also

set ospf area external - page 17-12
set ospf area nssa - page 17-14

set ospf enable|disable

This command enables or disables the use of OSPF on the PortMaster.



Note – You must issue the **save all** and **reboot** commands immediately after issuing the **set ospf enable** command, before you can continue with any other OSPF configuration.

set ospf enable|disable

enable	Enables the use of OSPF on the PortMaster.
disable	Disables the use of OSPF on the PortMaster and frees the system memory used by OSPF, after the next reboot. This is the default.

Usage

OSPF must be enabled with this command before OSPF can be configured or used on the PortMaster.

Example

```
Command> set ospf enable  
OSPF will be enabled after next reboot
```

set ospf priority

This command sets the OSPF priority used to determine the designated and backup routers.

set ospf priority *Number*

Number Number from 0 to 255. Choosing 0 means that this router cannot be assigned as a designated router at any time. 0 is the default.

Usage

The priority must be set for each PortMaster running OSPF. If priorities tie, the router ID is used as a tie breaker, with the lower-number ID selected.

The router with the highest priority on a network segment becomes the designated router. This calculation is performed on each interface separately. For example, on a PortMaster IRX-211, the router might be the designated router on Ether0, but not on Ether1. The router with the second highest priority on a network segment is chosen as the backup designated router. The backup designated router takes over as designated router if the designated router is unable to perform its duties.

Examples

```
Command> set ospf priority 1  
OSPF priority changed from 5 to 1
```

set ospf router-id

This command sets the OSPF router address or ID number.

set ospf router-id *Ipaddress|Number*

Ipaddress The OSPF router address, specified in decimal or dotted decimal notation. If the router address is set to 0.0.0.0, it defaults to the router's Ethernet address.

Number A 32-bit number in decimal format. If the router address is set to 0, it defaults to the router's Ethernet address.

Usage

By default, the Ether0 IP address is used. Lucent strongly recommends that you set the default.

You must use the **save all** and **reboot** commands for the settings to take effect.



Caution – Be careful when using this feature. When you set a new router ID, the links belonging to an old router ID might take as long as 1 hour to expire, and routing instability can result during the expiration period.

Example

```
Command> set ospf router-id 192.168.1.1
OSPF router-id changed from 0.0.0.0 to 192.168.1.1
This change will take effect on the next reboot, if a 'save global' or
'save all' command issued before then.
```

See Also

set ospf priority - page 17-19

show ospf areas

These commands show information on the configured OSPF areas.

show ospf areas

show table ospf

Usage

The command **show table ospf** generates the same result as **show ospf areas**.

Examples

1. This example shows information on a transit area (External Routes = Yes) with simple password authentication and MD5 secret of **abcd**.

Command> **show ospf areas**

Area	Network Range	Authentication			External Routes	Stub
		Type	ID	Key		Default Cost
-----	-----	-----	---	-----	-----	-----
192.168.96.0	192.168.96.0/24 172.16.1.0/24 192.168.1.0/24	Password		abcd	Yes	N/A

2. This example shows information on a stub area (External Routes = No) with an MD5 secret of **defg**, a key ID of **15**, a default route **0.0.0.0**, and a cost of **3** being injected into the stub area.

Command> **show ospf areas**

Area	Network Range	Authentication			External Routes	Stub Default Cost
		Type	ID	Key		
-----	-----	-----	---	-----	-----	-----
192.168.97.0	192.168.97.0/24	MD5	15	defg	No	3
	172.16.1.0/24					
	192.168.1.0/24					

3. This example shows information on a stub area with no default route, a current MD5 secret of **defg**, and an MD5 key ID of **15** being injected into the stub area. This router has learned of two other keys since the last **reset ospf** or **reboot** command: key ID 5 with a secret of **oldkey**, and key ID 3 with a secret of **olderkey**.

Command> **show ospf areas**

Area	Network Range	Authentication			External Routes	Stub Default Cost
		Type	ID	Key		
-----	-----	-----	---	-----	-----	-----
192.168.97.0	192.168.97.0/24	MD5	15	defg	No	Not Set
	*172.16.1.0/24	MD5	5	oldkey		
	*192.168.1.0/24	MD5	3	olderkey		

4. This example shows information on a not-so-stubby area (NSSA) with no default route, a current MD5 secret of **research**, and an MD5 key ID of **2**.

Command> **show ospf areas**

Area	Network Range	Authentication			Area Type	Stub Default Cost
		Type	ID	Key		
-----	-----	-----	---	-----	-----	-----
192.168.32.0	*192.168.32.0/24	MD5	2	research	NSSA	Not set

Explanation

Area	Configured area.	
Network Range	The list of network ranges configured for the area. The list corresponds to entries given in the set ospf area range command (see page 17-16). An asterisk (*) in front of a network range shows that the range is active —indicating that one or more networks learned via OSPF intra-area routes fall into that range. The range, therefore, is supported by those networks and can be advertised as an interarea route to other OSPF areas.	
Authentication:	Type	Type of authentication: password or MD5.
	ID	Key ID number for the MD5 authentication.
	Key	The password or MD5 secret used to authenticate with neighbors in this area. See the set ospf area password command on page 17-15, and the set ospf area md5 command on page 17-13.
External Routes	Indicates if external routes are flooded into this area. A <i>No</i> value indicates that the area is a stub area. A <i>Yes</i> value indicates that the area is a transit area. See the set ospf area external command on page 17-12.	
Stub Default Cost	The cost given to the stub route.	

show ospf links

This command shows a summary of the OSPF database with one line per link state advertisement (LSA). By default, router links, network links, summary links, NSSA links, and external links are listed in summary form. For more detailed information use the options separately.

show ospf links [**router**|**network**|**summary**|**external**|**nssa**]

router	Provides more detail for router links.
network	Provides more detail for network links.
summary	Provides more detail for summary links.
external	Provides more detail for external links.
nssa	Provides more detail for NSSA external links.

Example

Command> **show ospf links**

Router Links for Area 0.0.0.0

Link ID	Advertising Router	Sequence	TOS	Ext	Age
-----	-----	-----	----	----	----
192.168.1.2	192.168.1.2	0x8000009d	No	Yes	459
192.168.16.6	192.168.16.6	0x800000b9	No	Yes	672
192.168.1.30	192.168.1.30	0x800000c5	No	Yes	1709
192.168.1.31	192.168.1.31	0x800000b8	No	Yes	398

Network Links for Area 0.0.0.0

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
-----	-----	-----	----	----	----	-----
192.168.1.30	192.168.1.30	0x800000d8	No	Yes	1641	24
192.168.16.2	192.168.1.31	0x80000e49	No	Yes	755	24
192.168.96.2	192.168.1.30	0x80000085	No	Yes	1641	24

Summary Links from others for Area 0.0.0.0

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
-----	-----	-----	----	----	----	-----
192.168.64.19	192.168.1.64	0x80000f2a	No	No	305	N/A
192.168.64.10	192.168.1.64	0x80000f19	No	No	305	N/A
0						
192.168.32.0	192.168.1.32	0x80000f08	No	No	1118	24
192.168.64.0	192.168.1.64	0x80000c2f	No	No	614	24

Summary Links from ourself for Area 0.0.0.0

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
-----	-----	-----	----	----	----	-----

External Links for All Areas

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
-----	-----	-----	----	----	----	-----
0.0.0.0	192.168.1.3	0x80000ab1	No	Yes	1001	0
192.168.132.0	192.168.1.32	0x800002f2	No	Yes	263	24
199.173.157.0	192.168.1.32	0x800002f2	No	Yes	884	24
192.168.23.0	192.168.1.6	0x80000a30	No	Yes	392	24
10.0.0.0	192.168.1.30	0x800001ad	No	Yes	478	8

Explanation

Link ID	For router links, the value in this column identifies the router address. For network links, this value identifies the designated router address. For summary and external links, this value identifies the network address advertised by the route that those links represent.
Advertising Router	OSPF router ID of the router that originated the link state advertisement.
Sequence	Link state sequence number used to detect old and duplicate link state advertisements (LSAs). Typically, the larger the sequence number, the newer the advertisement. When a router is rebooted, it might receive its old advertisements that are still known to other routers. If so, the router then brings its neighbors up-to-date by flooding the network with a new advertisement that has a sequence number larger than the number used in the old LSAs.
TOS	Type of service YES—This router supports TOS. NO—This router does not support TOS. Currently only the TOS 0 metric is supported. For more information on TOS-based routing, see RFC 1349 and RFC 2178.
Ext	External. This column indicates if external advertisements are to be flooded into the area.
Age	Age of the LSA links in seconds. Links age out in 1 hour (3600 seconds), unless they are refreshed with a new (larger) sequence number.
Mask	Netmask for the link ID.

show ospf neighbor

This command shows information about routers directly accessible through your network interfaces.

show ospf neighbor

Example

Command> **show ospf neighbor**

Interface	Area	Neighbor	State	Pri	IP Address	Last Hello	MD5 ID
-----	-----	-----	-----	---	-----	-----	----
ether0	192.168.1.0	192.168.1.1	2Way	0	192.168.1.1	9	N/A
ether1	10.0.0.0	10.0.0.1	Full/DR	2	10.0.0.1	3	2

Explanation

Interface	Interface used to learn about the neighbor.
Area	Area to which the interface belongs.
Neighbor	Router ID of the neighboring router. This ID might not match the neighboring router's IP address.
State	<p>OSPF state of the neighbor. The possible states follow:</p> <p>Down: Either the link to the neighbor is down, or this router is currently not receiving hello packets from the neighbor.</p> <p>Init: The connection with this neighbor has been reset, and this router has received no answering hello packet from the neighbor to indicate that the neighbor has received a hello packet from this router.</p> <p>2Way: This router received a hello packet from the neighbor that indicates the neighbor has received a hello packet from this router.</p>

Exstart: The router is beginning to form an adjacency with this neighbor. This state occurs only between a designated router (DR) or backup designated router (BDR) and the other routers on the network segment they service. Neighbors that are neither designated routers nor backup designated routers never advance beyond the 2Way state with each other.

Exchange: The router is exchanging current LSA information with the neighbor.

Loading: The router and the neighbor have finished exchanging information and are updating each other with the LSAs they need to share.

Full: One of the following three states indicating that the router and the neighbor are now up-to-date with each other, sharing fully identical LSA information:

- Full—This neighbor is not a designated router or backup designated router.
- Full/DR—This neighbor is the designated router.
- Full/BDR—This neighbor is the backup designated router.

Refer to the examples for the **ifconfig** command on page 17-5 to see a designated router or backup designated router.

Pri	Stated priority of the neighbor.
IP Address	IP address of the neighbor. This value might not match the router ID.
Last Hello	Time in seconds that has elapsed since the router last received a hello packet from the neighbor.
MD5 ID	A neighbor can be using one of many MD5 secrets. This field shows the ID of the corresponding MD5 secret that is being used by the neighbor. See the set ospf area md5 command on page 17-13 for more information.

show routes

This command shows the IP routing table. See the information on routing in the *PortMaster Configuration Guide*.

show routes [*String*|*Prefix/NM*]

- String*

Displays only routes that contain the matching *String*. For example, **show routes ospf** shows only routes that contain the matching string **ospf** in a search of the route database.
- Prefix/NM*

Displays routes only to the destination indicated by this IP address prefix *Prefix* and netmask *NM*. The netmask indicates the number of high-order bits in the IP prefix.
 - Specify *Prefix* in dotted decimal notation.
 - Specify *NM* as number from 1 to 32, preceded by a slash (/)—for example, /24.

Example

Command> show routes ospf						
Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	-----	-----	-----	-----	----	-----
192.168.96.0	32	172.31.96.2	ospf/E2	HD	4	ether0
192.168.133.0	24	172.31.96.2	ospf/IA	ND	3	ether0
192.168.32.0	32	172.31.96.2	ospf	HD	3	ether0

Explanation

Destination	IP address of the host or network to which packets are sent.	
Mask	Netmask in use for the destination.	
Gateway	IP address of the directly connected host through which packets are forwarded to the destination.	
Source	Source of the route information:	
	local	Route learned from an interface on the PortMaster.
	rip	RIP route learned from a connected network.
	ospf	OSPF route learned from an internal neighbor.
	ospf/E1 ospf/E2	OSPF route learned from Type 1 external or Type 2 external routes.
	ospf/N1 ospf/N2	OSPF route learned as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).
	ospf/IA	OSPF route originating from another area and learned via an area border router.
	bgp/D	BGP route for the default network (network 0).
	bgp/E	BGP route learned from an external neighbor.
	bgp/I	BGP route learned from an internal neighbor.
	temp	Route learned from RADIUS. Removed from the routing table when the user logs off.

Flag	<ul style="list-style-type: none"> • H—A host route. • N—A network route. • S—A static route that is either configured (permanent) or learned via a RADIUS Framed-Route (temporary). • L—A route attached to an interface on the PortMaster. • D—A route dynamically learned via RIP or OSPF. • C—A changed route that has yet to be advertised to all interfaces. • O—An obsolete route scheduled for deletion.
Met	Metric—hop count to the remote destination.
Interface	Interface used for forwarding packets to the gateway for the destination.

This chapter describes the commands you use to configure a PortMaster IRX or PortMaster 3 when you are using the Border Gateway Protocol (BGP) as a routing protocol. Lucent implements version 4 of BGP, as defined in RFC 1771, with updates from the draft standard number 5 of January 1997. Also supported are the BGP communities attribute, defined in RFC 1997, BGP autonomous system confederations, defined in RFC 1965, and BGP route reflection, defined in RFC 1966.

See the *PortMaster Routing Guide* for BGP configuration instructions and examples before attempting to configure BGP.

Because the size of BGP routing tables can become very large, Lucent recommends that you upgrade the PortMaster 3 to 32MB and PortMaster IRX to 16MB of memory. See your hardware installation guide for more information on adding memory.



Note – After making any changes to the BGP configuration, you must use the **save all** and **reset bgp** commands to ensure the changes take effect, and are retained after PortMaster reboots. If you are changing only peer-specific policy information, however, you need only reset the affected individual peers with the **reset bgp peer *Ipaddress*** command.

Displaying BGP Information

To display BGP information on the console, use the following commands:

- **show global**—see page 2-28
- **show memory**—see page 2-31
- **show propagation**—see page 16-26
- **show bgp memory**
- **show bgp next-hop**
- **show bgp paths**
- **show bgp peers**
- **show bgp policy**
- **show bgp summarization**

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of BGP Commands

BGP commands, shown in Table 18-1, allow you to configure the PortMaster for BGP routing.

Table 18-1 BGP Commands

Command Syntax	
add bgp peer <i>Ipaddress(src) Ipaddress(dest) ASN</i>	- see page 18-4
add bgp policy <i>Policyname</i>	- see page 18-5
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 16-3
add bgp summarization <i>Prefix/NM</i>	- see page 18-6
delete bgp peer <i>Ipaddress(dest)</i>	- see page 18-7
delete bgp policy <i>Policyname all</i>	- see page 18-5
delete bgp summarization <i>Prefix/NM</i>	- see page 18-9
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 16-3
reset bgp [peer <i>Ipaddress</i>]	- see page 18-10
reset propagation	- see page 16-6
save bgp	- see page 18-11
set bgp as <i>ASN</i>	- see page 18-11
set bgp cluster-id <i>Ipaddress</i>	- see page 18-12
set bgp cma <i>ASN</i>	- see page 18-13
set bgp connect-retry-interval <i>Seconds</i>	- see page 18-14
set bgp enable disable	- see page 18-14
set bgp hold-time <i>Seconds</i>	- see page 18-15
set bgp id <i>Ipaddress</i>	- see page 18-16

Table 18-1 BGP Commands (Continued)

Command Syntax	
set bgp igp-lockstep on off	- see page 18-16
set bgp keepalive-timer <i>Seconds</i>	- see page 18-17
set bgp peer <i>Ipaddress(src) Ipaddress(dest) ASN</i> [assume-default <i>Number</i>]] [confederation-member] [route-reflector-client] [normal] [always-next-hop] { easy-multihome [accept-policy <i>Policyname</i> all] [inject-policy <i>Policyname</i> all] [advertise-policy <i>Policyname</i> all]}	- see page 18-18
set bgp policy <i>Policyname</i> [before] <i>RuleNumber</i> permit deny include <i>Policyname</i> [if [prefix [exactly] <i>Prefix/NM</i>] [prefix-longer-than <i>NM</i>] [as-path <i>String empty</i>][community <i>Tag</i>]] [then [input-multi-exit-disc <i>Number</i> strip] [degree-of-preference <i>Number</i>] [local-pref <i>Number</i>] [output-multi-exit-disc <i>Number</i> strip] [next-hop <i>Ipaddress</i>] [community add replace strip <i>Tag</i>] [ignore-community-restrictions]]	- see page 18-23, page 18-29, page 18-33
set bgp policy <i>Policyname</i> blank	- see page 18-39
set bgp summarization <i>Prefix/NM</i> [as <i>ASN</i>] [cms <i>ASN</i>] [multi-exit-disc <i>Number</i>] [local-pref <i>Number</i>] [community <i>Tag</i>]	- see page 18-40
set debug bgp-fsm bgp-decision-process bgp-opens bgp-keepalives bgp-updates bgp-notifications bgp-errors bgp-packets bgp-max on off	- see page 19-2
show bgp memory	- see page 18-43
show bgp next-hop	- see page 18-44
show bgp paths [<i>Prefix/NM</i>] [verbose]]	- see page 18-46

Table 18-1 BGP Commands (Continued)

Command Syntax	
show bgp peers [verbose packets]	- see page 18-49
show bgp policy [<i>Polycyname</i>]	- see page 18-55
show bgp summarization [all]	- see page 18-56
show routes [<i>String</i> <i>Prefix/NM</i>]	- see page 18-58

BGP Commands

These commands are used for configuring the BGP routing protocol on the PortMaster.



Note – BGP is a complex protocol to configure. Consult the instructions and examples in the *PortMaster Routing Guide* before configuring BGP on a PortMaster.

add bgp peer

This commands creates entries on the PortMaster for BGP peers.

add bgp peer *Ipaddress(src)* *Ipaddress(dest)* *ASN*

<i>Ipaddress(src)</i>	Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.
<i>Ipaddress(dest)</i>	Destination address of the peer, specified in dotted decimal notation.
<i>ASN</i>	Unique number that identifies the autonomous system—a 16-bit number ranging from 1 to 65535.

Usage

Adding or Changing Peer Parameters. The **set bgp peer** command permits you to specify the parameters for an existing BGP peer without deleting that peer. However, the command assumes a “clean slate” for all parameters, and requires that you reenter them completely. For example, supposing you want to change your configuration of a peer 192.168.1.5 configured with the following command:

```
add bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client  
always-next-hop accept all inject all
```

If you now want to add **advertise all** as a policy statement to the command, you must specify all the original parameters together with the new parameter in the **set bgp peer** command, as follows:

```
set bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client  
always-next-hop accept all inject all advertise all
```

See Also

set bgp peer - page 18-18
set bgp policy (acceptance) - page 18-23
set bgp policy (injection) - page 18-29
set bgp policy (advertisement) - page 18-33

add bgp policy

This command creates a BGP policy for route acceptance, injection, or advertisement.

```
add bgp policy Policyname
```

Policyname Name of the policy to be created or deleted. 15-characters long.

Usage

Use the **delete bgp policy** command to delete a BGP policy. Define BGP policies with the **set bgp policy** commands.

Example

Command> **add bgp policy admit**
New BGP policy admit successfully added

See Also

delete bgp policy - page 18-8
set bgp policy (acceptance) - page 18-23
set bgp policy (injection) - page 18-29
set bgp policy (advertisement) - page 18-33

add bgp summarization

This command creates a BGP summarization entries.

add bgp summarization *Prefix/NM*

<i>Prefix</i>	Address prefix that you want to advertise to the BGP peers. Specified in dotted decimal notation.
<i>/NM</i>	Netmask that indicates the number of high-order bits in the address prefix. This is a number from 1 to 32, preceded by a slash (/)—for example, /24.

See Also

set bgp policy - page 18-23

delete bgp peer

This command deletes existing BGP peer entries on the PortMaster.

delete bgp peer *Ipaddress(dest)*

Ipaddress(src) Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.

Ipaddress(dest) Destination address of the peer, specified in dotted decimal notation.

Usage

When a peer deletion is in process, the message and countdown timer “Deletion in Progress. Countdown 216” are displayed in the Accept, Inject, and Advertise columns of the **show bgp peers** command. Deletion is complete when the countdown drops to zero.

Examples

Command> **delete bgp peer 172.16.0.0**
BGP peer to 172.16.0.0 successfully deleted

See Also

add bgp peer - page 18-6
set bgp peer - page 18-40

delete bgp policy

This command deletes a BGP policy.



Caution – Be careful when deleting BGP policy statements. Make sure that they are no longer needed for BGP route selection.

delete bgp policy *Policyname* | **all**

Policyname Name of the policy to be deleted. 15-characters long.

all Predefined policy that you can use to permit all routes to be accepted, injected, or advertised.

Usage

Use the **add bgp policy** command to create a BGP policy. Define BGP policies with the **set bgp policy** commands.

Example

```
Command> delete bgp policy admit  
BGP policy admit successfully deleted
```

See Also

add bgp policy - page 18-5
set bgp policy (acceptance) - page 18-29
set bgp policy (injection) - page 18-29
set bgp policy (advertisement) - page 18-33

delete bgp summarization

This command deletes a BGP summarization entry.

delete bgp summarization *Prefix/NM*

delete	Deletes an existing BGP summarization entry.
<i>Prefix</i>	Address prefix that you want to advertise to the BGP peers. Specified in dotted decimal notation.
<i>/NM</i>	Netmask that indicates the number of high-order bits in the address prefix. This is a number from 1 to 32, preceded by a slash (/)—for example, /24.

Usage

Examples

Command> **delete bgp summarization 172.16.0.0/16**
BGP summarization to 172.16.0.0/16 successfully deleted

See Also

add bgp summarization - page 18-6
set bgp policy - page 18-23
set bgp summarization - page 18-40

reset bgp

This command recreates start-up conditions for BGP.

reset bgp [**peer** *Ipaddress*]

peer	Resets only the session with the specified peer.
<i>Ipaddress</i>	IP address of the peer to be reset, specified in dotted decimal notation.

Usage

When used with no parameters, this command causes the PortMaster to lose all currently known BGP information except for configuration information. The PortMaster then rereads configuration information for BGP and reestablishes sessions with peers. This process is not instantaneous, but takes some time to finish.

After you use this command, BGP is in a transient state, during which the **show** commands are inoperative.

Using the command **set console** before entering this command allows you to see the message “BGP Reset Complete” on the console when the reset process is complete. Otherwise, the command provides no response.

When you use the command with the optional **peer** *Ipaddress*, only the configuration session with the specified peer is reset.

Example

Command> **reset bgp**

save bgp

This command writes any changes in the BGP tables to the nonvolatile memory of the PortMaster.

save bgp



Note – To specify that all configuration information is saved, including BGP and global parameters such as the local system and local BGP router ID, use the **save all** command instead.

Example

```
Command> save bgp
New configurations successfully saved.
```

set bgp as

This command sets the number of the autonomous system that the PortMaster is a member of.

set bgp as *ASN*

<i>ASN</i>	Unique number that identifies the autonomous system—a 16-bit number ranging from 1 to 65535.
------------	--

Usage

Autonomous system identifiers are supplied by the Internet Network Information Center (InterNIC). If autonomous system confederations are in use, this number identifies your BGP confederation's autonomous system to BGP peers outside the confederation.

Example

Command> **set bgp as 106**
BGP AS number changed from 0 to 106

set bgp cluster-id

This command identifies the PortMaster as a BGP route reflector in a cluster.

set bgp cluster-id *Ipaddress*

Ipaddress IP address in dotted decimal notation. It can be any IP address, but is typically the BGP ID of one of the route reflectors. Setting the cluster ID to 0.0.0.0 removes it, and disables the ability of this PortMaster to be a route reflector.

Route reflection is disabled by default.

Usage

An autonomous system can be divided into many clusters. Each cluster contains one or more internal peers configured as route reflectors, with the remaining peers in the cluster called route reflector clients. Peers configured as route reflectors in an autonomous system are fully meshed with each other, but the clients are configured as peers only with route reflectors in their cluster.

The same cluster ID must be set on each route reflector in a cluster, but cluster IDs are not set on the reflector clients.

Advantages of Clustering. The use of clusters reduces the traffic and CPU overhead compared with a fully meshed system. When compared to confederations, route reflector clusters are simpler to configure, but do not allow the degree of policy control that is possible across confederation boundaries. The primary advantage of route reflector clusters is that they allow the PortMaster to interoperate with BGP peers that are third-party routers without the ability to be configured into confederations.

For information about the effects of route reflection on BGP Policies, see page 18-22.

Example

Command> **set bgp cluster-id 1.2.3.4**
BGP Cluster ID changed from 0.0.0.0 to 1.2.3.4

set bgp cma

This command sets the number of the BGP confederation member autonomous system (CMAS) that the PortMaster is in.

set bgp cma *ASN*

ASN CMAS identifier—a 16-bit number ranging from 0 to 65535.
A value of 0 disables the CMAS configuration.

Usage

You can divide an autonomous system into multiple autonomous systems and group them into a single confederation. To external autonomous systems, the confederation appears as a single autonomous system. When confederations are in use, the PortMaster advertises this autonomous system identifier to BGP peers that are marked as confederation members in its configuration.

Choosing a value of zero disables use of confederations on this PortMaster. Confederations are disabled by default.

Example

Command> **set bgp cma 120**
BGP Confederation member AS number changed from 0 to 120

set bgp connect-retry-interval

This command sets the BGP connection retry interval for the PortMaster.

set bgp connect-retry-interval *Seconds*

Seconds Connection retry interval in seconds. The valid range is from 30 to 1000 seconds. The default is 120 seconds.

Usage

This command sets the interval at which the PortMaster attempts to open sessions to peers that are not fully established.

Example

Command> **set bgp connect-retry-interval 180**
BGP connect retry interval changed from 120 to 180

set bgp enable|disable

This command enables or disables the use of BGP on the PortMaster.



Note – You must issue the **save all** and **reboot** commands immediately after issuing the **set bgp enable** command, before you can continue with any other BGP configuration.

set bgp enable|disable

enable	Loads the BGP software upon the next PortMaster reboot.
disable	Disables the use of BGP upon the next reboot of the PortMaster, and frees the system memory used by BGP.
	This is the default.

Usage

You must enable BGP and reboot the PortMaster before configuring or using BGP. The **save all** and **reboot** commands must be issued after you use this command with either the **enable** or **disable** options.

set bgp hold-time

This command sets the BGP hold time interval for the PortMaster.

set bgp hold-time *Seconds*

Seconds Hold time interval in seconds. The valid range is from 30 to 1000 seconds. The default is 90 seconds.

Usage

This command sets the interval that the PortMaster waits between keepalive, update, or notification messages from a peer, before identifying the peer as no longer operational and dropping all information learned from that peer.

Example

```
Command> set bgp hold-time 120  
BGP hold time changed from 90 to 120
```

set bgp id

This command identifies the PortMaster as a BGP router.

set bgp id *Ipaddress*

Ipaddress PortMaster IP address, specified in dotted decimal notation.

Usage

The BGP identifier must be an IP address on the PortMaster. A setting of 0.0.0.0 removes the BGP ID.

Examples

Command> **set bgp id 192.168.0.1**
BGP ID changed from 0.0.0.0 to 192.168.0.1

set bgp igp-lockstep

This command enables or disables a feature that forces the PortMaster to match a route learned from internal BGP peers with a route learned from OSPF, RIP, static routing, or RADIUS before advertising the route to external peers.

set bgp igp-lockstep on|off

on Enables the matching feature.

off Disables the matching feature.

Usage

Normally, when the PortMaster learns a route from internal peers, it forwards the information to any external peers as soon as possible. Enabling the lockstep feature forces the PortMaster to wait until it finds a suitable IGP route—an OSPF, RIP, or static

route, or a static route via RADIUS—that supports the route before advertising it. An IGP route supports a BGP route if it has the same IP address and prefix as the BGP route.



Note – Exact matches only are allowed because simple default routes to support BGP routes can lead to network instability or lost packets.

Example

```
Command> set bgp igp-lockstep on  
bgp igp-lockstep changed from off to on
```

set bgp keepalive-timer

This command sets the BGP keepalive timer interval.

set bgp keepalive-timer *Seconds*

Seconds Keepalive timer interval in seconds. The valid range is from 30 to 1000 seconds. The default is 30 seconds.

Usage

This command sets the interval at which the PortMaster sends keepalive messages to its peers, to let them know it is still reachable.

Example

```
Command> set bgp keepalive-timer 45  
BGP keepalive timer changed from 30 to 45
```

set bgp peer

This command modifies entries on the PortMaster for BGP peers, and provide options that control how policies are implemented for route selection.

```
set bgp peer Ipaddress(src) Ipaddress(dest) ASN
[assume-default [Number]] [confederation-member]
[route-reflector-client] [normal] [always-next-hop]
{easy-multihome|[accept-policy Policyname|all]}
[inject-policy Policyname|all] [advertise-policy Policyname|all]}
```

<i>Ipaddress(src)</i>	Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.
<i>Ipaddress(dest)</i>	Destination address of the peer, specified in dotted decimal notation.
<i>ASN</i>	Autonomous system number of the peer. If this autonomous system is the same as that of the PortMaster, the peer is an internal peer; if it is different, the peer is an external peer. The autonomous system number is a 16-bit number ranging from 1 to 65535.
assume-default	Indicates that a default route to this external peer is created if the peer is up. You must assign a hop-count value to the default routes of different peers to specify a preferred peer.
<i>Number</i>	Hop count to advertise this default route. When multiple peers are configured with assume-default , the one with the lowest hop count is the preferred router for default-route forwarding. <i>Number</i> is a value from 1 to 15.
confederation-member	When specified, identifies a peer that is a member of the same confederation as the PortMaster. By default this keyword is not specified.

route-reflector-client When specified, identifies a peer as a **route reflector client** that the PortMaster forwards internal routes to. For the peer to be enabled as a route-reflector client, you must have configured the PortMaster with a cluster ID using the **set bgp cluster-id** command.

normal When specified, identifies a peer that is neither a confederation member nor a route-reflector client. By default **normal** is specified.

always-next-hop When specified, identifies the PortMaster as the **next hop** in any update packet sent to it from the peer, even if the PortMaster determines that it is not always the best next hop choice for this peer.

This option is useful when you know that this peer has connectivity to the PortMaster, but possibly not to the same devices that you would choose as a next hop—for example, in a partially meshed Frame Relay network.

By default **always-next-hop** is disabled.



Note – Standard BGP speaker behavior is to forward **next hop** information to internal peers without modification. The **always-next-hop** parameter enables this behavior to be changed. Therefore, when using the **always-next-hop** parameter, you must take care to ensure that inconsistent routing information is not propagated from multiple external peers to the autonomous system.

easy-multihome Enables an alternative method to policies for handling multihome paths from the PortMaster. The **easy-multihome** keyword restricts the BGP routing table to accept only paths through the remote autonomous system, and optionally through one additional autonomous system. Otherwise, the PortMaster uses the **assume-default** keyword to determine how to route packets.

accept-policy	<p>Enables a BGP policy <i>Policyname</i> whose criteria must be met for the PortMaster to accept any IP prefix from this peer as a viable BGP route. If a then degree-of-preference parameter is specified in the policy (see set bgp policy (acceptance) on page 18-23), it is used in place of any information learned from the path for path preference calculation purposes only. Advertisement filters indicate what the other peers are told.</p> <p>If not specified, and easy-multihome is not enabled for this peer, then nothing is accepted from this peer.</p>
all	<p>Predefined policy that you can use to permit all routes to be accepted, injected, or advertised.</p>
<i>Policyname</i>	<p>Name of a BGP policy statement defined by the set bgp policy command.</p>
inject-policy	<p>Enables a BGP policy <i>Policyname</i> whose criteria must be met for the PortMaster to place any IP address prefix received from this peer in the routing table. No then parameters are used in this policy.</p> <p>If not specified, and easy-multihome is not enabled for this peer, then nothing is injected from this peer into the routing table.</p>
advertise-policy	<p>Enables a BGP policy <i>Policyname</i> whose criteria must be met for the PortMaster to advertise any IP address prefix to this peer. The advertisement you set with the set bgp policy command indicates the metrics and any community information to advertise with the prefix.</p> <p>If not specified, and easy-multihome is not enabled for this peer, then nothing is advertised to this peer into the routing table.</p>

Usage

If no policy is defined, then the default behavior is **not** to accept, advertise, or inject any BGP routes. Therefore, when you define a peer you must do one of the following:

- Define explicit policies with the **set bgp policy** command to learn, use, or advertise routes.
- Use the predefined policy **all** to permit all routes to be accepted, used or advertised.
- Use the **easy-multihome** option.

Adding or Changing Peer Parameters. The **set bgp peer** command permits you to specify the parameters for an existing BGP peer without deleting that peer. However, the command assumes a “clean slate” for all parameters, and requires that you reenter them completely. For example, supposing you want to change your configuration of a peer 192.168.1.5 configured with the following command:

```
add bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client
always-next-hop accept all inject all
```

If you now want to add **advertise all** as a policy statement to the command, you must specify all the original parameters together with the new parameter in the **set bgp peer** command, as follows:

```
set bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client
always-next-hop accept all inject all advertise all
```

Requirement for Internal Peers to Be Fully Meshed. Unless route reflection is used, BGP requires that all BGP peers within an autonomous system or within a confederation member autonomous system (CMAS) be linked to each other. In this way, when one BGP peer learns an external route—path attributes and destination—it forwards this information to all its internal peers. Because they are fully meshed, each peer has the same information as its internal peers in the autonomous system and does not need to forward it again to them. If route reflector clusters are used, only the route reflectors—but not the route reflection clients—need to be fully meshed.

Length of Time Information Is Held Before Forwarding. When information is first learned from a peer, that information is held for at least 30 seconds before being forwarded to other peers as trustworthy and stable.

Peer Deletion. When a peer deletion is in process, the message and countdown timer “Deletion in Progress. Countdown 216” are displayed in the Accept, Inject, and Advertise columns of the **show bgp peers** command. Deletion is complete when the countdown drops to zero.

Effects of Route Reflection on BGP Policies. When a route reflector reflects an **internal route** that it learned from other internal peers either from or to a reflector client, the BGP policies for the cluster changes as follows:

- For advertisement policies, the route reflector ignores **then** portions and forwards every permitted route as learned. As a result, no modifications are made to the community, next hop, multiexit discriminator, or local preference values.
- For acceptance policies, any multiexit discriminator is advertised as it was originally received and is not modified upon acceptance.

This modified behavior applies **only** to reflected internal routes learned from other internal peers, and **not** to routes originating from the route reflector itself. The route reflector can generate routes from locally configured summarizations, or from routing information learned via external peers attached to the route reflector.

You can use policy statements to permit or deny certain routes from being reflected.

Examples

```
Command> set bgp peer 192.168.0.0 172.16.0.0 21 easy-multihome  
New BGP peer successfully added
```

```
Command> delete bgp peer 172.16.0.0  
BGP peer to 172.16.0.0 successfully deleted
```

See Also

set bgp policy (acceptance) - page 18-23
set bgp policy (injection) - page 18-29
set bgp policy (advertisement) - page 18-33

set bgp policy (acceptance)

This command creates a policy rule for admitting an IP prefix learned from a peer into a BGP database on the PortMaster for further consideration as a route.



Caution – The creation of long, complex lists of policy rules can adversely affect PortMaster CPU performance.

```
set bgp policy Polycname [before] RuleNumber
permit|deny|include Polycname
[if
[prefix [exactly] Prefix/NM]
[prefix-longer-than NM]
[as-path String|empty]
[community Tag]]
[then
[input-multi-exit-disc Number|strip]
[degree-of-preference Number]]
```

Polycname Name of an acceptance policy already created.

before Optionally inserts this BGP rule before an existing rule in the policy.

RuleNumber Number of a rule in the policy.

- Use the *RuleNumber* of an existing rule to replace that rule.
- Add this rule to the end of the list of rules by using a *RuleNumber* value that is 1 greater than the current largest rule number.
- A maximum of 160 rules is permitted in a policy. If more rules are needed, they can be added with the **include** *Polycname* option.

permit Allows the IP prefix into the BGP database if the criteria in the rule are met.

deny Prohibits the IP prefix from the BGP database if the criteria in the rule are met.

include <i>Polycynname</i>	Inserts an existing policy <i>Polycynname</i> into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.
if	<p>Compares the prospective IP prefix against corresponding elements specified after if in this rule. Specifying no if elements causes all prefixes to match the current rule.</p> <ul style="list-style-type: none"> • If all elements of the IP prefix match these if criteria, this rule is applied to the prefix and the prefix is either permitted or denied. • If the elements do not match, the list of policy rules is further scanned for a matching rule. • If no matches are found, the IP prefix is denied from the BGP database.
prefix <i>Prefix/NM</i>	<p>IP prefix <i>Prefix</i> and netmask <i>NM</i> to compare the prospective IP prefix against. The netmask indicates the number of high-order bits in the IP prefix.</p> <ul style="list-style-type: none"> • Specify <i>Prefix</i> in dotted decimal notation. • Specify <i>NM</i> as number from 1 to 32, preceded by a slash (/)—for example, /24. <p>By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.</p>
exactly	Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.
prefix- longer-than <i>NM</i>	When used with the deny keyword, prohibits from the BGP database any prospective IP address with a prefix containing more high-order bits than are specified by the netmask <i>NM</i> .
as-path <i>String</i>	<p>Autonomous system path <i>String</i> to compare the prospective IP prefix against.</p> <p><i>String</i> is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.</p>

When *String* is compared to an autonomous system path **sequence**, the order of the sequence must match the order of *String*. When *String* is compared to an autonomous system path **set**, the **set** is put in ascending numerical order, and then matched against *String*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *String*.

The following special characters have the following meaning in the expression:

- An asterisk (*) matches one or more entries in the autonomous system sequence.
- A question mark (?) matches any single item in the autonomous system sequence.

empty

Value for *String* that matches only paths containing no autonomous system path information.

Use **as-path empty** only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.

community

Identifier *Tag* that categorizes a group of destinations to compare the prospective IP prefix against.

See RFC 1997 for more information on a BGP community.

Tag

Thirty-two-bit number that indicates a destination category in one of the following forms:

- One 32-bit value identifying the autonomous system of the destination
- Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *Tag*, replace the second 16-bit value with the keyword **any**.
- One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:

	no-export	Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.
	no-advertise	No destinations. Do not advertise this route.
	no-export-subconfed	Internal destinations only. Advertise this route only to internal BGP peers.
	The restrictions imposed by these reserved community keywords do not apply to the PortMaster originating this information.	
then	Assigns the following metric or metrics to any IP prefix selected for acceptance by the rule.	
input-multi-exit-disc <i>Number</i> strip	Assigns an arbitrary <i>Number</i> for the learned multiexit discriminator, overriding any that is learned from the peer. <i>Number</i> is a 32-bit integer. The strip keyword causes any multiexit discriminator information learned from a peer to be ignored.	
	input-multi-exit-disc can be abbreviated as imed in this command.	
	Lower numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.	
degree-of-preference <i>Number</i>	Assigns a degree-of-preference <i>Number</i> to a route. <i>Number</i> is a 32-bit integer.	
	degree-of-preference can be abbreviated as dop in this command	
	Higher numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example.	

If you do not assign a degree of preference to the IP prefix, one of the following values is assigned by default:

- If the route comes from an internal peer, the learned local preference number is assigned.
- If the route comes from an external peer, *Number* is based on the autonomous system path length, with a shorter path being preferred.

Usage

A BGP **policy** is a list of rules that restrict the BGP routes your PortMaster accepts from its peers, uses, and advertises to its peers. You can use the **easy-multihome** alternative to policies—or **accept-policy all** to accept all routes—when you add each BGP peer to your peer group, or you can define your own policies.

A PortMaster uses an **acceptance policy** to determine whether to admit an IP prefix received in a update from a BGP peer into its BGP database for further consideration as a route. If the PortMaster accepts the IP prefix, it uses an **injection policy** to determine whether to use the route to forward packets, and an **advertisement policy** to determine whether to advertise the route to its BGP peers.

You can create any number of acceptance, injection and advertisement policies.

Performing Three Functions in One Policy. You can create separate policies for each function, or create one policy to perform all three functions.

Permitting or Denying All Prefixes. If you define a rule that contains no **if** or **then** clauses, the rule universally permits or denies all prefixes, with no modification.

Applying and Saving a Rule. After adding or changing a rule in a BGP policy, use one of the following commands to apply and save the modified policy:

- Use **reset bgp peer** *Ipaddress(dest)* to reset only those peers that use a policy.
- Use **reset bgp** to reset all peers.

Removing a Rule. Specifying only the rule number *RuleNumber* in the command, as in **set bgp policy policyname 1**, removes that rule from the BGP policy.

Creating a Common Policy. You can create a common BGP policy for inclusion in other BGP policies. For example:

1. Create and define a common BGP policy as follows:

```
add bgp policy permit1011  
  
set bgp policy permit1011 1 permit if prefix 10.0.0.0/8  
  
set bgp policy permit1011 2 permit if prefix 11.0.0.0/8
```

2. Include this policy by reference in another policy as follows:

```
set bgp policy otherone 5 include permit1011
```

This command inserts the statements of the **permit1011** policy at line 5 of the **otherone** policy.

Policy inclusions can be nested to a maximum depth of 10 levels. Any inclusions beyond the 10th level are ignored.

Reducing the Number of Advertised Routes. Some BGP routes received by your PortMaster might not be summarized. Unsummarized routes can include IP prefixes containing as many as 32 high-order bits—many specific addresses rather than fewer route summaries. If your BGP policy rules accept such routes into your BGP database, you can propagate extremely large numbers of routes to your BGP peers and possibly overwhelm them. To avoid this problem, use the **prefix-longer-than** keyword in a BGP acceptance policy to deny IP prefixes with a netmask longer than a particular *NM* value. Specifying **prefix-longer-than 16**, for example, would be highly effective for this purpose.

For more information about the effects of route reflection on BGP policies, see page 18-22.

Example

```
Command> set bgp policy acdeg10 1 permit then degree-of-preference 10  
Added rule 1 in policy acdeg10  
BGP policy acdeg10 updated
```

set bgp policy (injection)

This command creates a policy rule for injecting IP prefixes into the routing table—displayed by the **show route** command—that the PortMaster uses to forward packets it receives to their ultimate destination.



Caution – The creation of long, complex lists of policy rules can adversely affect PortMaster CPU performance.

```
set bgp policy Policyname [before] RuleNumber
permit|deny|include Policyname
if
  [prefix [exactly] Prefix/NM]
  [as-path String|empty]
  [community Tag]
```

<i>Policyname</i>	Name of an injection policy already created.
before	Optionally inserts this BGP rule before an existing rule in the policy.
<i>RuleNumber</i>	Number of a rule in the policy. Use the <i>RuleNumber</i> of an existing rule to replace that rule. Add this rule to the end of the list of rules by using a <i>RuleNumber</i> value that is 1 greater than the current largest rule number.
permit	Allows the IP prefix into the PortMaster routing table if the criteria in the rule are met.
deny	Prohibits the IP prefix from the PortMaster routing table if the criteria in the rule are met.
include <i>Policyname</i>	Inserts an existing policy <i>Policyname</i> into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.

if	<p>Compares the prospective IP prefix against corresponding elements specified after if in this rule. Specifying no if elements causes all prefixes to match the current rule.</p> <ul style="list-style-type: none"> • If all elements of the IP prefix match these if criteria, this rule is applied to the prefix and the prefix is either added or not added to the PortMaster routing table. • If the elements do not match, the list of policy rules is further scanned for a matching rule. • If no matches are found, the IP prefix is prohibited from the routing table.
prefix <i>Prefix/NM</i>	<p>IP prefix <i>Prefix</i> and netmask <i>NM</i> to compare the prospective IP prefix against. The netmask indicates the number of high-order bits in the IP prefix.</p> <ul style="list-style-type: none"> • Specify <i>Prefix</i> in dotted decimal notation. • Specify <i>NM</i> as number from 1 to 32, preceded by a slash (/)—for example, /24. <p>By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.</p>
exactly	<p>Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.</p>
as-path <i>String</i>	<p>Autonomous system path <i>String</i> to compare the prospective IP prefix against.</p> <p><i>String</i> is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.</p> <p>When <i>String</i> is compared to an autonomous system path sequence, the order of the sequence must match the order of <i>String</i>.</p>

When *String* is compared to an autonomous system path **set**, the **set** is put in ascending numerical order, and then matched against *String*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *String*.

The following special characters have the following meaning in the expression:

- An asterisk (*) matches one or more entries in the autonomous system sequence.
- A question mark (?) matches any single item in the autonomous system sequence.

empty

Value for *String* that matches only paths containing no autonomous system path information.

Use **as-path empty** only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.

community

Identifier *Tag* that categorizes a group of destinations to compare the prospective IP prefix against.

See RFC 1997 for more information on a BGP community.

Tag

Thirty-two-bit number that indicates a destination category in one of the following forms:

- One 32-bit value identifying the autonomous system of the destination
- Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *Tag*, replace the second 16-bit value with the keyword **any**.
- One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:

no-export	Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.
no-advertise	No destinations. Do not advertise this route.
no-export-subconfed	Internal destinations only. Advertise this route only to internal BGP peers.

The restrictions imposed by these reserved community keywords do not apply to the PortMaster originating this information.

Usage

A BGP **policy** is a list of rules that restrict the BGP routes your PortMaster accepts from its peers, uses, and advertises to its peers. You can use the **easy-multihome** alternative to policies—or **inject-policy all** to use all routes—when you add each BGP peer to your peer group, or you can define your own policies.

A PortMaster uses an **injection policy** to determine whether to add an IP prefix to its routing table, as shown in the output of the **show route** command. The PortMaster has already accepted this IP prefix for consideration as a BGP route via an **acceptance policy**. If the PortMaster injects the route, it will use the route to forward packets. The PortMaster also subjects the IP prefix to an **advertisement policy** to determine whether to share the route with its BGP peers.

An injection policy allows the PortMaster to receive and forward BGP routing information, but to forward packets based on simpler criteria. For example, you might want to forward packets only on routes received from OSPF or on a configured default route.

For more information about creating policies, see page 18-27.

Example

```
Command> add bgp policy inj.one 1 permit if prefix 172.16.0.0/16 community 108 108
Added rule 1 in policy inj.one
BGP policy inj.one updated
```


set bgp policy (advertisement)

This command creates a policy rule for advertising an IP prefix that the PortMaster learned from another peer to a BGP internal or external peer.



Caution – The creation of long, complex lists of policy rules can adversely affect PortMaster CPU performance.

```
set bgp policy Policyname [before] RuleNumber
permit|deny|include Policyname
[if
[prefix [exactly] Prefix/NM]
[as-path String|empty]
[community Tag]]
[then
[local-pref Number]
[output-multi-exit-disc Number|strip]
[next-hop Ipaddress]
[community add|replace|strip Tag]
[ignore-community-restrictions]]
```

<i>Policyname</i>	Name of an advertisement policy already created.
before	Optionally inserts this BGP rule before an existing rule in the policy.
<i>RuleNumber</i>	Number of a rule in the policy. <ul style="list-style-type: none">• Use the <i>RuleNumber</i> of an existing rule to replace that rule.• Add this rule to the end of the list of rules by using a <i>RuleNumber</i> value that is 1 greater than the current largest rule number.
permit	Allows the IP prefix to be advertised if the criteria in the rule are met.
deny	Prohibits the IP prefix from being advertised if the criteria in the rule are met.

include <i>Polycyname</i>	Inserts an existing policy <i>Polycyname</i> into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.
if	<p>Compares the prospective IP prefix against corresponding elements specified after if in this rule. Specifying no if elements causes all prefixes to match the current rule.</p> <ul style="list-style-type: none">• If all elements of the IP prefix match these if criteria, this rule is applied to the prefix and the prefix is either advertised or not advertised.• If the elements do not match, the list of policy rules is further scanned for a matching rule.• If no matches are found, the IP prefix is not advertised.
prefix <i>Prefix/NM</i>	<p>IP prefix <i>Prefix</i> and netmask <i>NM</i> to compare the prospective IP prefix against. The netmask indicates the number of high-order bits in the IP prefix.</p> <ul style="list-style-type: none">• Specify <i>Prefix</i> in dotted decimal notation.• Specify <i>NM</i> as number from 1 to 32, preceded by a slash (/)—for example, /24. <p>By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.</p>
exactly	Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.

as-path <i>String</i>	<p>Autonomous system path <i>String</i> to compare the prospective IP prefix against.</p> <p><i>String</i> is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.</p> <p>When <i>String</i> is compared to an autonomous system path sequence, the order of the sequence must match the order of <i>String</i>. When <i>String</i> is compared to an autonomous system path set, the set is put in ascending numerical order, and then matched against <i>String</i>. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to <i>String</i>.</p> <p>The following special characters have the following meaning in the expression:</p> <ul style="list-style-type: none">• An asterisk (*) matches one or more entries in the autonomous system sequence.• A question mark (?) matches any single item in the autonomous system sequence.
empty	<p>Value for <i>String</i> that matches only paths containing no autonomous system path information.</p> <p>Use as-path empty only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.</p>
community	<p>Identifier <i>Tag</i> that categorizes a group of destinations to compare the prospective IP prefix against.</p> <p>See RFC 1997 for more information on a BGP community.</p>

Tag	<p>Thirty-two-bit number that indicates a destination category in one of the following forms:</p> <ul style="list-style-type: none">• One 32-bit value identifying the autonomous system of the destination.• Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community <i>Tag</i>, replace the second 16-bit value with the keyword any.• One of the following reserved community keywords that restrict route advertisement for peers receiving the route information: <table><tr><td>no-export</td><td>Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.</td></tr><tr><td>no-advertise</td><td>No destinations. Do not advertise this route.</td></tr><tr><td>no-export-subconfed</td><td>Internal destinations only. Advertise this route only to internal BGP peers.</td></tr></table> <p>The restrictions imposed by these reserved community keywords do not apply to the PortMaster originating this information.</p>	no-export	Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.	no-advertise	No destinations. Do not advertise this route.	no-export-subconfed	Internal destinations only. Advertise this route only to internal BGP peers.
no-export	Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.						
no-advertise	No destinations. Do not advertise this route.						
no-export-subconfed	Internal destinations only. Advertise this route only to internal BGP peers.						
then	<p>Assigns the following metric or set of metrics to any IP prefix selected for advertisement before advertising it.</p>						

local-pref *Number* Assigns an arbitrary rating *Number* to an external route for advertisement to internal or confederation-member peers only. *Number* is a 32-bit integer.

local-pref can be abbreviated as **lp** in this command.

Higher numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example.

If you do not assign a local preference rating to the IP prefix, one of the following values is assigned by default:

- If the route comes from an internal peer, the learned local preference number is assigned.
- If the route comes from an external peer, *Number* is based on the autonomous system path length, with a shorter path being preferred.

**output-multi-
exit-disc
Number | strip**

Assigns an arbitrary rating *Number* for the multiexit discriminator to an external route for advertisement to external or confederation member peers only. *Number* is a 32-bit integer.

A multiexit discriminator configured in a policy takes precedence over one configured in a route summarization.

output-multi-exit-disc can be abbreviated as **omed** in this command.

Lower numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.

If you do not assign a multiexit discriminator, no value is sent unless the PortMaster is advertising one of its own summarizations that specifies a multiexit discriminator. In this case, the value specified in the **add bgp summarization** command is used if none is present in the policy.

	To avoid advertising any multiexit discriminator, use the strip keyword.
next-hop <i>Ipaddress</i>	Assigns the IP address to advertise as the next hop. If you do not assign a value, a value is computed automatically for the best possible next hop to reach this route. However, if this peer is configured with the set peer always-next-hop on option, this router's local IP address is always used as the next hop.
add	Adds the community categories identified in <i>Tag</i> to the IP prefix to be advertised.
replace	Replaces the community categories identified in the community <i>Tag</i> of the IP prefix to be advertised with new <i>Tag</i> values.
strip	Removes existing community categories from the IP prefix to be advertised.
ignore-community-restrictions	Instructs the PortMaster to ignore the restrictive keywords no-advertise , no-export , and no-export-subconfed when advertising this route to a peer. Use this keyword in the rule to override these restrictions received from other peers.

Usage

A BGP **policy** is a list of rules that restrict the BGP routes your PortMaster accepts from its peers, uses, and advertises to its peers. You can use the **easy-multihome** alternative to policies—or **advertise-policy all** to advertise all routes—when you add each BGP peer to your peer group, or you can define your own policies.

A PortMaster uses an **advertisement policy** to determine whether to share an IP prefix as a route with its internal and external BGP peers. The PortMaster has already accepted this IP prefix for consideration as a BGP route via an **acceptance policy**. The PortMaster also subjects the IP prefix to an **injection policy** to determine whether to add an IP prefix to its routing table, as shown in the output of the **show route** command.

For more information about creating policies, see page 18-27.

Examples

```
Command> add bgp policy adver.one 1 permit if prefix 172.16.0.0/16
then community add 108 108
Added rule 1 in policy adver.one
BGP policy adver.one updated
```

```
Command> set bgp policy adver.one 2 permit then local-pref 5 community
add 108 108
Added rule 2 in policy adver.one
BGP policy adver.one updated
```

set bgp policy blank

This command deletes all policy rules from a BGP policy list.

```
set bgp policy Policyname blank
```

Policyname Name of the policy created.

Usage

Use the **set bgp policy blank** command to remove all the policy rules from a BGP policy list.

Example

```
Command> set bgp policy admit blank
Removed all rules from BGP policy admit
```

See Also

```
delete bgp policy - page 18-8
set bgp policy (acceptance) - page 18-23
set bgp policy (advertisement) - page 18-33
set bgp policy (injection) - page 18-29
```

set bgp summarization

This command modifies a BGP summarization entry that indicates how Interior Gateway Protocol (IGP) routing information from OSPF, RIP, or static routing is forwarded into BGP for advertisement to other BGP peers.

```
set bgp summarization Prefix/NM
[as ASN] [cma ASN] [multi-exit-disc Number]
[local-pref Number] [community Tag]
```

<i>Prefix</i>	Address prefix that you want to advertise to the BGP peers in dotted decimal notation.
<i>/NM</i>	Netmask that indicates the number of high-order bits in the address prefix. This is a number from 1 to 32, preceded by a slash (/)—for example, /24.
as	Autonomous system that receives this summarization. Include your local autonomous system number in this list to enable the summarization to go to local internal peers. You can list up to 14 autonomous systems.
<i>ASN</i>	Autonomous system number.
cma	Your confederation member autonomous system (CMAS) that receives this summarization. Include your CMAS number in this list to enable the summarization to go to internal peers in your CMAS.
multi-exit-disc <i>Number</i>	<p>Assigns an arbitrary rating <i>Number</i> to an external route for advertisement to external or confederation-member peers only. <i>Number</i> is a 32-bit integer.</p> <p>multi-exit-disc can be abbreviated as med in this command.</p> <p>Lower numbers indicate an increased preference for a specific route. Use this metric to discriminate among multiple exit or entry points between the same pair of neighboring autonomous systems.</p>

If you do not assign a multiexit discriminator, the value 1 is assigned by default.

A multiexit discriminator configured in a policy takes precedence over one configured in this route summarization.

To explicitly prevent advertisement of a multiexit discriminator for IP prefixes matching this rule, set this keyword to zero (0). The PortMaster never forwards a 0 value of this metric to any peer, even if 0 was explicitly received from a peer.

local-pref *Number* Assigns an arbitrary rating *Number* to an external route for advertisement to internal or confederation-member peers only. *Number* is a 32-bit integer.

local-pref can be abbreviated as **lp** in this command.

Higher numbers indicate an increased preference for a specific route when more than one route exists. Use this metric to screen a particular autonomous system from your map of routes, for example.

If you do not assign a local preference rating to the IP prefix, one of the following values is assigned by default:

- If the route comes from an internal peer, the learned local preference number is assigned.
- If the route comes from an external peer, *Number* is based on the autonomous system path length, with a shorter path being preferred.

A local preference value configured in a policy takes precedence over one configured in this summarization.

community Advertises the 32-bit community attribute, defined by *Tag*, along with this summarization.

Tag

Thirty-two-bit number that indicates a destination category in one of the following forms:

- One 32-bit value identifying the autonomous system of the destination.
- Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *Tag*, replace the second 16-bit value with the keyword **any**.

One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:

- | | |
|----------------------------|--|
| no-export | Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system. |
| no-advertise | No destinations. Do not advertise this route. |
| no-export-subconfed | Internal destinations only. Advertise this route only to internal BGP peers. |

The restrictions imposed by these reserved community keywords do not apply to the PortMaster originating this information.



Note – Whenever you modify any BGP summarization setting, you must respecify all settings.

Usage

BGP originates to peers only the routing information that is explicitly indicated by—and supported by—the interior routing protocols in use (OSPF, RIP, static routes, or directly attached routes). These special advertisements are called **summarizations**, and must be explicitly configured in most cases.

The settings you configure for community, local preference, and multiexit discriminator in this summarization command interact with advertisement policy definitions as follows:

- The advertisement policy definition overrides any values for local preference and multiexit discriminator.
- If the advertisement policy definition adds new community categories (**community add**), that information is added to the community information specified in the summarization.
- If the advertisement policy definition replaces community categories (**community replace**), it replaces any community information specified in the summarization.

To help provide stability in the Internet, summarizations are advertised only when supported by one or more specific routes that exist for at least 30 seconds before the advertisement.

Example

```
Command> set bgp summarization 172.16.0.0/16 multi 55 as 2 as 3 as 4
BGP summarization successfully added
```

See Also

set bgp policy - page 18-23

show bgp memory

This command displays information on BGP memory usage.

show bgp memory

Example

```
Command> show bgp memory
BGP is using a total of 7024480 bytes of memory for 42313 destinations:
```

```
Destination-specific use:    3296384 bytes
Peer-specific use:          3728096 bytes
```

Explanation

Memory usage is an important concern when you are running BGP because of the large number of routes that are stored in the BGP database.

Destination-specific use: 3,296,384	This value depends on the total number of IP prefixes accepted in the network layer reachability information (NLRI) from all peers, whether or not multiple peers provide the same prefix. Destination-specific bytes of memory are normally consumed only once for each unique destination.
Peer-specific use: 3,728,096 bytes	This value depends on the total amount of information accepted from all peers. Redundant information from multiple peers can increase this value.

show bgp next-hop

This command displays the known BGP next hop addresses and gateways to them.

show bgp next-hop

Example

Command> show bgp next-hop					
Next Hop	Gateway	Src Addr to it	Source	Metric	Interface
-----	-----	-----	-----	-----	-----
192.168.1.2	172.16.96.2	172.16.95.1	ospf/IA	1	ether0
172.16.96.129	172.16.96.129	172.16.96.1	local	1	ether0
172.16.96.133	172.16.96.129	172.16.96.1	local	1	ether0

Explanation

Use this command to conveniently determine where packets go when forwarded. The information displayed is based on entries in the routing table that are used to forward BGP packets to their destinations.

Next Hop	Next hop address, learned from the next hop attribute in a BGP route.	
Gateway	Address of the directly adjacent router that forwards packets so that they reach the next hop. If the next hop and gateway addresses are the same, the next hop router is directly adjacent to the PortMaster.	
Src Addr to it	Local network address of the interface on the PortMaster that is used to reach the next hop.	
Source	Origin of the route information:	
	local	Route learned from an interface on the PortMaster.
	rip	RIP route learned from a connected network.
	ospf	OSPF route learned from an internal neighbor.
	ospf/E1 ospf/E2	OSPF route learned from Type 1 external or Type 2 external routes.
	ospf/N1 ospf/N2	OSPF learned route as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).
	ospf/IA	OSPF route originating from another area and learned via an area border router.
	bgp/D	BGP route for the default network (network 0).
	bgp/E	BGP route learned from an external neighbor.
	bgp/I	BGP route learned from an internal neighbor.
Metric	Hop count to the next hop.	
Interface	Interface used for forwarding packets to the gateway for the next hop.	

show bgp paths

This command displays BGP path information learned by the PortMaster.

show bgp paths [*Prefix/NM* [**verbose**]]

<i>Prefix</i>	IP prefix address, specified in dotted decimal notation. If you do not include the verbose keyword, the display shows only the NLRI for the best match to this specified prefix address.
<i>/NM</i>	Netmask that indicates the number of high-order bits in the IP prefix. This value is a number from 0 to 32, preceded by a slash (/)—for example, /24.
verbose	Displays all the NLRI associated with the paths that the specified prefix address is on.

Example

This example shows a simple path, with few routes.

```
Command> show bgp paths
O: INC      AAS: 12345      AIP: 1.2.3.4      OID: 192.168.1.130
Cluster List: 192.168.135.1
Sequence: 60149 1 2 3
NH: 172.16.96.76 LP: 99000 MED Learned/Used: 100/200
Metrics to NH: 3/2/0/2/0 Gateway to NH: 192.168.10.1
Communities info: 129/129/8454273
NLRI: +10.24.0.0/16/8/7
```

Explanation

O:	The origin of the learned path information:
IGP:	NLRI originated from an interior gateway protocol (IGP) such as OSPF.
EGP:	NLRI originated from the Exterior Gateway Protocol (EGP).
INC:	Full origin of the information is not known for this path.
AAS:	Aggregating autonomous system number.
AIP:	Aggregating IP address.
OID:	ID of the originating router for the route, if learned across a route reflector in the local autonomous system.
Cluster List:	The chain of route reflector clusters that the route has traversed in the local autonomous system.
Sequence:	Ordered set of autonomous systems in the path. The closest autonomous system in the path is shown first.
Set:	Unordered collection of autonomous systems in the path.
Confederation Sequence:	Ordered set of autonomous systems for a confederation. The closest autonomous system in the path is shown first.
Confederation Set:	Unordered collection of autonomous systems for a confederation.
NH:	IP address of the next hop that is used to reach the following NLRI addresses. The next hop is usually, but not always, the router that advertises them.
	The message “self-generated” in this field indicates that the path was generated from a summarization configured on the PortMaster.
LP:	Learned local preference attribute for this path. In most cases, internal peers prefer paths that have the highest local preference. When the local preference is not learned for the path, the message “not present” is shown.

MED	Multiexit discriminator for this path that indicates a preference for a specific path when more than one exists. Both the learned and the one used—which can be different due to acceptance policy criteria—are shown. If none is either learned or used, the message “not present” is shown.						
Learned/Used:	A lower value indicates a higher preference for the path. The multiexit discriminator value is a 32-bit nonnegative integer.						
Metrics to NH:	Metrics to the next hop—an <i>A/B/C/D/E</i> string, used for debugging.						
Gateway to NH:	IP address of the adjacent router that leads to the next hop router.						
Communities info:	One of the reserved community keywords that restrict route advertisement for peers receiving the route information: no-export , no-advertise , or no-export-subconfed . Or: Values of communities attribute information in the path, in the format <i>A/B/C</i> : <table><tr><td><i>A</i></td><td>Autonomous system number—the first 16-bit portion of the communities attribute.</td></tr><tr><td><i>B</i></td><td>Additional information about the autonomous system—the second 16-bit portion of the communities attribute.</td></tr><tr><td><i>C</i></td><td><i>A+B</i>—a single 32-bit number for the communities attribute.</td></tr></table>	<i>A</i>	Autonomous system number—the first 16-bit portion of the communities attribute.	<i>B</i>	Additional information about the autonomous system—the second 16-bit portion of the communities attribute.	<i>C</i>	<i>A+B</i> —a single 32-bit number for the communities attribute.
<i>A</i>	Autonomous system number—the first 16-bit portion of the communities attribute.						
<i>B</i>	Additional information about the autonomous system—the second 16-bit portion of the communities attribute.						
<i>C</i>	<i>A+B</i> —a single 32-bit number for the communities attribute.						
NLRI:	Network layer reachability information (NLRI), shown in the format <i>+Prefix/NM/BMAd/BMP</i> : <table><tr><td>+</td><td>Indicates the path was chosen as the best path for this NLRI among all available paths that contain this NLRI.</td></tr><tr><td>Prefix</td><td>IP address prefix of the NLRI.</td></tr><tr><td>NM</td><td>Netmask of the NLRI.</td></tr></table>	+	Indicates the path was chosen as the best path for this NLRI among all available paths that contain this NLRI.	Prefix	IP address prefix of the NLRI.	NM	Netmask of the NLRI.
+	Indicates the path was chosen as the best path for this NLRI among all available paths that contain this NLRI.						
Prefix	IP address prefix of the NLRI.						
NM	Netmask of the NLRI.						

BMAAd	Combined bit mask, in hexadecimal, of all peers that have advertised this NLRI and path to this PortMaster. The bit mask for each peer can be found in the output of show bgp peers verbose .
BMP	Combined bit mask, in hexadecimal, of all peers to whom the PortMaster has advertised this NLRI for this path.

show bgp peers

This command displays a list of BGP peers and, optionally, a summary of packets sent to and received from the peers.

show bgp peers [**verbose**|**packets**]

show table bgp

verbose	Provides detailed information about BGP peers.
packets	Provides a summary of packets sent to and received from the peers.

Usage

Using the command without either optional keyword provides summary information. This is the default.

The command **show table bgp** displays the same output as **show bgp peers**.

Example 1—Summary Information

Command> show bgp peers							
Remote IP	AS	Fl	DH	Up	Accept	Inject	Advertise
-----	---	---	---	---	-----	-----	-----
192.168.1.2	2	RN	2	Up	only207	only207	only207
192.168.1.3	3	C	--	Dn	all	all	all

Explanation

Remote IP	IP address of the BGP peer.
AS	Autonomous system number of the BGP peer.
Fl	Flags: C Identifies this peer as a confederation member peer of the PortMaster. R Identifies this peer as a route-reflector client of the PortMaster. N This peer is configured to always consider the PortMaster as the next hop for any update packet sent from this peer.
DH	Hop count for the default route to this peer, if one is configured with the assume-default keyword.
Up	State of the peer: Up Peer is in a fully established state. Dn Peer is not in a fully established state.
Accept	Acceptance policy name, if configured.
Inject	Injection policy name, if configured.
Advertise	Advertisement policy name, if configured.



Note – When a peer deletion is in process, a message and countdown timer is displayed in the Accept, Inject, and Advertise columns, as follows:

-- Deletion in Progress. Countdown 216 --

Deletion is complete when the countdown drops to zero. A similar “idling” message is shown when the peer is idling **down** from a previously established **up** state.

Example 2—Verbose Information

```

Command> show bgp peers verbose
Incoming Peer Source: 192.168.96.135   Destination: 192.168.96.130
Remote Autonomous System: 60149       Remote Id: 192.168.96.130
Current state: Established              Last Event: Received Update
Timer expiration in 64 seconds         Bitmask: 8
NLRI from/to this peer: 43839/ 43211   Peer up 10:40.80
Last sent error: 0/0. Last received error: 2/3.
Accept Naris Policy: all
Inject Naris Policy: all
Advertise Naris Policy: all

```

Packet Type	Sent	Received
-----	-----	-----
Opens	2	2
Keepalives	5	5
Notifications	2	0
Updates	3375	4852

Explanation

Incoming Peer Source	Local IP address used to attach to the peer.	
	Each peer consists of two subpeers, only one of which is active at any time:	
	Incoming	Local subpeer is attempting a connection.
	Outgoing	Local subpeer is listening for connections from others.

Destination	Destination of the remote peer.																		
Remote Autonomous System	Remote autonomous system number of the peer.																		
Remote Id	BGP ID of the remote peer.																		
Current state	Current state of the BGP peer, as defined in RFC 1771: <table> <tr> <td>Established</td><td>Full connectivity is established to this peer.</td></tr> <tr> <td>Other</td><td>The PortMaster is attempting to establish connectivity to this peer.</td></tr> </table>	Established	Full connectivity is established to this peer.	Other	The PortMaster is attempting to establish connectivity to this peer.														
Established	Full connectivity is established to this peer.																		
Other	The PortMaster is attempting to establish connectivity to this peer.																		
Last Event	The most recent events for this peer: <table> <tr> <td>Start</td><td>Connection attempt started.</td></tr> <tr> <td>Stop</td><td>Result of a reset bgp command.</td></tr> <tr> <td>Transport Open</td><td>TCP session opened.</td></tr> <tr> <td>Transport Closed</td><td>TCP session closed.</td></tr> <tr> <td>Transport Open Fail</td><td>TCP open session failed—for example, because the PortMaster was unable to reach the remote host.</td></tr> <tr> <td>Transport Error</td><td>TCP session reported an error.</td></tr> <tr> <td>Connect Time Expired</td><td>BGP connection time expired, and BGP is starting to open a new connection after being in an idle state.</td></tr> <tr> <td>Hold Time Expired</td><td>Remote BGP peer did not send a keepalive message within the hold time, so the peer is dropped.</td></tr> <tr> <td>Keepalive Time Expired</td><td>Keepalive timer expired for the peer. This event indicates that the PortMaster needed to send another keepalive packet.</td></tr> </table>	Start	Connection attempt started.	Stop	Result of a reset bgp command.	Transport Open	TCP session opened.	Transport Closed	TCP session closed.	Transport Open Fail	TCP open session failed—for example, because the PortMaster was unable to reach the remote host.	Transport Error	TCP session reported an error.	Connect Time Expired	BGP connection time expired, and BGP is starting to open a new connection after being in an idle state.	Hold Time Expired	Remote BGP peer did not send a keepalive message within the hold time, so the peer is dropped.	Keepalive Time Expired	Keepalive timer expired for the peer. This event indicates that the PortMaster needed to send another keepalive packet.
Start	Connection attempt started.																		
Stop	Result of a reset bgp command.																		
Transport Open	TCP session opened.																		
Transport Closed	TCP session closed.																		
Transport Open Fail	TCP open session failed—for example, because the PortMaster was unable to reach the remote host.																		
Transport Error	TCP session reported an error.																		
Connect Time Expired	BGP connection time expired, and BGP is starting to open a new connection after being in an idle state.																		
Hold Time Expired	Remote BGP peer did not send a keepalive message within the hold time, so the peer is dropped.																		
Keepalive Time Expired	Keepalive timer expired for the peer. This event indicates that the PortMaster needed to send another keepalive packet.																		

Received Open	PortMaster received an open message from the peer.
Received Keepalive	PortMaster received a keepalive message from the peer.
Received Update	PortMaster received an update message from the peer. Update messages contain the path and route data updates.
Received Notification	PortMaster received a notification message from the peer. This event indicates that the peer requires the PortMaster to drop the current session.
Deleted	PortMaster has deleted the peer.
Dropped	Peer was dropped by the PortMaster because a notification error message had to be sent to the peer.
Idling Down Done	PortMaster has finished idling down this peer from an established state to an idle state.
Timer expiration...	<p>Number of seconds that must elapse before the next timed event will occur:</p> <ul style="list-style-type: none"> • For sessions not in an open state, the time that must elapse until the next connection attempt. • For sessions either open or established, the time that must elapse before the required keepalive message is received from the peer. If the PortMaster does not receive a keepalive message from the peer, the peer is unreachable.
Bitmask	Gives the bit mask of this peer. This value is useful when you are looking at the NLRI information in the output of show bgp path .
NLRI from/to this peer	Total active NLRI received from and sent to the peer.
Peer up	Time that peer has been up in <i>hours:minutes.seconds</i> .

Last sent error	Last error sent in a notification message to this peer. BGP notification error codes are fully described in RFC 1771.
Last received error	Last error received in a notification message from this peer. BGP notification error codes are fully described in RFC 1771.
Accept NLRIs Policy	Acceptance policy name, if configured.
Inject NLRIs Policy	Injection policy name, if configured.
Advertise NLRIs Policy	Advertisement policy name, if configured.
Packet Type	Type of BGP packet sent to or received from the peer.
Sent	Number of packets of each type sent to the peer since it was defined.
Received	Number of packets of each type received from the peer since it was defined.



Note – When a BGP peer has been deleted or idled, you might see one of the following messages in place of a configured policy name:

- “Waiting for TCP close before deletion”
- “Waiting for TCP close before idle”

This message appears because a peer is not fully deleted or idled until the peer has acknowledged the close of the TCP session.

Example 3—Packets Sent and Received Information

Command> show bgp peers packets						
Remote IP	Up	Open In/Out	Keepalive In/Out	Notification In/Out	Update In/Out	NLRI In/Out
-----	---	-----	-----	-----	-----	-----
192.168.1.135	Up	2	24	0	3933	44073
		3	23	3	1005	354
192.168.1.133	Dn	5	23	0	7714	44092
		6	21	4	7717	44089

192.168.1.130	Up	4	21	0	3525	44085
		4	23	2	3535	44094

Explanation

Remote IP	IP address of the BGP peer.
Up	State of the peer:
	Up Peer is in a fully established state.
	Dn Peer is not in a fully established state.
Open In/Out	Number of open messages received from and sent to the peer since the last reboot or reset bgp command.
Keepalive In/Out	Number of keepalive messages received from and sent to the peer since the last reboot or reset bgp command.
Notification In/Out	Number of notification messages received from and sent to the peer since the last reboot or reset bgp command.
Update In/Out	Number of update messages received from and sent to the peer since the last reboot or reset bgp command.
NLRI In/Out	The total active NLRI received from and sent to the peer.

show bgp policy

This command shows BGP policy names and definitions.

show bgp policy [*Polycyname*]

<i>Polycyname</i>	Name of existing policy for which details are to be displayed. Without this option only the names of existing BGP policies are displayed.
-------------------	---

Examples

```
Command> show bgp policy
add401admit
```

```
Command> show bgp policy add401
set bgp policy add401 1 permit
if prefix 10.0.0.0/8
then community add 401 401
```

show bgp summarization

This command shows the route summaries configured by the network administrator for advertisement to BGP peers.

show bgp summarization [all]

all Displays both manually configured summaries, and those automatically built with the **add propagation static bgp** command. The manually configured summaries are shown with /C after the prefix and netmask, and the automatically generated ones are shown with /A. The default is to display only manually configured summaries.

Example

The following example shows a summary configured for a route to an IP address with a prefix of 10.0.0.0, a netmask of /8, and a multiexit discriminator of 5. The summary is being forwarded to autonomous systems 1, 2, and 3.

```
Command> show bgp summarization all
10.0.0.0/8/C          Count of Supporting Routes:      53
LP: 0                MED: 5                CAS: no-advertise
Export to AS: 1 2 3
Export to CMA: 4
```


Explanation

10.0.0.0/8/C	<p>IP prefix and netmask of the route summary.</p> <p>/C—A configured summarization.</p> <p>/A—Automatically generated from static route information with the add propagation static bgp command.</p>
Count of Supporting Routes	<p>Number of routes known to the system that are learned from an interior routing protocol (such as OSPF), or are directly connected or statically configured and support this summary. If the count is zero, the PortMaster does not advertise the summary to any of its peers.</p>
LP	<p>Configured local preference value to use when advertising this summary to internal or confederation member peers. Zero (0) indicates that no local preference will be advertised.</p>
MED	<p>Configured multiexit discriminator to use when advertising this summary to external and confederation member peers.</p>
CAS	<p>Community autonomous system information configured to be sent when this summary is advertised. Shown as a pair of numbers, the first is the autonomous system number, and the second is information about the autonomous system. A value of “0 0” indicates that no communities attribute is advertised. If the communities attribute is a reserved value, as in this example, it is shown as a text string.</p>
Export to AS	<p>List of the numbers of adjacent autonomous systems to which this summary is advertised. If the autonomous system of the PortMaster is displayed, this summarization is also advertised to internal peers in the same autonomous system.</p>
Export to CMA	<p>List of the numbers of adjacent confederation member autonomous systems (CMAs) to which this summary is advertised. If the CMAs of the PortMaster are displayed, this summarization is also advertised to internal confederation-member peers.</p>

show routes

Shows the IP routing table. For more information, see the explanation of routing tables in the *PortMaster Configuration Guide*.

show routes [*String*|*Prefix/NM*]

- String*

Displays only routes that contain the matching *String* in their **show routes** command output. For example, **show routes bgp** shows only routes that contain the string **bgp**.
- Prefix/NM*

Displays routes only to the destination indicated by this IP address prefix *Prefix* and netmask *NM*. The netmask indicates the number of high-order bits in the IP prefix.

 - Specify *Prefix* in dotted decimal notation.
 - Specify *NM* as number from 1 to 32, preceded by a slash (/)—for example, /24.

Example

Command> show routes bgp						
Destination	Mask	Gateway	Source	Flag	Met	Interface
-----	-----	-----	-----	-----	-----	-----
0.0.0.0	0	172.31.96.129	bgp/D	ND	3	ether0
192.168.1.0	24	172.31.96.129	bgp/E	ND	1	ether0
172.16.0.0	16	172.31.96.130	bgp/I	ND	2	ether0

Explanation

- Destination IP address of the host or network to which packets are sent.
- Mask Netmask in use for the destination.
- Gateway IP address of the directly connected host through which packets are forwarded to the destination.

Source	Source of the route information:
	local Route learned from an interface on the PortMaster.
	rip RIP route learned from a connected network.
	ospf OSPF route learned from an internal neighbor.
	ospf/E1 OSPF route learned from Type 1 external or Type 2
	ospf/E2 external routes.
	ospf/N1 OSPF route learned as Type 1 external or Type 2 external
	ospf/N2 routes from not-so-stubby areas (NSSAs).
	ospf/IA OSPF route originating from another area and learned
	via an area border router.
	bgp/D BGP route for the default network (network 0).
	bgp/E BGP route learned from an external neighbor.
	bgp/I BGP route learned from an internal neighbor.
Flag	<ul style="list-style-type: none">• H—A host route.• N—A network route.• S—A static route that is either configured (permanent) or learned via a RADIUS Framed-Route (temporary).• L—A route attached to an interface on the PortMaster.• D—A route dynamically learned via RIP or OSPF.• C—A changed route that has yet to be advertised to all interfaces.• O—An obsolete route scheduled for deletion.
Met	Metric—hop count to the remote destination.
Interface	Interface used for forwarding packets to the gateway for the destination.

This chapter describes the debug commands used for troubleshooting PortMaster configuration or operation.

For general information about command line interface commands, see Chapter 1, “Introduction.”

Summary of Debug Commands

The debug commands in Table 19-1 are used for PortMaster debugging sessions.

Table 19-1 Debug Commands

Command Syntax	
set debug bgp-fsm bgp-decision-process bgp-opens bgp-keepalives bgp-updates bgp-notifications bgp-errors bgp-packets bgp-max on off	- see page 19-2
set debug ccp-stac on off	- see page 19-4
set debug choicenets on off	- see page 19-5
set debug clock on off	- see page 19-5
set debug Hex	- see page 19-5
set debug isdn isdn-dframes isdn D0 isdn-l1 D0 termination isdn-v120 on off	- see page 19-8
set debug l2tp max packets [Bytes] setup stats on off	- see page 19-9
set debug mcppp-event on off	- see page 19-10
set debug mdp-status mdp-events mdp-max on off	- see page 19-11
set debug nat-ftp nat-icmp-err nat-rt-interface nat-max on off	- see page 19-12

Table 19-1 Debug Commands (Continued)

Command Syntax	
set debug nfas on off	- see page 19-13
set debug off	- see page 19-6
set debug ospf-hello ospf-event ospf-spfcalc ospf-lsu ospf-lsa ospf-dbdesc ospf-error ospf-routing ospf-max on off	- see page 19-14



Note – You can stop debug sessions by turning off the individual debug commands—for example, **set debug isdn off**. However, any and all debug commands can be turned off with the **set debug off** command.

Debug Commands

set debug bgp

This command sets debug flags used for BGP troubleshooting. Debug information is displayed to the console.

set debug bgp-fsm|bgp-decision-process|bgp-opens|bgp-keepalives|bgp-updates|bgp-notifications|bgp-errors|bgp-packets|bgp-max on|off

bgp-fsm	Set on to show events that change the state of the BGP session with any peer.
bgp-decision-process	Set on to show decisions among routes about the best path to a destination.
bgp-opens	Set on to show open messages sent and received between any peers.
bgp-keepalives	Set on to show keepalive messages sent and received between any peers.
bgp-updates	Set on to show update messages sent and received between any peers.

bgp-notifications	Set on to show notification messages sent and received between any peers.
bgp-errors	Set on to show protocol errors occurring between BGP peers.
bgp-packets	Set on to enable bgp-opens , bgp-keepalives , bgp-updates , and bgp-notifications options.
bgp-max	Set on to enable all BGP debugging options.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

Use of the **set debug bgp-max** command on a connection where large routing tables are exchanged between peers creates a flood of output that is useless for debugging. The **set debug bgp-max** command is best used in controlled environments where problems of peer interaction are being debugged and limited routing information is exchanged.

Example

To track any protocol errors occurring between BGP peers, enter the following commands:

```
Command> set console
Command> set debug bgp-errors on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```

set debug ccp-stac

This command sets debug flags used for troubleshooting Stac LZS compression implementation. Debug information is displayed to the console.

set debug ccp-stac on|off

ccp-stac Set **on** to display debugging messages for Stac LZS compression.

off Clears all debug settings—including *Hex* debug settings—currently active on the PortMaster.

Usage

The **set debug ccp-lzs** command displays the allocation of compression data structures, error messages, and re-initializations if the Compression Control Protocol (CCP) is renegotiated and if resets are sent or received when decompression is not synchronized with compression.

Example

To track Stac LZS compression operation, enter the following commands:

```
Command> set console
Command> set debug ccp-stac on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```


set debug choicen

This command sets debug flags used for troubleshooting ChoiceNet. Debug information is displayed to the console.

set debug choicen on|off

on Set **on** to display the information related to ChoiceNet events.

off Clears all debug settings—including *Hex* debug settings—currently active on the PortMaster.

Example

To track ChoiceNet events, enter the following commands:

```
Command> set console
Command> set debug choicen on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```

set debug (Hex and Clock)

These commands set debug flags for general PortMaster troubleshooting. Debug information is displayed to the console.

set debug clock on|off

set debug Hex

set debug off

clock	Set on to time-stamp the console debug messages. The time is measured since the last reboot and is specified in hours, minutes, seconds, and hundredths of a second. To turn the time stamp off, use the set debug clock off command.
<i>Hex</i>	<p>One of the following hex codes:</p> <ul style="list-style-type: none">• 0x0 disables the output for a <i>Hex</i> debug. This is the default.• 0x1100 outputs information about routing table updates from RIP.• 0x51 allows observation of Point-to-Point Protocol (PPP), Local Management Interface (LMI), and Annex-D configuration requests and acknowledgments.• 0x54 allows observation of the last 60 characters sent and received on an asynchronous port, and the last two termination causes, when a show command is entered on the port.• 0x72 displays interactively between ComOS and nonvolatile RAM when ComOS is reading from or writing to the nonvolatile RAM.• 0x74 displays the last 60 characters of I/O.• 0x75 same as 0x51 and 0x54 with more detail.• 0x78 shows Telnet negotiation options when someone is connecting to the PortMaster by Telnet.• 0x81 shows updates being made to the Address Resolution Protocol (ARP) cache.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The **debug** command is useful for troubleshooting such PortMaster activities as the PPP negotiation process.

Example

To debug PPP negotiations, enter the following commands:

```
Command> set console  
Command> set debug 0x51
```

To stop the debug output, enter the following:

```
Command> set debug off  
Command> reset console
```

Refer to the *PortMaster Configuration Guide* for information on interpreting the output.

See Also

ptrace - page 2-13
set console - page 2-20
traceroute - page 2-44

set debug isdn

This command sets debug flags for ISDN troubleshooting. Debug information is displayed to the console.

```
set debug isdn|isdn-dframes|isdn D0|isdn-l1 D0|termination|
isdn-v120 on|off
```

isdn	Set on to show ISDN debugging information on the console.
isdn-dframes	Set on to show all D channel frames loading into or out of the PortMaster on the BRI or PRI lines connected. To turn off debugging, re-enter the command.
isdn D0	Set on to show debugging of a single BRI line designated by the value of <i>D0</i> . To turn off debugging, re-enter the command.
isdn-l1 D0	Set on to show Layer 1 activation tracing on a BRI line designated by the value of <i>D0</i> . Layer 1 is the physical layer of the OSI model.
termination	Set on to display detailed port termination information.
isdn-v120	Set on to display debugging of the V.120 protocol exchanges in V.120 connections. Debug output indicates the following conditions when they exist: <ul style="list-style-type: none">• An ISDN V.120 connection is active.• An ISDN V.120 connection is established at 64Kbps.• An ISDN V120 connection is a data call.
off	Clears debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster, except ISDN debug settings for a specific D channel.

Usage

The **debug** command is useful for displaying ISDN information—such as connections, disconnections, and service profile identifier (SPID) registration—on the console.

Example

To track any errors occurring while ISDN lines are in use, enter the following commands:

```
Command> set console
Command> set debug isdn on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```

set debug 12tp

This command displays L2TP activities to the console.



set debug 12tp max|packets [Bytes] |setup|stats on|off

max	Set on to display all the information generated when you use all the other debug options listed below.
packets [Bytes]	Set on to display L2TP packets. <i>Bytes</i> is an optional integer between 0 and 1500 that specifies the number of bytes to display.
setup	Set on to display control messages and errors.
stats	Set on to display L2TP session statistics.
off	Clears all debug setting—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

set debug mcppp-event

This command sets debug flags used for troubleshooting Multichassis PPP events. Debug information is displayed to the console.

set debug mcppp-event on|off

mcppp-event	Set on to display all the information related to the Multichassis PPP events.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The **set debug mcppp-event on** command is useful for troubleshooting all Multichassis PPP events.

Example

To track Multichassis PPP events, enter the following commands:

```
Command> set console
Command> set debug mcppp-event on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```

set debug mdp

This command sets debug flags used for troubleshooting PortMaster 3 digital modems. Debug information is displayed to the console.

set debug mdp-events|mdp-max|mdp-status on|off

mdp-events	Set on to display the progress of the modems as they initialize.
mdp-max	Set on to display both the status of the digital modems and their progress as they initialize.
mdp-status	Set on to display the status of the digital modems.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The **debug** command is useful for troubleshooting PortMaster 3 digital modems as they are initialized and while their operating code is being loaded.

Example

To track digital modem operation, enter the following commands:

```
Command> set console
Command> set debug mdp-status on
```

To stop the debugging output, enter the following:

```
Command> set debug off
Command> reset console
```

set debug nat

This command sets debug flags for troubleshooting NAT sessions. Debug information is displayed to the console.

3.9

set debug nat-ftp|nat-icmp-err|nat-rt-interface|nat-session|nat-max on|off

nat-ftp	Set on to view FTP payload processing.
nat-icmp-err	Set on to view ICMP error payload processing.
nat-rt-interface	Set on to view NAT parameter changes during interface binding.
nat-max	Set on to view full NAT debugging.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The PortMaster supports this command in ComOS 3.9 and later relevant releases.

Examples

```
Command> set console
Command> set debug nat-ftp
Enabling NAT FTP payload debugging
```

```
NAT: ptp5: Out FTP (11.0.0.2,3023)->(172.16.6.1,21) Payload: PORT 11
,0,0,2,11,208
NAT: ptp5: Out FTP Xlated (192.168.1.36,20001)->(172.16.6.1,21) Payload: POR
T 192,168,1,36,78,34
NAT: ptp5: In FTP (172.16.6.1,21)->(192.168.1.36,20001) Xlation failed: Session
may have prematurely timed out.
```

```
Command> set debug off
Command> set reset console
```



```

Command> set console
Command> set deb nat-icmp
Enabling NAT ICMP Error payload debugging

NAT: ptp5: In    ICMP Error(type: 11,code 0) 192.168.1.37->192.168.1.36
Payload:
    45:00:00:5c:23:48:00:00:01:1f:ac:c0:a8:01:24:95:c6:20:1b:
    08:00:e9:34:04:02:0a:c9:
NAT: ptp5: In    ICMP Error(type: 11,code 0) Xlated 192.168.1.37->11.0.0.2
Payload:
    45:00:00:5c:23:48:00:00:01:d6:76:0b:00:00:02:95:c6:20:1b:
    08:00:ec:36:01:00:0a:c9:
    08:00:e4:36:01:00:12:c9:

Command> set debug off
Command> set reset console

```

set debug nfas

This command enables or disables the PortMaster to log NFAS events to the console.

3.9

set debug nfas on|off

on Logs NFAS events.
off Disables the logging of NFAS events.

Usage

The PortMaster supports NFAS on ComOS 3.9 and later relevant releases. Before using this command, issue the **set console** command to display NFAS events to the console.

See Also

reset console - page 2-15
set console - page 2-20
set Line0 nfas - page 12-14

set debug ospf

This command sets debug flags used for troubleshooting OSPF. Debug information is displayed to the console.

```
set debug ospf-hello|ospf-event|ospf-spfcalc|ospf-lsu|ospf-lsa|ospf-dbdesc|ospf-error|ospf-routing|ospf-max on|off
```

ospf-hello	Set on to show hello packets sent between neighbors.
ospf-event	Set on to show changes in state between neighbors.
ospf-spfcalc	Set on to show details of the shortest path first (SPF) calculation for an area each time this calculation is run.
ospf-lsu	Set on to show link state update packets sent or received.
ospf-lsa	Set on to show link state advertisement packets sent or received.
ospf-dbdesc	Set on to show the initial exchange of database information sent between OSPF neighbors when they are forming an adjacency.
ospf-error	Set on to show information when the current PortMaster OSPF configuration does not match a neighbor's OSPF configuration.
ospf-routing	Set on to show when the routing table receives input from the OSPF database, or the OSPF database receives input from the routing table.
ospf-max	Set on to show all OSPF debug information.
off	Clears all debug settings—including <i>Hex</i> debug settings—currently active on the PortMaster.

Example

To track OSPF link state update packets, enter the following commands:

```
Command> set console  
Command> set debug ospf-lsu on
```

To stop the debugging output, enter the following:

```
Command> set debug off  
Command> reset console
```

Configurable Ports

A

The command line interface can be used to configure your PortMaster ports. Table A-1 lists the configurable ports by PortMaster model.

Table A-1 Configurable Ports Available for Each PortMaster Model

Model	Ports								
	Ethernet	Asyn-chronous	Syn-chronous	Parallel	BRI U	BRI S/T	T1 Lines	E1 Lines	Analog Phone
OR-M	ether0	s0–s ¹							
OR-ST	ether0	s0				s1–s2			
OR-U	ether0	s0			s1–s2				
OR-LS	ether0	s0	w1						
OR-HS	ether0	s0	w1						
OR-U-AP	ether0	s0			s1–s2				pots
OR-ST-AP	ether0	s0				s1–s2			ports
PM-2	ether0	s0–s9		p0					
PM-2E-10	ether0	s0–s9		p0					
PM-2E-20	ether0	s0–s19 ¹		p0	s10–s19 ¹	s10–s19 ¹			
PM-2E-30	ether0	s0–s29 ¹		p0	s10–s29 ¹	s10–s29 ¹			
PM-2ER-10	ether0	s0–s9	w1						

Table A-1 Configurable Ports Available for Each PortMaster Model (Continued)

Model	Ports								
	Ethernet	Asyn-chronous	Syn-chronous	Parallel	BRI U	BRI S/T	T1 Lines	E1 Lines	Analog Phone
PM-2ER-20	ether0	s0–s19 ¹	w1		s10–s19 ¹	s10–s19 ¹			
PM-2ER-30	ether0	s0–s29 ¹	w1		s10–s29 ¹	s10–s29 ¹			
PM-2R	ether0	s0–s9	w1						
PM-25	ether0	s0–s24 ²							
PM-2i-U	ether0	c0			s0–s9				
PM-2i-ST	ether0	c0				s0–s9			
PM-2Ei-10I-U	ether0	c0			s0–s29 ¹				
PM-2Ei-10I-ST	ether0	c0				s0–s29 ¹			
IRX-111	ether0	s0	s1						
IRX-112	ether0	s0	s1–s2						
IRX-114	ether0	s0	s1–s4						
IRX-211	ether0–ether1	s0	s1						
PM-3A-IT	ether0	c0					line0		
PM-3A-2T	ether0	c0					line0–line1		
PM-3D-1T	ether0	c0					line0		

Table A-1 Configurable Ports Available for Each PortMaster Model (Continued)

Model	Ports								
	Ethernet	Asyn-chronous	Syn-chronous	Parallel	BRI U	BRI S/T	T1 Lines	E1 Lines	Analog Phone
PM-3D-2T	ether0	c0					line0–line1		
PM-3A-1E	ether0	c0						line0	
PM-3A-2E	ether0	c0						line0–line1	
PM-3D-1E	ether0	c0						line0	
PM-3D-2E	ether0	c0						line0–line1	

1. Ports S10 through S19 are ISDN B channels if a MOD-10I-U or MOD-10I-ST card is placed in the first expansion slot. Ports S20 through S29 are ISDN B channels if a MOD-10I-U or MOD-10I-ST card is placed in the second expansion slot.
2. A single asynchronous serial port (S0) is provided, as well as three high-density 68-pin connectors, each of which supports eight asynchronous serial devices.

Table B-1 lists the basic PortMaster commands. Some are complete commands; most require additional keywords or values as described in this reference.

Table B-1 Basic PortMaster Commands

Command	Description
!!	Repeats the last command.
add	Adds an entry to a PortMaster table.
attach	Allows you to communicate directly to a device attached to a specified asynchronous or ISDN PortMaster port.
clear	Deletes an entry.
create	Creates an entry.
delete	Deletes an entry from a PortMaster table.
dial	Begins dialing to the specified network location.
done	See quit .
erase	Removes all or part of nonvolatile RAM.
exit	See quit .
get	See tftp get .
help	Provides information on each of the commands, including usage and syntax.
ifconfig	Displays configuration values for all interfaces.
ping	Sends an Internet Control Message Protocol (ICMP) echo request packet to test connectivity.
pmlogin	Establishes a login using the PortMaster login service to a specified host on the network.
ptrace	Displays packet traffic passing through the PortMaster, using the specified filter.

Table B-1 Basic PortMaster Commands (Continued)

Command	Description
quit, done, or exit	Exits the command line interface.
reboot	Reboots, using the currently saved configuration.
reset	Resets a specific physical or virtual port (or ports) to the current default configuration, and drops any active sessions on the port.
rlogin	Establishes a login using the rlogin service to a specified host on the network.
save	Writes the current configuration to PortMaster nonvolatile RAM.
set	Configures a value on a port, or configures a value globally, for a PortMaster table, or for a protocol.
show	Shows the status of each specified port, file, filter, board, slot, PortMaster table, and so on, or the global configuration.
telnet	Connects via Telnet from the PortMaster to a specified host on the network.
tftp get	Retrieves a file of configuration commands or a ComOS image from a host using the Trivial File Transfer Protocol (TFTP).
traceroute	Traces network routes to show a connectivity path.
version	Displays the version number of the ComOS software that runs the PortMaster, and the uptime since the last boot.

Table C-1 describes the values (arguments) that are used in command line interface commands. These values must be replaced in the commands with appropriate values for your specific needs. For example in the command **add filter** *Filtername*, replacing the value *Filtername* with the name **inet.in** adds a new filter named **inet.in** to the filter table.

Table C-1 Command Line Values

Value	Represents	Format and/or Value(s)
<i>Alarm-id</i>	Specific instance of an SNMP alarm.	Number.
<i>Area</i>	OSPF area.	Decimal or dotted decimal notation.
<i>ASN</i>	Autonomous system number.	A 16-bit number ranging from 1 to 65535.
<i>Bytes</i>	Number of bytes.	Integer 0 or higher.
<i>Cgroup</i>	Group of channels.	1 through 63.
<i>Channel-list</i>	Series of one or more channel numbers.	<ul style="list-style-type: none"> • For T1, any number(s) from 1 through 24, separated by spaces. • For E1, any number(s) from 1 through 30, separated by spaces.
<i>CommandName</i>	Name of a ComOS command.	One of the general commands. See Chapter 2.
<i>D0</i>	Any ISDN D channel.	d0 or d1 .
<i>Device</i>	Name of a network device or pseudo-tty on a UNIX host.	/dev/ttyp0 , or /dev/network .
<i>Dlci</i>	DLCI number.	1 through 1023.
<i>Dlci_list</i>	Space separated list of DLCIs.	Maximum of 240 characters.

Table C-1 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Ether0</i>	Ethernet interface.	<ul style="list-style-type: none"> • ether0 or ether1 on an IRX-211. • ether0 on all others. <p>Defaults to ether0 if omitted.</p>
<i>Facility.Priority</i>	Loghost facility and priority of syslog messages sent to the facility.	<p>One syslog facility keyword and one syslog priority keyword separated by a period.</p> <p>See page 3-20 for more information.</p>
<i>Filtername</i>	Name of input or output packet filter.	String of up to 15 printable, nonspace, ASCII characters.
<i>Group</i>	Number of group.	<p>Integer from 0 to 100; 0 is the default.</p> <p>For NFAS entries, an integer between 0 and 99 common to all the T1 lines belonging to the same NFAS group.</p>
<i>Handle</i>	Network identifier.	n followed by a number, with no space in between.
<i>Hex</i>	Number in hexadecimal (hex) notation.	Hex number with a leading 0x .
<i>Identifier</i>	NFAS group identifier.	Integer between 0 and 19 that uniquely identifies a T1 interface in an NFAS group.
<i>Interface</i>	Interface specification.	For example, ether0 , frm1 , ptp1 , frmw1 , or ptpw1 .
<i>Ipaddress</i>	IP address or hostname.	Dotted decimal notation or hostname of between 1 and 39 characters.
<i>Ipaddrxfrom</i>	IP address to be translated using NAT.	Dotted decimal notation.
<i>Ipaddrxto</i>	IP address to be translated to using NAT.	Dotted decimal notation.

Table C-1 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Iplist</i>	List of IP addresses.	Comma-separated list of IP addresses and/or IP address ranges.
<i>Ipmask</i>	IP subnet mask—also called a netmask .	Dotted decimal notation with ones in high-order bits, and zeros in low-order bits.
<i>Ipxaddress</i>	IPX address.	Hex notation in following format: <i>Ipxnetwork:Ipxnode</i> . <i>Ipxnode</i> is a 48-bit number.
<i>Ipxnetwork</i>	IPX network number.	32-bit hex number.
<i>Ipxnode</i>	IPX node address.	48-bit hex number. On PortMaster products this is usually the media access control (MAC) address.
<i>Ipxsock</i>	Port number for the IPX socket.	Integer from 0 to 65535.
<i>Itype</i>	ICMP packet type.	0 or higher.
<i>Line0</i>	T1 or E1 line on a PortMaster 3.	line0 or line1 .
<i>Line2</i>	T1 card on a PortMaster 3.	line2 .
<i>ListName</i>	Name of a list of source or destination sites used for packet filters.	String of up to 15 printable, nonspace, ASCII characters.
<i>Locname</i>	Name of an internetwork dial-out destination.	String of up to 12 printable, nonspace, ASCII characters.
<i>Logtype</i>	One of five areas used for logging with the set syslog command.	The alternatives are admin-logins , user-logins , packet-filters , commands , and termination .
<i>M0</i>	Digital modem number.	m0 through m59 .
<i>Macaddress</i>	MAC (hardware) address.	12-digit hexadecimal notation: <i>xx:xx:xx:xx:xx:xx</i> .

Table C-1 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Mapname</i>	Name of a NAT map.	String of up to 15 characters.
<i>Method1</i> <i>Method2</i>	Encryption and/or authentication protocol for an IPS security association.	esp-des , esp3des , ah-md5 , or ah-sha .
<i>Metric</i>	Hop count to a remote destination.	Integer from 1 to 15.
<i>Minutes</i>	Number of minutes.	Integer from 0 to 240.
<i>ModemName</i>	User-defined long or short name for a modem in the modem table.	Printable ASCII characters.
<i>MTU</i>	Maximum transmission unit. The maximum packet size, in bytes, that an interface can send.	Integer from 100 to 1520.
<i>NM</i>	Alternative netmask notation. The number of high-order bits set to 1.	/n where n is an integer from 0 to 32.
<i>Number</i>	Quantity.	Any number 0 or higher.
<i>Password</i>	PortMaster administrative password.	String of up to 15 printable, nonspace, ASCII characters.
<i>Policyname</i>	Name of a BGP policy statement.	String of up to 16 printable, nonspace, ASCII characters.
<i>Portlabel</i>	Physical port designation for Ethernet subinterfaces.	<ul style="list-style-type: none"> • ether0 or ether1 on an IRX-211. • ether0 on all others.
<i>Portname</i>	Name of service provided by a TCP or UDP port.	For NAT entries, telnet , ftp , tftp , http , dns , or smtp .

Table C-1 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Prefix</i>	IP prefix address.	Dotted decimal notation with ones in high-order bits, and zeros in low-order bits.
<i>Profile</i>	Type of inband signaling for channelized E1.	Integer between 0 and 4 for E1.
<i>Protocol</i>	Type of routing protocol.	bgp, ospf, rip, or static.
<i>RuleNumber</i>	Number indicating the order of a filter rule, or BGP policy statement, or network address translator (NAT) address map entry.	Integer 1 or higher. For filters, the limit is from 1 to 256 for the PortMaster 3 and IRX, and from 1 to 100 for other PortMaster products. For BGP policy rules, the limit is from 1 to 160. For NAT map entries, the limit is from 1 to 20.
<i>S0</i>	Any asynchronous port or ISDN PRI port.	<ul style="list-style-type: none"> • c0 or s0 through s29, depending on PortMaster model. • all —Applies the command simultaneously to all asynchronous or ISDN PRI ports.
<i>S1</i>	Any asynchronous or synchronous port.	<ul style="list-style-type: none"> • s0 through s29 or w1, depending on PortMaster model. • all —Applies the command simultaneously to all asynchronous or synchronous ports.
<i>S10</i>	Any ISDN BRI port.	s0 through s59 , depending on PortMaster model.
<i>Seconds</i>	Number of seconds.	Any number 0 or higher; note that 1 has special meaning for idle timeout commands.

Table C-1 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Sessionid</i>	Identification number of a NAT session.	Integer.
<i>String</i>	Character string.	One or more characters in the ASCII printable character set.
<i>Tag</i>	Community attribute used to identify a BGP community.	A 32-bit number, two 16-bit numbers, or a reserved community keyword.
<i>Tport</i>	TCP/IP port.	Integer from 1 to 65535.
<i>Ticks</i>	Number of 50ms increments of time required to send a packet to the destination network.	Integer.
<i>Uport</i>	User Datagram Protocol (UDP)/IP port.	Integer from 0 to 65535.
<i>Username</i>	Name of user.	String of up to 8 printable ASCII characters.
<i>V0</i>	Any virtual port created for Multichannel Point-to-Point Protocol (PPP) connections.	v0 and up, depending on the number of Multichannel PPP connections made in the PortMaster 3.
<i>W1</i>	Any synchronous port.	<ul style="list-style-type: none">• s1 through s4 or w0 through w63, depending on the PortMaster model.• all—Applies the command simultaneously to all synchronous ports.

TCP and UDP Ports and Services

D

Table D-1 lists 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*.

Table D-1 TCP and UDP Ports and 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)
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
nnntp	119	TCP	Network News Transfer Protocol (NNTP)
nntp	123	TCP	Network Time Protocol (NTP)
nntp	123	UDP	NTP

Table D-1 TCP and UDP Ports and Services (Continued)

Service	Port	Protocol	Description
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
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)

Command Index

A

- add bgp peer 18-4
- add bgp policy 18-5, 18-8
- add dlci (location) 8-33
- add dlci (synchronous port) 6-10
- add filter 13-4
- add host 10-2
- add ipdlci (location) 8-33
- add ipdlci (synchronous port) 6-10
- add ipxdlci (location) 8-33
- add ipxdlci (synchronous port) 6-10
- add ipxroute 16-14
- add location 8-4
- add map 14-3
- add modem 5-5
- add netmask 16-23
- add netuser 7-4
- add ospf area 17-4
- add propagation 16-3
- add route 16-15
- add snmphost any 3-35
- add snmphost none 3-35
- add snmphost reader 3-35
- add snmphost writer 3-35
- add subinterface 4-14
- add user 7-5
- attach S0 5-6
- attach S10 5-6

C

- clear alarm 3-37
- create l2tp tunnel udp 15-2

D

- delete bgp peer 18-7
- delete bgp policy 18-8
- delete bgp summarization 18-9
- delete dlci (location) 8-35
- delete dlci (synchronous port) 6-4
- delete filter 13-4
- delete host 10-2
- delete ipdlci (location) 8-35
- delete ipdlci (synchronous port) 6-4
- delete ipxdlci (location) 8-35
- delete ipxdlci (synchronous port) 6-4
- delete ipxroute 16-16
- delete location 8-5
- delete map 14-4
- delete modem 5-8
- delete nat session 14-5
- delete netmask 16-24
- delete ospf area 17-5
- delete propagation 16-3
- delete route 16-17
- delete snmphost reader 3-38
- delete snmphost writer 3-38
- delete subinterface 4-14

delete user 7-6
dial 2-4
done 2-5

E

erase all-flash 2-6
erase comos 2-6
erase configuration 2-6
erase file 2-6
erase partition 2-6
exit 2-5

H

help 2-7

I

ifconfig 2-9
ifconfig (OSPF) 17-5

P

ping 2-11
pmlogin 2-12
ptrace 2-13
ptrace extended 2-13

Q

quit 2-5

R

reboot 2-15
reset all 2-15
reset bgp 2-15, 18-10
reset console 2-15
reset dialer 2-16
reset l2tp 2-16

reset l2tp stats 15-3
reset l2tp tunnel 15-3
reset M0 2-16, 12-5
reset nat 2-16, 14-6
reset nHandle 2-16
reset nic 2-16
reset Number 2-16
reset ospf 2-16, 17-6
reset p0 2-16
reset propagation 2-16, 16-6
reset S0 2-16
reset S10 2-16
reset V0 2-16, 12-5
reset W1 2-16
rlogin 2-17

S

save all 2-18
save bgp 2-18, 18-11
save console 2-18
save filter 2-18, 13-5
save global 2-18
save host 2-18
save hosts 10-3
save location 2-18, 8-5
save map 14-7
save netmask 2-18, 16-24
save ospf 2-18, 17-7
save P0 2-18
save ports 2-18
save route 2-18, 16-17
save S0 2-18
save snmp 2-18, 3-38
save user 2-18, 7-6
save W1 2-18
set accounting 3-24

set accounting count 3-26
 set accounting interval 3-27
 set all access 5-9
 set all cd 5-11
 set all databits 5-14
 set all dialback_delay 5-17
 set all directory 11-11
 set all dn 11-11
 set all dtr_idle 5-18
 set all extended 5-19
 set all group 5-19
 set all hangup 5-20
 set all host default 5-21
 set all host Ipaddress 3-8, 5-21
 set all host prompt 5-21
 set all idletime 5-22
 set all ifilter 5-24
 set all login network dialin 5-26
 set all login network dialout 5-26
 set all login network twoway 5-26
 set all map 5-27
 set all message 5-28
 set all modem-type 5-29
 set all mtu 5-30
 set all network dialin 5-32
 set all network dialout 5-32
 set all network hardwired 5-33, 11-12
 set all network twoway 5-32
 set all ofilter 5-34
 set all override 5-35
 set all parity 5-36
 set all prompt 5-37
 set all rts/cts 5-39
 set all security 5-40
 set all service_device netdata 5-41
 set all service_device portmaster 5-41

set all service_device rlogin 5-41
 set all service_device telnet 5-41
 set all service_login netdata 5-42
 set all service_login portmaster 5-42
 set all service_login rlogin 5-42
 set all service_login telnet 5-42
 set all speed 5-43
 set all spid 11-14
 set all stopbits 5-44
 set all termtype 5-45
 set all xon/xoff 5-48
 set alternate_auth_server 3-30
 set assigned_address 3-3
 set authentication_server 3-31
 set authentication failover 3-29
 set authentication interval 3-30
 set bgp as 18-11
 set bgp cluster-id 18-12
 set bgp cma 18-13
 set bgp connect-retry-interval 18-14
 set bgp disable 18-14
 set bgp enable 18-14
 set bgp hold-time 18-15
 set bgp id 18-16
 set bgp igp-lockstep 18-16
 set bgp keepalive-timer 18-17
 set bgp peer 18-18
 set bgp policy (acceptance) 18-23
 set bgp policy (advertisement) 18-33
 set bgp policy (injection) 18-29
 set bgp policy blank 18-39
 set bgp summarization 18-40
 set call-check 3-4, 5-38
 set chap 3-6
 set choicenet 3-33
 set choicenet-secret 3-34

set console 2-20
set debug bgp-decision-process 19-2
set debug bgp-errors 19-2
set debug bgp-fsm 19-2
set debug bgp-keepalives 19-2
set debug bgp-max 19-2
set debug bgp-notifications 19-2
set debug bgp-opens 19-2
set debug bgp-packets 19-2
set debug bgp-updates 19-2
set debug ccp-stac 19-4
set debug choicenet 19-5
set debug clock 19-5
set debug Hex 19-5
set debug isdn 19-8
set debug isdn D0 19-8
set debug isdn-dframes 19-8
set debug isdn-l1 D0 19-8
set debug isdn-v120 19-8
set debug l2tp max 19-9
set debug l2tp packets 19-9
set debug l2tp setup 19-9
set debug l2tp stats 19-9
set debug mcppp-event 19-10
set debug mdp-events 19-11
set debug mdp-max 19-11
set debug mdp-status 19-11
set debug nat-ftp 19-12
set debug nat-icmp-err 19-12
set debug nat-max 19-12
set debug nat-rt-interface 19-12
set debug nfas 19-13
set debug off 19-6
set debug ospf-dbdesc 19-14
set debug ospf-error 19-14
set debug ospf-event 19-14
set debug ospf-hello 19-14
set debug ospf-lsa 19-14
set debug ospf-lsu 19-14
set debug ospf-max 19-14
set debug ospf-routing 19-14
set debug ospf-spfcalc 19-14
set debug termination 19-8
set default broadcast 16-18
set default listen 16-18
set default off 16-18
set default on 16-18
set domain 3-7
set endpoint 12-6
set Ether0 address 4-3
set Ether0 broadcast 4-4
set Ether0 ifilter 4-5
set ether0 ip 4-6
set ether0 ipx 4-7
set Ether0 ipxframe 4-8
set Ether0 ipxnet 4-9
set Ether0 nat defaultnapt 14-14
set Ether0 nat inmap 14-14
set Ether0 nat log 14-16
set Ether0 nat outmap 14-14
set Ether0 nat session-direction-fail-action 14-19
set Ether0 nat sessiontimeout 14-17
set Ether0 netmask 16-7
set Ether0 ofilter 4-10
set Ether0 ospf 17-8
set Ether0 ospf accept-rip 17-7
set Ether0 ospf cost 17-8
set Ether0 ospf dead-time 17-8
set Ether0 ospf hello-interval 17-8
set Ether0 rip broadcast 16-19
set Ether0 rip listen 16-19
set Ether0 rip on 16-19

set Ether0 route-filter 16-8
set filter (ICMP) 13-16
set filter (IP) 13-6, 13-7
set filter (IPX) 13-19
set filter (SAP) 13-22
set filter (TCP) 13-10
set filter (UDP) 13-13
set filter blank 13-6
set gateway 16-12
set host 3-8
set ipx 3-9
set ipxfilter 13-19
set ipxgateway 3-10
set isdn-msn 11-4
set isdn-numberauto 11-5
set isdn-numberplan 11-6
set isdn-numbertype 11-7
set isdn-switch (BRI) 11-9
set isdn-switch (PRI) 12-7
set l2tp authenticate-remote 15-6
set l2tp choose-random-tunnel-endpoint 15-7
set l2tp disable 15-4
set l2tp enable 15-4
set l2tp secret 15-8
set Line0 e1 12-11
set Line0 encoding 12-8
set Line0 fractional 12-11
set Line0 framing 12-9
set Line0 group 12-9
set Line0 group channels 12-10
set Line0 inband 12-11
set Line0 isdn 12-11
set Line0 isdn-fractional 12-11
set Line0 loopback 12-13
set Line0 nfes 12-14
set Line0 pcm 12-16
set Line0 signaling 12-17
set Line0 signaling mfr2 12-18
set Line0 t1 12-11
set line2 clock 12-19
set line2 encoding 12-8
set line2 fractional 12-11
set line2 framing 12-9
set line2 group 12-9
set line2 group channels 12-10
set line2 loopback 12-13
set line2 t1 12-11
set location analog 8-6, 12-20
set location automatic 8-7
set location chap 8-8
set location compression 8-9
set location destination 8-10
set location group 8-11
set location high_water 8-12
set location idletime 8-13
set location ifilter 8-14
set location ipxnet 8-15
set location local-ip-address 8-16
set location manual 8-7
set location map 8-17
set location maxports 8-18
set location mtu 8-19
set location multilink 8-20
set location nat defaultnapt 14-14
set location nat inmap 14-14
set location nat log 14-16
set location nat outmap 14-14
set location nat session-direction-fail-action 14-19
set location nat sessiontimeout 14-17
set location netmask 8-21
set location ofilter 8-21
set location on_demand 8-7

set location ospf 17-9
set location ospf cost 17-9
set location ospf dead-time 17-9
set location ospf hello-interval 17-9
set location ospf nbma 17-9
set location ospf point-to-multipoint 17-9
set location ospf wan-as-stub-ptmp 17-9
set location password 8-22
set location protocol 8-23
set location rip broadcast 16-20
set location rip listen 16-20
set location rip on 16-20
set location route-filter 16-8
set location script 8-24
set location telephone 8-26
set location username 8-27
set location v25bis 8-24
set location voice 8-28
set loghost 3-11
set M0 12-20
set M0 lastcall 12-21
set map addressmap 14-8
set map blank 14-11
set map staticaddressmap 14-8
set map static-tcp-udp-portmap 14-12
set maximum pmconsole 3-12
set nameserver 3-13
set namesvc 3-14
set netbios 3-15
set ospf area external 17-12
set ospf area md5 17-13
set ospf area nssa 17-14
set ospf area password 17-15
set ospf area range 17-16
set ospf area stub-default-cost 17-17
set ospf disable 17-18
set ospf enable 17-18
set ospf priority 17-19
set ospf router-id 17-20
set p0 device 9-2
set p0 disabled 9-2
set p0 disconnect 9-3
set p0 extended 9-4
set p0 host 9-4
set p0 service_device netdata 9-5
set p0 service_device portmaster 9-5
set p0 service_device rlogin 9-5
set p0 service_device telnet 9-5
set pap 3-16
set password 3-17
set pool 3-17
set pots 3-18
set reported_ip 3-19
set S0 access 5-9
set S0 address 5-10
set S0 autolog 5-47
set S0 cd 5-11
set S0 compression 5-13
set S0 databits 5-14
set S0 destination 5-15
set S0 device 5-16
set S0 device network dialin 5-16
set S0 device network dialout 5-16
set S0 device network twoway 5-16
set S0 dialback_delay 5-17
set S0 directory 12-22
set S0 dtr_idle 5-18
set S0 extended 5-19
set S0 group 5-19
set S0 hangup 5-20
set S0 host 5-21
set S0 host default 5-21

set S0 host prompt 5-21
set S0 idletime 5-22
set S0 ifilter 5-24
set S0 ipxnet 5-25
set S0 login 5-26
set S0 login network dialin 5-26
set S0 login network dialout 5-26
set S0 login network twoway 5-26
set S0 map 5-27
set S0 message 5-28
set S0 modem-type 5-29
set S0 mtu 5-30
set S0 nat defaultnapt 14-14
set S0 nat inmap 14-14
set S0 nat log 14-16
set S0 nat outmap 14-14
set S0 nat session-direction-fail-action 14-19
set S0 nat sessiontimeout 14-17
set S0 netmask 5-31, 16-7
set S0 network dialin 5-32
set S0 network dialout 5-32
set S0 network hardwired 5-33
set S0 network twoway 5-32
set S0 ofilter 5-34
set S0 ospf 17-9
set S0 ospf cost 17-9
set S0 ospf dead-time 17-9
set S0 ospf hello-interval 17-9
set S0 ospf nbma 17-9
set S0 ospf point-to-multipoint 17-9
set S0 ospf wan-as-stub-ptmp 17-9
set S0 override 5-35
set S0 parity 5-36
set S0 prompt 5-37
set S0 protocol 5-38
set S0 rip broadcast 16-19
set S0 rip listen 16-19
set S0 rip on 16-19
set S0 route-filter 16-8
set S0 rts/cts 5-39
set S0 security 5-40
set S0 service_device netdata 5-41
set S0 service_device portmaster 5-41
set S0 service_device rlogin 5-41
set S0 service_device telnet 5-41
set S0 service_login netdata 5-42
set S0 service_login portmaster 5-42
set S0 service_login rlogin 5-42
set S0 service_login telnet 5-42
set S0 speed 5-43
set S0 stopbits 5-44
set S0 termtype 5-45
set S0 twoway 5-46
set S0 twoway network dialin 5-46
set S0 twoway network dialout 5-46
set S0 twoway network twoway 5-46
set S0 username 5-47
set S0 xon/xoff 5-48
set S10 address 5-10
set S10 autolog 5-47
set S10 destination 11-10
set S10 device 5-16
set S10 dialback_delay 5-17
set S10 directory 11-11
set S10 dn 11-11
set S10 extended 5-19
set S10 group 5-19
set S10 hangup 5-20
set S10 host 5-21
set S10 host default 5-21
set S10 host prompt 5-21
set S10 idletime 5-22

set S10 ifilter 5-24
set S10 login network dialin 5-26
set S10 login network dialout 5-26
set S10 login network twoway 5-26
set S10 message 5-28
set S10 network dialin 5-32
set S10 network dialout 5-32
set S10 network hardwired 11-12
set S10 network twoway 5-32
set S10 ofilter 5-34
set S10 ospf 17-9
set S10 ospf cost 17-9
set S10 ospf dead-time 17-9
set S10 ospf hello-interval 17-9
set S10 ospf nbma 17-9
set S10 ospf point-to-multipoint 17-9
set S10 ospf wan-as-stub-ptmp 17-9
set S10 prompt 5-37
set S10 security 5-40
set S10 service_device netdata 5-41
set S10 service_device portmaster 5-41
set S10 service_device rlogin 5-41
set S10 service_device telnet 5-41
set S10 service_login netdata 5-42
set S10 service_login portmaster 5-42
set S10 service_login rlogin 5-42
set S10 service_login telnet 5-42
set S10 speed 11-13
set S10 spid 11-14
set S10 termtype 5-45
set S10 twoway network dialin 5-46
set S10 twoway network dialout 5-46
set S10 twoway network twoway 5-46
set S10 username 5-47
set sapfilter 13-22
set secret 3-32
set serial-admin 3-20
set snmp 3-39
set snmp readcommunity 3-40
set snmp writecommunity 3-40
set subinterface address 4-15
set subinterface broadcast 4-16
set subinterface netmask 4-16
set subinterface port-name 4-17
set syslog 3-20
set sysname 2-21
set telnet 3-22
set user address 7-7
set user callback 7-9
set user compression 7-8
set user destination 7-7
set user dialback 7-9
set user host 7-10
set user idle 7-11
set user ifilter 7-12
set user ipxnet 7-14
set user local-ip-address 7-15
set user map 7-16
set user maxports 7-17
set user mtu 7-18
set user nat defaultnapt 14-14
set user nat inmap 14-14
set user nat log 14-16
set user nat outmap 14-14
set user nat session-direction-fail-action 14-19
set user nat sessiontimeout 14-17
set user netmask 7-19
set user-netmask 16-13
set user ofilter 7-20
set user ospf 17-9
set user ospf cost 17-9
set user ospf dead-time 17-9

set user ospf hello-interval 17-9
 set user ospf nbma 17-9
 set user ospf point-to-multipoint 17-9
 set user ospf wan-as-stub-ptmp 17-9
 set user password 7-21
 set user protocol 7-21
 set user rip broadcast 16-21
 set user rip listen 16-21
 set user rip on 16-21
 set user route-filter 16-8
 set user service 7-22
 set user session-limit 7-23
 set W1 address 6-5
 set W1 annex-d 6-6
 set W1 cd 6-7
 set W1 compression 6-8
 set W1 destination 6-9
 set W1 dlci 6-10
 set W1 extended 6-12
 set W1 group 6-12
 set W1 hangup 6-13
 set W1 idletime 6-14
 set W1 ifilter 6-15
 set W1 ipxnet 6-16
 set W1 lmi 6-17
 set W1 mtu 6-18
 set W1 nat defaultnapt 14-14
 set W1 nat inmap 14-14
 set W1 nat log 14-16
 set W1 nat outmap 14-14
 set W1 nat session-direction-fail-action 14-19
 set W1 nat sessiontimeout 14-17
 set W1 netmask 6-19, 16-7
 set W1 network dialin 6-20
 set W1 network dialout 6-20
 set W1 network hardwired 6-20
 set W1 network twoway 6-20
 set W1 ofilter 6-21
 set W1 ospf 17-9
 set W1 ospf cost 17-9
 set W1 ospf dead-time 17-9
 set W1 ospf hello-interval 17-9
 set W1 ospf nbma 17-9
 set W1 ospf point-to-multipoint 17-9
 set W1 ospf wan-as-stub-ptmp 17-9
 set W1 protocol 6-22
 set W1 rip broadcast 16-19
 set W1 rip listen 16-19
 set W1 rip on 16-19
 set W1 route-filter 16-8
 set W1 speed 6-23
 show alarms 3-41
 show all 2-22
 show arp 2-24
 show bgp memory 18-43
 show bgp next-hop 18-44
 show bgp paths 18-46
 show bgp peers 18-49
 show bgp peers packets 18-49
 show bgp peers verbose 18-49
 show bgp policy 18-55
 show bgp summarization 18-56
 show Ether0 4-11
 show files 2-25
 show filter 13-24
 show global 2-28
 show ipxfilter 13-24
 show ipxroutes 16-25
 show isdn 11-15
 show isdn d0 11-15
 show isdn S0 11-15
 show l2tp global 15-9

show l2tp sessions 15-9
show l2tp stats 15-9
show l2tp tunnels 15-9
show Line0 12-23
show location 8-29
show M0 12-27
show map 14-20
show mcppp 12-29
show memory 2-31
show modem 5-49
show modems 12-30
show modules 2-32
show nat mapusage 14-21
show nat sessions 14-22
show nat statistics 14-24
show netconns 2-33
show netstat 2-34
show nfas 12-31
show nfas stat 12-34
show ospf areas 17-21
show ospf links 17-24
show ospf neighbor 17-27
show p0 2-35
show pots 3-23
show propagation 16-26
show routes 16-27, 17-29, 18-58
show route to-dest 16-29
show S0 2-35
show S10 2-35
show sap 2-38
show sapfilter 13-24
show sessions 2-39
show syslog 2-40
show table 2-41
show table bgp 18-49
show table filter 2-41, 13-25

show table host 10-3
show table location 8-32
show table map 14-26
show table modem 5-50
show table netmask 16-31
show table ospf 17-21
show table snmp 3-42
show table subinterface 4-18
show table user 7-24
show user 7-25
show W1 6-24

T

telnet 2-42
tftp get 2-43
traceroute 2-44

V

version 2-45

Subject Index

A

- access filter 5-9
 - login users 5-24
- access override 5-9
- accounting packets, RADIUS 3-26
- accounting packets, setting intervals 3-27
- accounting server daemon 3-25
- accounting server, RADIUS 3-24
 - retry count 3-26
 - retry interval 3-27
- adding
 - BGP peer 18-4
 - BGP policy 18-5, 18-8
 - BGP summarization 18-6
 - DLCI to DLCI table 6-10, 8-33
 - filter to filter table 13-4
 - host to host table 10-2
 - IPX route 16-14
 - location to location table 8-4
 - modem to modem table 5-5
 - NAT maps 14-3
 - netmask to netmask table 16-23
 - netuser to user table 7-4
 - OSPF area 17-4
 - propagation 16-3
 - SNMP host 3-35
 - static route to IP route table 16-15
 - subinterface 4-14
 - user to user table 7-5
- address maps
 - attaching to an interface 14-14
 - deleting contents 14-11
 - deleting NAT map rules 14-11
 - displaying contents 14-20
 - dynamic 14-8
 - rule entry 14-8
 - rule removal 14-9
 - saving to nonvolatile RAM 14-7
 - specifying direction 14-14
 - static 14-8
- administrative logins
 - disabling 3-20
 - enabling 3-20
 - using serial ports 3-20
- administrative password 1-1
- advertising network routes 17-3, 17-16
- alarms 3-37, 3-41
- A-law encoding 12-16
- am 14-13
- analog modems, enabling 8-6, 12-20
- analog port, enabling 3-18
- Annex-D polling interval 6-6
- area border router 17-4
- ARP tables for interface 2-24
- assigned base address 3-3
- assigned pool size 3-17
- asynchronous port commands
 - description 5-5
 - summary 5-2
- asynchronous ports
 - assigning to groups 5-19
 - automatic login name 5-47
 - callback delay 5-17
 - carrier detect signal 5-11
 - configuring 5-1
 - data bits 5-14
 - destination address 5-15
 - device service 5-16, 5-41
 - displaying data 5-1
 - extended mode 5-19
 - hardware flow control 5-39
 - hardwired network 5-33

- idle time 5-22
- input filter 5-24
- local IP address 5-10
- login message 5-28
- login prompt 5-37
- modem pools 5-19
- network hardwired for IPX networks 5-25
- network hardwired, transport protocol 5-38
- output filter 5-34
- parity checking 5-36
- RTS/CTS 5-45
- security level 5-40
- stop bits 5-44
- TCP/IP header compression 5-13
- terminal type 5-45
- transport protocol 5-38
- two-way device 5-46
- types 5-4
- user login 5-26
- attached devices, to PortMaster 5-6
- authentication
 - CHAP 3-6
 - failover 3-29
 - L2TP 15-2, 15-6
 - PAP 3-16
 - RADIUS 3-31
 - RADIUS, alternate 3-28
- autonomous system
 - export summary information to 18-40
 - setting identifier 18-11

B

- backbone area 17-4
- backup router 17-19
- BACP 11-11, 12-23
- Bandwidth Allocation Control Protocol. See BACP
- Bandwidth Allocation Protocol. See BAP
- bandwidth on demand 11-11, 12-23
- BAP 11-11, 12-23
- Basic Rate Interface. See ISDN

- basic routing configuration 16-1
- baud rate 5-43, 11-13
- BBS 5-18
- BGP
 - adding peers to routing table 18-4, 18-7
 - clearing a policy list 18-39
 - CMAS 18-13, 18-40
 - community 18-25, 18-31, 18-35, 18-57
 - community information 18-41
 - confederation member autonomous system.
 - See BGP, CMAS
 - confederation member, setting ID 18-13
 - connection retry interval 18-14
 - creating policy 18-5, 18-8
 - defining an acceptance policy rule 18-23
 - defining an advertisement policy rule 18-33
 - defining an injection policy rule 18-29
 - degree of preference 18-23, 18-47
 - displaying information 18-1
 - displaying memory usage 18-43
 - displaying next hop information 18-44
 - displaying path information 18-46
 - displaying peer information 18-49
 - displaying policy information 18-55
 - displaying route summaries 18-56
 - enabling or disabling 18-14
 - hold time 18-15
 - keepalive timer 18-17
 - local preference 18-37, 18-41, 18-47
 - lockstep feature 18-16
 - multiexit discriminator 18-23, 18-33, 18-48
 - peer 18-4, 18-7, 18-18
 - reducing numbers of advertised routes 18-28
 - resetting 18-10
 - route reflector setup 18-12
 - route summarization 18-6, 18-40, 18-42
 - saving changes 18-11
 - setting autonomous system identifier 18-11
 - setting identifier 18-16
- BGP commands summary 18-2
- BGP community, setting identifier tag 18-25, 18-31, 18-35

BGP policy
 clearing 18-39
 creating 18-5, 18-8
 defining acceptance rule 18-23
 defining advertisement rule 18-33
 defining injection rule 18-29
bidirectional communications 5-18
Border Gateway Protocol. See BGP
BRI. See ISDN
broadcast routing 16-19
bulletin board service 5-18

C

callback delay 5-17
callback login user
 location 7-9
 telephone number 7-9
call-check 3-4, 15-1, 15-5
carrier detect signal. See DCD
Challenge Handshake Authentication Protocol.
 See CHAP
channel rate 12-9
channelized E1 12-12, 12-18
channelized T1 12-12, 12-17
CHAP
 dial-in users 3-6
 locations 8-8
 system name for 2-21
ChoiceNet
 authentication 3-33
 client configuration 3-33
 commands 3-33
 debugging 19-5
 secret 3-34
 server 3-33
 server configuration 3-33
 shared secret 3-34
classes, PortMaster xv
clocking
 E1 12-12
 internal and external 12-19

 T1 12-12
 T1 card 12-19
cluster ID for route reflector 18-12
command line interface
 introduction to 1-1
 starting 1-1
COMMAND status 2-23
commands
 basic B-1
 repeating last B-1
ComOS
 displaying functional modules 2-32
 erasing 2-6
 upgrading 2-43
 version 2-45
companding 12-16
compression, Van Jacobson and Stac LZS 5-49,
 7-8, 8-9
CONNECTING status 2-23
connections, two-way network 5-16
contact information
 CALA xv
 Europe, Middle East, and Africa xiv
 mailing lists xv
 North America, Latin America, and Asia
 Pacific xv
conventions in this manual xiii
cost setting
 default, for OSPF stub area 17-17
 Ethernet interface 17-8, 17-9

D

D channel
 backup 12-14
 primary 12-14
 secondary 12-14
Data Carrier Detect. See DCD
data link connection identifier. See DLCI
data over voice 3-18
databits, setting for asynchronous ports 5-14
DCD 5-11, 6-7

- dead time, Ethernet interface 17-8, 17-10
- debug commands, summary 19-1
- debugging
 - adjacency formation between OSPF neighbors 19-14
 - ChoiceNet events 19-5
 - clearing all debug settings 19-3, 19-6
 - complete OSPF information 19-14
 - digital modems 19-11
 - from a terminal session 2-13
 - hexadecimal commands 19-5
 - I/O events 19-6
 - interactivity between ComOS and nonvolatile RAM 19-6
 - ISDN information 19-8
 - L2TP 19-9
 - link state advertisement packets 19-14
 - link state update packets 19-14
 - LMI and Annex-D requests and acknowledgments 19-6
 - Multichassis PPP 19-10
 - NAT 19-12
 - NFAS 19-13
 - OSPF database and routing table exchanges 19-14
 - OSPF errors in configuration 19-14
 - OSPF events 19-14
 - OSPF hello packets 19-14
 - RIP routing table updates 19-6
 - routing 16-29
 - Stac LZS messages 19-4
 - Telnet negotiation options 19-6
 - termination causes 19-6
 - updates to the ARP cache 19-6
- dedicated network connection 5-33, 11-13
- default route information 16-18
- degree of preference, BGP 18-47
 - for acceptance 18-23
- deleting
 - BGP peer 18-6
 - BGP policy 18-8
 - BGP summarization 18-9
 - DLCI from DLCI table 6-4, 6-10, 8-35
 - filter from filter table 13-4
 - host from host table 10-2
 - location from location table 8-5
 - modem from modem table 5-8
 - NAT maps 14-4
 - NAT sessions 14-5
 - netmask from netmask table 16-24
 - OSPF area 17-5
 - propagation 16-3
 - SNMP host 3-38
 - static route from IP route table 16-17
 - static route from IPX route table 16-16
 - subinterface 4-14
 - timestamping debug messages 19-6
 - user from user table 7-6
- designated router 17-19
- device designation 5-16
- device service
 - netdata 5-41, 9-5
 - PortMaster 5-41, 9-5
 - rlogin 5-41, 9-5
 - Telnet 5-41, 9-5
- dial group 5-19
- dial script 8-24
- dialback. See callback
- dial-in network 6-20
- dialing to a network location 2-4
- dial-out network 6-20
- digital modems
 - ADMIN mode for hot swap 12-21
 - debugging 19-11
 - display status 2-32
- directory number 11-11, 12-22
- disconnecting a dial-in user 5-22
- DISCONNECTING status 2-23
- displaying
 - NAT maps 14-26
 - NAT sessions 14-22
- displaying contents of address maps 14-20
- displaying TCP/UDP resources for a port. 14-21

- DLCI
 - adding to location 8-33
 - adding to synchronous port 6-10
 - deleting 6-4, 8-35
 - feature 8-34
 - list 6-6, 6-17
 - table commands 8-33
- DNS 3-7, 3-14
- document conventions xiii, xiv
- domain name 3-6
- Domain Name System. See DNS
- DOV 3-18
- DTR
 - dropped signal 5-20
 - idle 5-18
 - signal 5-18, 5-20
- E**
- E & M wink start protocol 12-17
- E1 lines
 - displaying status 12-23
 - encoding method 12-8
 - framing format 12-9
 - pulse code modulation 12-16
 - services 12-1
 - setting use 12-11
 - signaling for channelized E1 12-18
- encoding method 12-8
- end point discriminator, setting for Multichassis PPP 12-6
- erasing nonvolatile RAM 2-6
- ESTABLISHED status 2-23
- establishing login sessions 5-42
- Ethernet
 - 802.2 protocol 2-9, 4-8
 - 802.2_ii protocol 2-9, 4-8
 - 802.3 protocol 2-9, 4-8
 - configuration values 4-11
 - configuring for OSPF 17-8
 - II protocol 2-9, 4-8
 - input filter 4-5
 - IP protocol 4-6
 - IPX protocol 4-7
 - output filter 4-10
- Ethernet commands
 - description 4-3
 - subinterface commands 4-13
 - summary 4-2
- Ethernet interface
 - configuring 2-10, 4-1
 - displaying configuration 4-1
- Ethernet subinterface
 - adding 4-14
 - associating configuration with port 4-17
 - broadcast address 4-16
 - deleting 4-14
 - displaying configuration 4-13
 - IP address 4-15
 - IP netmask 4-15
 - netmask 4-16
 - port 4-17
- exiting the command line interface 2-5
- extended mode
 - asynchronous port 5-19
 - synchronous ports 6-12
- external clocking 12-19
- external routes, propagating 17-12
- F**
- failover
 - enabling 3-29
 - interval 3-30
- file statistics 2-25
- filter table
 - displaying data 2-42
 - saving changes 13-5
- filter table commands
 - description 13-4
 - summary 13-2
- filters
 - adding 13-4
 - configuring ICMP 13-16

- configuring IP 13-6
- configuring IPX 13-19
- configuring SAP 13-22
- configuring TCP 13-10
- configuring UDP 13-13
- deleting 13-4
- displaying content 13-24
- displaying data 13-1
- emptying 13-6
- for dial-in locations 5-24
- for dial-out locations 5-24
- for routes 16-8
- input 4-5, 6-15
- using in ptrace 2-13

Flash RAM. See nonvolatile RAM

foreign exchange station 12-17

fractional E1

- enabling 12-11
- grouping channels 12-10

fractional ISDN

- enabling 12-11
- grouping channels 12-9

fractional T1

- enabling 12-11
- grouping channels 12-10

Frame Relay 6-10, 6-22, 8-23, 8-34

- subinterfaces 8-34

FTP, displaying NAT sessions 14-22

FXS loop start protocol 12-17

G

- gateway address 16-3, 16-12
- general commands 2-1
- global commands, summary 3-1
- global settings 2-28
 - displaying 3-1
- group number 5-19, 6-12, 8-11

H

- hardware flow control 5-39
- hardwired network 6-20
- hello interval for Ethernet interface 17-8, 17-10
- help commands 2-8
 - !! B-1
- help file, recreating 2-43
- high-water mark 8-12, 8-18
- host
 - alternate 3-8
 - default 3-8, 5-21
 - device 5-16
 - device service 3-8, 5-21
 - for login sessions 3-8, 5-21
 - override parameters 5-35
 - prompt 5-21
- host table
 - adding host 10-2
 - configuring 10-1
 - deleting host 10-2
 - displaying 10-1
 - saving 10-3
 - summary of commands 10-1
- hostname lookups 3-7
- HOSTNAME status 2-23
- hot-swappable modem 12-21
- hot-swappable T1 card 12-1

I

ICMP

- echo request packets 2-11
- filter, configuring 13-16
- message types 13-17
- time expired packets 2-44

IDLE status 2-23

idle time

- asynchronous port 5-22
- location 8-13
- NAT session 14-17, 14-24
- synchronous port 6-14
- user 7-11

- ifconfig 2-9, 17-5
- IGP routes, using to advertise to an external BGP
 - peer 18-16
- imed 18-26
- in.pmd daemon 5-16, 5-42, 9-2
- inband signaling
 - E & M wink start protocol 12-17
 - FXS loop start protocol 12-17
- INITIALIZING status 2-23
- input filter
 - location 8-14
 - user 7-12
- internal clocking 12-19
- Internet Control Message Protocol. See ICMP
- Internet Network Information Center 18-11
- InterNIC, supplier of autonomous system
 - numbers 18-11
- IP address
 - assigned pool size 3-17
 - asynchronous 5-10
 - base 3-3
 - ChoiceNet server 3-33
 - default 5-21
 - Ethernet 4-3
 - format for NAT 14-9
 - gateway 16-12
 - loghost 3-11
 - NAT maps 14-8
 - network user 7-7
 - pool 3-3
 - private 14-9
 - RADIUS accounting server 3-25
 - RADIUS authentication server 3-31
 - remote router 5-15
 - reported 3-19
 - synchronous 6-5
- IP broadcast address 4-4
- IP filter, configuring 13-6
- IP netmask
 - asynchronous 5-31
 - user 7-19
- IPX
 - filter, configuring 13-19
 - frame type 4-8
 - gateway 3-10
 - NetBIOS 3-15
- IPX network number 6-16
- IPX networks
 - asynchronous port, network hardwired 5-25
 - Ethernet 4-7
 - Ethernet encapsulation 4-8
 - location 8-15
 - synchronous 6-16
 - user 7-14
- IPX route table
 - adding routes 16-14
 - deleting routes 16-16
 - displaying 16-25
- ISDN
 - automatic number plan determination 11-5
 - configuring BRI ports 11-1
 - configuring PRI 12-1
 - debugging 19-8
 - description of BRI commands 11-4
 - description of PRI commands 12-4
 - directory number for B channels 12-22
 - displaying BRI port data 11-1
 - displaying PRI port data 12-2
 - displaying status of BRI ports 11-15
 - encoding method for PRI line 12-8
 - leased line 11-12
 - number plan 11-6
 - number type 11-7
 - pulse code modulation for PRI line 12-16
 - setting fractional lines 12-11
 - setup of PRI line 12-11
 - summary of BRI commands 11-1
 - summary of PRI commands 12-3
 - supported BRI switches 11-9
 - supported PRI switches 12-7

L

L2TP

- authentication 15-2, 15-6
- creating a manual tunnel 15-2
- debugging 19-9
- disabling 15-4
- displaying session information 15-9
- enabling 15-4
- multiple redundant tunnel endpoints 15-7
- password 15-8
- RADIUS accounting 15-5
- resetting tunnels 15-3
- secret 15-8
- troubleshooting 15-3

L2TP access concentrator. See LAC

L2TP network server. See LNS

LAC 15-1

- enabling 15-4

last call 12-21

Layer 2 Tunneling Protocol. See L2TP

leased line ISDN 11-12

lines

- analog to digital 12-16
- channels 12-10
- encoding 12-8
- framing 12-9
- groups 12-9
- loopback 12-13
- setting 12-11
- setting E1 12-11
- setting fractional 12-11
- setting inband 12-11
- setting T1 12-11

listen routing 16-19

LMI polling interval 6-17

LNS 15-1

- enabling 15-4

local IP address

- asynchronous port 5-10
- for outsource NAT 14-9, 14-15

location 8-16

synchronous port 6-5

user 7-15

Local Management Interface 6-17

local preference, BGP

displaying 18-47

for advertisement 18-33

location

automatic dial scripting 8-26

CHAP configuration 8-8

configuring 8-7

destination address 8-10

dial script 8-24

displaying 8-29

force voice call 8-28

high-water mark 8-12

idle time 8-13

input filter 8-14

IPX network 8-15

local IP address 8-16

maximum dial-out ports 8-18

MTU 8-19

multilink 8-20

netmask 8-21

output filter 8-21

password 8-22

port groups 8-11

protocol 8-23

routing 16-20

Stac LZS compression 8-9

TCP/IP header compression 8-9

telephone number for dial-out 8-26

username 8-27

location table

adding locations 8-4

configuring 8-1

deleting locations 8-5

displaying 8-1

saving changes 8-5

location table commands summary 8-1

lockstep, matching advertised route to BGP peer
18-16

- logging NAT sessions 14-9, 14-16
- loghost address 3-11
- login
 - asynchronous port 5-26
 - host 5-21
 - message 5-28
 - name, automatic 5-47
 - prompt 5-21, 5-28, 7-11
 - prompt, asynchronous ports 5-37
 - service 5-42
- loopback, enabling on T1 or E1 lines 12-13
- Lucent technical support, contacting xiv

M

- MAC address
 - displaying 4-11
 - DLCI IPX node 6-10, 8-33
 - static IPX routing 16-14
- mailing lists, subscribing to xv
- mapping, NAT 14-10
- maps, NAT
 - adding 14-3
 - addresses 14-9
 - blank 14-15
 - defining 14-8
 - deleting 14-4
 - displaying 14-20
 - saving 14-7
 - static 14-12
 - table 14-26
- maximum transmission unit. *See* MTU
- MCPPP
 - debugging 19-10
 - displaying neighbors 12-29
 - enabling 12-6
 - resetting a virtual port 12-5
- MD5 authentication
 - CHAP for a location 8-8
 - OSPF 17-13

- MED 18-48
 - displaying 18-48
 - input for acceptance 18-23
 - output for advertisement 18-33
- memory
 - BGP usage 18-44
 - system, displaying 2-31
- MFR2 signaling 12-18
- modem card, replacing 12-21
- modem control 5-11
- modem initialization string 5-6
- modem name
 - long 5-5
 - short 5-5, 5-49
- modem switch 12-7
- modem table
 - adding modem 5-5
 - configuration 5-49
 - deleting modem 5-8
 - displaying 5-51
- modems
 - configuring 5-6
 - digital. *See* digital modems
 - resetting 12-5
- MSN 11-4
- MTU
 - location 8-19
 - synchronous port 6-18
 - user 7-18
- Multichassis PPP. *See* MCPPP
- multiexit discriminator. *See* MED
- Multifrequency R2 signaling 12-18
- multiline load-balancing 7-17, 8-20
- Multilink PPP 7-17, 8-20
- Multilink V.120 7-17
- multiple subscriber network 11-4

N

- name server 3-14
- name service, selecting 3-14
- NAPT 14-1

- NAT 14-1, 14-24
 - adding a map 14-3
 - address map 14-8
 - basic 14-1
 - blank map 14-11
 - debugging 19-12
 - defining maps 14-8
 - deleting active sessions 14-5
 - deleting maps 14-4
 - direction of session 14-23
 - displaying a map 14-20
 - displaying map contents 14-20
 - displaying maps 14-26
 - displaying session information 14-22
 - displaying sessions 14-22
 - displaying statistics 14-24
 - displaying TCP/UDP resources 14-21
 - displaying use 14-21
 - failed translations 14-24
 - map table 14-26
 - mapping 14-10
 - outsource 14-1, 14-10, 14-15
 - outsource mode 14-1
 - outsource, enabling 14-14
 - resetting 14-6
 - saving a map 14-2
 - session failure action 14-19
 - session identification number 14-23
 - session timeout 14-17
 - session type 14-23
 - static map 14-12
 - static map entry for port 14-12
 - statistics 14-24
 - translated IP addresses 14-24
- NAT maps, rule removal 14-9
- negotiated address 7-7
- netdata login service 5-41, 5-42
- netmask
 - adding 16-23
 - deleting 16-24
 - hardwired asynchronous port 5-31
 - location 8-21
 - saving configuration 16-24
 - setting for specified interface 16-7
 - subinterface 4-16
 - synchronous port 6-19
- netmask table
 - description of commands 16-22
 - displaying 16-31
- network
 - connections 2-33
 - connections, two-way 5-16
 - routes 2-35, 16-27, 17-29, 18-58
 - statistics 2-33
- network address port translation. See NAPT
- network address translator. See NAT
- network hardwired port
 - asynchronous 5-34
 - MTU 5-27, 5-30
 - netmask 5-31
 - transport protocol 5-38
- Network Information Service. See NIS
- network interface statistics, displaying 2-34
- network service
 - netdata 5-42
 - PortMaster 5-42
 - rlogin 5-42
 - Telnet 5-42
- network type
 - dial-in 6-20
 - dial-out 6-20
 - hardwired 6-20
 - two-way 6-20
- NetworkCare
 - technical support xiv
 - training xv
- NFAS 12-14
 - debugging 19-13
 - displaying history 12-33
 - displaying information 12-31
 - displaying status of calls 12-34
- NIS 3-7, 3-14
- non-facility associated signaling. See NFAS.
- nonvolatile memory. See nonvolatile RAM

nonvolatile RAM
 debugging 19-6
 erasing 2-6

NO-SERVICE status 2-23

not-so-stubby area. See NSSA

Novell NetWare

 Version 3.11 2-9, 4-8

 Version 4.0 2-9, 4-8

NSSA 17-14

 default cost 17-17

number plan 11-5, 11-6

O

omed 18-37

online help 2-7

Open Shortest Path First. See OSPF

OSPF

 adding area 17-4

 advertising router 17-26

 asynchronous interface 17-9

 authentication key 17-21, 17-22

 configuring 17-1

 debugging 19-14

 deleting area 17-9

 displaying configured areas 17-21

 displaying information 17-1

 displaying neighbors 17-27

 displaying summary of links 17-24

 enabling or disabling 17-8

 Ethernet interface 17-8

 examples of ifconfig output 17-5

 external routes 17-23

 link ID 17-26

 MD5 authentication 17-13

 NSSA 17-14

 priorities of designated and backup routers
 17-19

 range and type of route propagation 17-9

 RIP routing 17-9

 route propagation 17-9

 router ID 17-20

 saving changes 17-7

 stub area 17-12

 stub area default cost 17-17

 stub area default route 17-17

 synchronous interface 17-9

 transit area 17-12

 Type 1 external routes 17-14

 Type 2 external routes 17-7, 17-14

OSPF area

 adding 17-4

 default route 17-12

 deleting 17-5

 network range 17-23

 range 17-9

OSPF commands

 description of 17-4

 summary 17-2

OSPF Ethernet interface

 cost 17-8, 17-9

 dead time 17-8, 17-10

 enabling 17-8

 hello interval 17-8, 17-10

output filter

 Ethernet 4-10

 location 8-21

 synchronous port 6-21

 user 7-20

outsource, NAT 14-1, 14-10, 14-15

P

PAP

 authentication 3-16

 configuration 3-16

parallel port

 configuration 9-1

 device 9-5

 disabling 9-2

 displaying configuration 9-1

 extended mode 9-4

 host 9-4

 services 9-5

- parallel port commands
 - description 9-2
 - summary 9-1
- parity checking 5-36
- password
 - setting L2TP tunnel 15-8
 - setting location 8-22
 - setting user 7-21
- Password Authentication Protocol. See PAP
- PASSWORD status 2-23
- peer
 - BGP 18-4, 18-7, 18-18
 - requirement for meshing 18-21
- peers, fully-meshed 18-21
- permanent network connection 5-33, 11-12
- PHONE port
 - displaying 3-23
 - setting 3-18
- ping 2-11
- PMVision vii
- Point-to-Point Protocol. See PPP
- policy, creating for BGP 18-8
- port idle time 5-22
- port session information 2-39
- PortMaster
 - administrative password 1-1
 - debug commands 19-5
 - in.pmd daemon 5-16, 9-2
 - IP broadcast address 4-4
 - login service 2-12, 5-41, 5-42
 - new software releases xiv
 - rebooting 1-2
 - shared device 5-17
 - software upgrades xiv
 - system console 2-20
 - training xv
 - uptime 2-45
- PortMaster 3
 - line use 12-11
- portmaster-announce mailing list xvi
- portmaster-radius mailing list xvi
- portmaster-users mailing list xv

- PPP
 - asynchronous control map 5-49, 7-16, 8-17
 - connections 5-30
 - negotiated address 7-7
 - negotiation 3-19
 - protocol 5-38, 6-22, 7-21, 8-23
- PRI. See ISDN
- Primary Rate Interface. See ISDN
- printer port. See parallel port
- propagating external routes 17-12
- propagation rules, displaying 16-26
- ptrace 2-13

Q

- quitting the command line interface 2-5

R

- R2 signaling 12-18
- RADIUS
 - accounting packets 3-26
 - accounting server 3-33
 - authentication failover 3-29
 - authentication, secondary 3-32
 - call-check 3-4
 - client configuration 3-24
 - filters 5-24
 - interval between accounting packet transmissions 3-27
 - port-limit attribute 7-17
 - security 5-40
 - shared secret 3-32
- RADIUS accounting, and L2TP 15-5
- reboot 2-15
- redundant L2TP tunnel endpoints 15-7
- references ix
 - books xi
 - RFCs ix
- releases, new software xiv
- remote login 2-17
- reported IP address 3-19
- Requests for Comments. See RFC

resetting

- BGP 18-10
- console 2-15
- dialer 2-16
- ISDN channel 2-16
- L2TP 15-3
- modems 12-5
- NAT 14-6
- network identifier 2-16
- NIC controller 2-16
- OSPF interface 17-6
- ports 2-15
- propagation 16-6
- virtual ports 12-5

RFC

- list of RFCs ix

RIP routing 17-9

- enabling on specified interface 16-19

rlogin service 5-41, 5-42

route filter 16-8

- effects 16-9

route gateway 16-12

route propagation 17-16

route reduction in BGP 18-24

route reflector setup 18-12

route table

- adding routes 16-15
- deleting routes 16-17
- saving 16-15

route, tracing 2-15, 16-29

routing information, displaying 16-1

routing loops, preventing 16-4

routing options 16-18

S

sam 14-8

SAP filter, configuring 13-22

SAP, PortMaster information 2-38

saving configurations 2-19

script for dialing 8-24

sdfa 14-19

secret

- ChoiceNet 3-34

- RADIUS 3-32

security level 5-40

security, enabling and disabling 5-40

Serial Line Internet Protocol. See SLIP

Service Advertising Protocol. See SAP

service profile identifier 11-14

session time limit 7-23

session timeout 14-17

shared secret

- ChoiceNet 3-34

- RADIUS 3-32

Simple Network Management Protocol. See

- SNMP

SLIP

- connections 5-30

- dialout configuration 8-22, 8-26, 8-27

- notification 3-19

- protocol 5-38, 6-22, 7-21, 8-23

SNMP

- alarms 3-37, 3-41

- configuration 3-35

- host, deleting 3-38

- host, specifying 3-35

- parameters, saving 3-38

- read/write strings 3-40

- support, enabling 3-39

SNMP table, displaying 3-42

software flow control 5-48

software, new releases and upgrades xiv

SPID number 11-14

Stac LZS compression 5-13, 6-8, 7-8, 8-9

- debugging 19-4

static NAT map entry for ports 14-12

static routing commands 16-14

status

- COMMAND 2-23

- CONNECTING 2-23

- DISCONNECTING 2-23

- ESTABLISHED 2-23

- HOSTNAME 2-23

- IDLE 2-23
- INITIALIZING 2-23
- NO-SERVICE 2-23
- PASSWORD 2-23
- USERNAME 2-23
- stop bits 5-44
- stub area
 - default route to 17-17
 - defining 17-12
- stupm 14-12
- subinterface, Ethernet 4-13
- summarization 18-6
- switches
 - supported for ISDN BRI 11-9
 - supported for ISDN PRI 12-7
- synchronous
 - hardwired network 11-12
 - IPX network 6-16
 - modem pools 6-12
 - reference speed 6-23
- synchronous port commands
 - description 6-3
 - summary 6-2
- synchronous ports
 - Annex-D polling interval 6-6
 - carrier detect signal 6-7
 - compression 6-8
 - configuring 6-1
 - destination IP address 6-9
 - displaying configuration 6-24
 - displaying data 6-1
 - DTR signal 6-13
 - extended mode 6-12
 - input filter (network hardwired) 6-15
 - IPX network number 6-16
 - LMI polling interval 6-17
 - local IP address 6-5
 - MTU 6-18
 - netmask 6-19
 - network type, setting 6-20
 - output filter 6-21
 - port groups 6-12

- port idle time 6-14
- setting reference speed 6-23
- transport protocol 6-22
- syslog
 - displaying current settings 2-40
 - facilities and priorities 3-21
 - log types 3-20
 - setting loghost 3-11
 - settings for logged events 3-20
- system name parameter (sysname) 2-21

T

- T1 expansion card 12-12
 - encoding 12-8
 - framing 12-9
 - hot-swapping 12-1
 - setting fractional lines 12-11
- T1 lines
 - backup D channel 12-14
 - encoding method 12-8
 - framing format 12-9
 - pulse code modulation 12-16
 - services 12-1
 - setting use 12-11
- TCP
 - displaying NAT sessions 14-22
 - filters 13-10
 - services D-1
- tech-bulletin@livingston.com mailing list xvi
- technical support, contacting xiv
- Telnet
 - address 2-42
 - administrative port 3-22
 - device service 5-41
 - login service 5-42
 - service device 5-41
- terminal type 5-45
 - login 5-45
 - two-way 5-45
- testing a location configuration 2-4
- TFTP, retrieving file from host 2-43, B-2

- timeout value
 - asynchronous ports 5-22
 - location 8-13
 - NAT 14-17
 - parallel port 9-3
 - synchronous 6-14
 - user 7-11
- tracing a route 2-15
- training, PortMaster xv
- transit area 17-12
- transport protocol
 - asynchronous port 5-38
 - synchronous port 6-22
- Trivial File Transfer Protocol. See TFTP
- tunneling. See L2TP
- two-way network 6-20
 - connections 5-16, 5-32, 5-46
- two-way operation 5-46

U

- UDP
 - displaying NAT sessions 14-22
 - filter, configuring 13-13
 - services D-1
- U-law encoding 12-16
- upgrades, software xiv
- upgrading ComOS 2-43
- user
 - idle timeout 7-11
 - input filter 7-12
 - IPX network 7-14
 - local IP address 7-15
 - login host 7-10
 - login service 7-22
 - maximum dialout ports 7-17
 - MTU 7-18
 - netmask 7-19
 - output filter 7-20
 - password 7-21
 - session time limit 7-23
 - Stac LZS compression 7-8

- TCP/IP header compression 7-8
 - transport protocol 7-21
- user commands, summary B-1
- user configuration 7-25
- User Datagram Protocol. See UDP
- user login mode 5-47
- user table 7-24
 - adding login users 7-5
 - adding network users 7-4
 - configuring 7-1
 - deleting users 7-6
 - displaying data 7-1
 - saving changes 7-6
 - setting user password 7-21
- user table commands summary 7-2
- USERNAME status 2-23
- users in user table 7-24

V

- V.25bis 8-22, 8-24
- V.90 support 12-16
- Van Jacobson TCP/IP header compression 5-13,
6-8, 7-8, 8-9
- variable-length subnet masks 16-13
- virtual port, resetting for Multichassis PPP 12-5
- VLSM 16-13

X

- X.75 protocol 5-38, 7-21, 8-23

