

PortMaster®

Command Line Reference

Lucent Technologies

Remote Access Business Unit

4464 Willow Road

Pleasanton, CA 94588

925-737-2100

800-458-9966

November 1998

950-1184E

Copyright and Trademarks

© 1996, 1997, 1998 Lucent Technologies. All rights reserved.

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

Contents

About This Reference	
Audience	viii
PortMaster Documentation	viii
Additional References	ix
RFCs	ix
Books	x
Document Conventions	xi
Document Advisories	xii
Contacting Lucent Remote Access Technical Support	xiii
For the EMEA Region	xiii
For North America, Latin America, and the Asia Pacific Region	xiii
PortMaster Training Courses	xiv
Subscribing to PortMaster Mailing Lists	xiv
1. Introduction	
PortMaster Configurable Ports	1-1
Accessing the Command Line Interface	1-4
Rebooting a PortMaster	1-6
Command Values	1-7
2. General Commands	
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	3-25
ChoiceNet Client Commands	3-29
SNMP Commands	3-32
4. Ethernet Interface	
Displaying Ethernet Information	4-1
Summary of Ethernet Commands	4-2
Ethernet Commands	4-3
Ethernet Subinterface Commands	4-12
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	5-51
6. Synchronous Ports	
Displaying Synchronous Port Information	6-1
Summary of Synchronous Port Commands	6-2
Synchronous Commands	6-3
7. Parallel Port	
Displaying Parallel Port Information	7-1
Summary of Parallel Port Commands	7-1
Parallel Port Commands	7-2
8. ISDN BRI Ports	
Displaying ISDN Port Information	8-1
Summary of ISDN BRI Commands	8-1
ISDN BRI Commands	8-4

9. ISDN PRI, T1, and E1 Configuration

Displaying ISDN PRI, T1, and E1 Diagnostic Information	9-1
Summary of ISDN PRI, T1, and E1 Commands	9-2
ISDN PRI, T1, and E1 Commands	9-4

10. Routing

Displaying Routing Information.	10-1
Summary of Routing Commands.	10-1
General Routing Commands	10-3
Static Routing Commands	10-14
RIP Commands	10-18
Netmask Commands	10-22
Routing Information	10-25

11. OSPF Routing

Displaying OSPF Information.	11-1
Summary of OSPF Commands.	11-2
OSPF Commands	11-4

12. BGP Routing

Displaying BGP Information	12-1
Summary of BGP Commands	12-2
BGP Commands.	12-4

13. Users

Displaying User Information	13-1
Summary of User Commands	13-2
User Commands.	13-3

14. Locations and DLCIs

Displaying Location Information	14-1
Summary of Location Commands	14-1

Location Commands	14-3
DLCI Commands	14-28
15. Filters	
Displaying Filter Information	15-1
Summary of Filter Commands	15-2
Filter Commands	15-4
16. Hosts	
Displaying Host Information	16-1
Summary of Host Commands	16-1
Description of Host Commands	16-2
17. Debug	
Summary of Debug Commands	17-1
Debug Commands	17-2
Command Index	
Subject Index	

About This Reference

The *PortMaster® Command Line Reference* documents the ComOS® command line interface available on all PortMaster products from the Remote Access Business Unit of Lucent Technologies, Inc. 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*.

Refer to your hardware installation guide for information on attaching to a console before attempting to configure your PortMaster with the command line interface.

Release-Specific Information. The ComOS 3.8 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 PMVision commands, keywords, and features.

PortMaster 4 Commands. If you have a PortMaster 4 Integrated Access Concentrator, consult this reference along with the *PortMaster 4 Installation Guide* for the complete set of commands that work on the PortMaster 4.

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.



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

Audience

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

PortMaster Documentation

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

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

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

- *ChoiceNet® Administrator's Guide*

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

- *PortMaster Command Line Reference*

This 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 Administrator's Guide*

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

Additional References

RFCs

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

RFC 768, *User Datagram Protocol*

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specification*

RFC 950, *Internet Standard Subnetting Procedure*

RFC 1058, *Routing Information Protocol*

RFC 1112, *Host Extensions for IP Multicasting*

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

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

RFC 1166, *Internet Numbers*

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

RFC 1256, *ICMP Router Discovery Messages*

RFC 1321, *The MD5 Message-Digest Algorithm*

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

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

RFC 1334, *PPP Authentication Protocols*

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

RFC 1413, *Identification Protocol*

RFC 1490, *Multiprotocol Interconnect Over Frame Relay*

RFC 1541, *Dynamic Host Configuration Protocol*

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

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

RFC 1587, *OSPF NSSA Options*

RFC 1597, *Address Allocations for Private Internets*

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

Books

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

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

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

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

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))

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

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

TCP/IP Network Administration. Craig Hunt. Sebastopol, CA: O'Reilly & Associates, Inc. 1994. (ISBN 0-937175-82-X)

Document Conventions

The following conventions are used in this reference:

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.

Convention	Use	Examples
Square brackets ([])	Enclose optional keywords and values in command syntax.	<ul style="list-style-type: none">• set nameserver [2] <i>Ipaddress</i>• set S0 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 S0 W1 ospf on off• set S0 host default prompt <i>Ipaddress</i>

Document Advisories



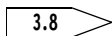
Note – means take note. Notes contain information of importance or special interest.



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 Remote Access Technical Support

The PortMaster comes with a 1-year hardware warranty.

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

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

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

For the EMEA Region

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

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

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

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

Contact Lucent Remote Access Monday through Friday between the hours of 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, or +1-925-737-2100 from elsewhere.
- By fax, dial +1-925-737-2110.
- By email, send mail as follows:

- From North America and Latin America to **support@livingston.com**.
- From the Asia Pacific Region to **asia-support@livingston.com**.
- Using the World Wide Web, see **<http://www.livingston.com/>**.

PortMaster Training Courses

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

Subscribing to PortMaster Mailing Lists

Lucent maintains the following Internet mailing lists for PortMaster users:

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

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

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

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

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

The command line interface can be used to administer any PortMaster Communications Server (PM-2 series), Internetwork Router (IRX™ series), Office Router (OR series), Integrated Access Server (PM-3 series), or Integrated Access Concentrator (PM-4 series). When the name *PortMaster* is used in this guide, it can refer to any of these PortMaster models.

This chapter provides a summary of PortMaster configurable ports, by model. It also describes how to start the command line interface and reboot the PortMaster, and provides an overview of PortMaster commands and arguments—or **values**.

PortMaster Configurable Ports

The command line interface can be used to configure your PortMaster ports. Table 1-1 lists the configurable ports by PortMaster model.

Table 1-1 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	s0–1							
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				1
OR-ST-AP	ether0	s0				s1–s2			1

Table 1-1 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-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						
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						

Table 1-1 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
IRX-114	ether0	s0	s1-s4						
IRX-211	ether0-1	s0	s1						
PM-3A-IT	ether0	c0					0		
PM-3A-2T	ether0	c0					0-1		
PM-3D-1T	ether0	c0					0		
PM-3D-2T	ether0	c0					0-1		
PM-3A-1E	ether0	c0						0	
PM-3A-2E	ether0	c0						0-1	
PM-3D-1E	ether0	c0						0	
PM-3D-2E	ether0	c0						0-1	

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.

PortMaster 4 Configurable Ports. The manager board of the PortMaster 4 contains two Ethernet ports and two asynchronous ports. Each board of the PortMaster 4 can hold up to four T1 lines or three E1 lines. Consult the *PortMaster 4 Installation Guide* for more information about the configurable ports of the PortMaster 4.

Accessing the Command Line Interface

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 1-2 lists the basic PortMaster commands. Some are complete commands; others require additional keywords or values as described in following chapters.

Table 1-2 User Commands

Command	Description
add	Adds an entry to a PortMaster table.
delete	Deletes an entry from a PortMaster table.
dial	Begins dialing to the specified network location.
erase	Erases all or part of PortMaster nonvolatile RAM.
help	Provides information on each of the commands, including usage and syntax.
ifconfig	Displays configuration values for all interfaces and allows modification of active values.
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.

Table 1-2 User Commands (Continued)

Command	Description
ptrace	Displays packet traffic passing through the PortMaster, using the specified filter.
quit, done, or exit	Exits the command line interface.
reboot	Reboots, using the currently saved configuration.
reset	Resets a specific 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 database table, or for a protocol.
show	Shows the status of each specified port, all ports, global configuration, or table.
telnet	Connects via Telnet from the PortMaster to a specified host on the network.
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.
!!	Repeats the last command.

2. **Configure your PortMaster, referring to the port-specific, protocol-specific, or table-specific chapters in this guide and the *PortMaster Configuration Guide*, *PortMaster Routing Guide*, and *PortMaster 4 Installation Guide*.**

Rebooting a PortMaster

After configuring the following settings, you must reboot the PortMaster to activate them:

- 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**

In addition, you must reboot after erasing the configuration in nonvolatile RAM or after loading software from nonvolatile RAM.

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.

Command Values

Table 1-3 describes the different kinds of values 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 1-3 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>Device</i>	Name of network device or pseudo-tty on a UNIX host.	/dev/ttyp0 , or /dev/network
<i>Dlci</i>	A DLCI number.	1 through 1023.
<i>Dlci_list</i>	Space separated list of DLCIs.	A maximum of 240 characters.
<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>

Table 1-3 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Facility.Priority</i>	Loghost facility and priority of syslog messages sent to the facility.	One syslog facility keyword and one syslog priority keyword separated by a period. See page 3-21 for more information.
<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.	Integer from 0 to 100; 0 is default.
<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 leading 0x .
<i>Interface</i>	Interface specification.	For example, ether0 , frml , ptp1 , frmw1 , or ptpw1 .
<i>Ipaddress</i>	IP address or hostname.	Address is in dotted decimal notation; 39-character hostname.
<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 PortMaster3.	line2 .
<i>ListName</i>	Name of list of source or destination sites used for packet filters.	String of up to 15 printable, nonspace, ASCII characters.

Table 1-3 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Locname</i>	Name of internetwork dial-out destination.	String of up to 12 printable, nonspace, ASCII characters.
<i>Logtype</i>	One of five areas used for logging with 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>MTU</i>	Maximum transmission unit. Maximum packet size, in bytes, that an interface can send.	Integer from 100 to 1520.
<i>Metric</i>	Hop count to 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>NM</i>	Alternative netmask notation. 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>Polycyname</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>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.

Table 1-3 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<i>Protocol</i>	Type of routing protocol.	bgp, ospf, rip, or static.
<i>RuleNumber</i>	Number indicating the order of a filter rule or a BGP policy statement.	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.
<i>S0</i>	Any asynchronous port.	<ul style="list-style-type: none"> • c0 or s0 through s29, depending on PortMaster model. • all —Applies the command simultaneously to all asynchronous 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 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.
<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 50-ms increments of time required to send a packet to the destination network.	Integer.

Table 1-3 Command Line Values (Continued)

Value	Represents	Format and/or Value(s)
<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.	<i>V0</i> and up, depending on 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 PortMaster model.• all—Applies the command simultaneously to all synchronous ports.

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 Filtername extended dump Bytes</i>]	- see page 2-13
reboot	- see page 2-15
reset	- see page 2-15
all S0 W1 console dialer nic p0 nHandle dNumber ospf bgp v0	
rlogin <i>Ipaddress</i>	- see page 2-17
save all Ether0 S0 W1 global console filter host location netmask p0 ports route snmp user ospf bgp	- see page 2-18

Table 2-1 General Commands (Continued)

Command Syntax	
set console [<i>S0 p0</i>]	- see page 2-19
set debug	- see page 17-5
set sysname [<i>String</i>]	- see page 2-20
show all	- see page 2-21
show arp <i>Interface</i>	- see page 2-23
show bgp memory	- see page 12-42
show bgp next-hop	- see page 12-43
show bgp paths [<i>Prefix/NM</i> [verbose]]	- see page 12-45
show bgp peers [verbose packets]	- see page 12-48
show bgp policy [<i>Policyname</i>]	- see page 12-54
show bgp summarization [all]	- see page 12-55
show Ether0	- see page 4-10
show files	- see page 2-24
show filter	- see page 15-25
show global	- see page 2-27
show ipxroutes	- see page 10-25
show isdn	- see page 8-15
show Line0	- see page 9-19
show location <i>Locname</i>	- see page 14-27
show M0	- see page 9-23
show mcppp	- see page 9-26
show memory	- see page 2-30
show modems	- see page 9-25
show modem <i>ModemName</i>	- see page 5-52
show modules	- see page 2-31
show netconns	- see page 2-32

Table 2-1 General Commands (Continued)

Command Syntax	
show netstat	- see page 2-33
show ospf areas	- see page 11-21
show ospf links [router network summary external nssa]	- see page 11-24
show ospf neighbor	- see page 11-27
show routes [String Prefix/NM]	- see page 10-28, page 11-29, page 12-57
show pots	- see page 3-24
show propagation	- see page 10-26
show route to-dest <i>Ipaddress</i>	- see page 10-30
show S0	- see page 2-34
show sap	- see page 2-37
show sessions	- see page 2-38
show syslog	- see page 2-39
show table filter host location modem netmask snmp subinterface user	- see page 2-40
show user <i>Username</i>	- see page 13-25
show W1	- see page 6-22
telnet <i>Ipaddress</i> [<i>Tport</i>]	- see page 2-41
tftp get [comos] <i>Ipaddress String</i>	- see page 2-42
tracert [<i>Ipaddress</i>]	- see page 2-43
version	- see page 2-44

General Commands

The general commands are described below.

dial

This command initiates dialing to a network location.

```
dial Locname [-x]
```

<i>Locname</i>	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 2-19
set debug - page 17-5

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

This command erases 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.
file	Erases a specified file from nonvolatile RAM.
<i>String</i>	The name of the file to be erased; see show files on page 2-24 for filenames.
partition	Use this keyword only when told to do so by Lucent Remote Access Technical Support.
<i>Number</i>	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 supports 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
traceroute	- 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 – This command should be entered 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>	The interface specification—for example, ether0 , frm1 , frmw1 .
<i>Ipaddress</i>	The IP address of the interface.
<i>Ipmask</i>	The netmask for the interface IP address.
<i>Ipaddress(dest)</i>	The IP address of the destination of a point-to-point connection.
<i>Ipxnetwork</i>	The IPX network number of the interface.
<i>ipxframe</i>	The frame type used for sending IPX packets out of the Ethernet interface. Options include the four protocols that follow.
ethernet_802.2	Use Ethernet 802.2 protocol. This is the default encapsulation used by Novell NetWare Version 4.0.
ethernet_802.3	Use Ethernet 802.3 protocol. This is the default encapsulation used by Novell NetWare Version 3.11.
ethernet_802.2_ii	Use Ethernet 802.2_ii protocol. This encapsulation is not commonly used.
ethernet_ii	Use Ethernet II protocol. This is sometimes used for networks that handle both TCP/IP and IPX traffic.

up	The interface is brought up.
down	The interface is shut down.
private	No routing information will be transmitted on this interface.
-private	Routing information is broadcast 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. Because Ethernet subinterfaces are rebuilt every time a new subinterface is added, you can view but not modify an Ethernet subinterface configuration using the **ifconfig** command.



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 ffffffff0 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 fffffff00 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 fffffff00 broadcast 192.168.100.0 mtu 1500
```

See Also

ifconfig - page 11-5

ping - page 2-11

traceroute - page 2-43

ping

This command sends 10 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
```

See Also

ptrace - page 2-13

set reported_ip - page 3-19

traceroute - page 2-43

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 socket TCP 1642.

Example

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

See Also

rlogin - page 2-17

telnet - page 2-41

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

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 15-4
set console - page 2-19
set filter - page 15-6 to page 15-23
show filter - page 15-25
show table filter - page 15-26

reboot

This command restarts the software using the currently saved configuration.

reboot

Usage

A PortMaster must be rebooted for a changed IP or 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

After making any changes to port configuration, you must reset PortMaster ports to make the changes take effect.

reset all | S0 | W1 | console | dialer | nic | p0 | nHandle | dNumber | ospf | bgp | V0

all	Resets all ports.
S0	Any asynchronous port.
W1	Any synchronous port.
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.
nic	Resets the network interface card (NIC) controller.

<code>p0</code>	The parallel port.
<code>nHandle</code>	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 2-32 for an example display.
<code>dNumber</code>	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 8-15 for an example display.
<code>ospf</code>	See page 11-6.
<code>bgp</code>	See page 12-14.
<code>V0</code>	See page 9-4.

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 2-19

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 2-41

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 *SO|WI|all|global|console|filter|host|location|netmask|p0|ports|route|snmp|user|ospf|bgp*

all	All configuration changes.	
SO	Any asynchronous port.	See Chapter 5.
WI	Any synchronous port.	See Chapter 6.
global	Global configuration changes.	See Chapter 3.
console	Console port setting.	See page 2-19.
filter	Filter configuration changes.	See Chapter 15.
host	Host table settings.	See Chapter 16.
location	Location table settings.	See Chapter 14.
netmask	Netmask table settings.	See Chapter 10.
p0	Parallel port settings.	See Chapter 7.
ports	All ports.	
route	Static route table settings.	See Chapter 10.
snmp	SNMP table settings.	See Chapter 3.
user	User table settings.	See Chapter 13.
ospf	OSPF configuration.	See Chapter 11.
bgp	BGP configuration.	See Chapter 12.

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 17-5
show files - page 2-24

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*]

<i>S0</i>	Any asynchronous port.
<i>p0</i>	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 17-5

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 A 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 3-5
set snmp - page 3-36

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 2-22 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.

Table 2-2 Port Status Messages (Continued)

Status	Description
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*

Interface 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, 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, such as the SNMP table, that are not loaded are not displayed.

show files

Examples

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

From a PortMaster 3 with internal digital modems:

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

Examples

```
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 2-20.
Default Host	Host used for login services.	See page 5-22.
Alternate Hosts	Alternate host.	See page 5-22.
IP Gateway	Default route gateway address.	See page 10-12.
Gateway Metric	Metric for the default route.	See page 10-12.
Default Routing	Default routing options for all interfaces.	See page 10-18.
OSPF Priority	OSPF priority assigned to the router.	See page 11-19.
OSPF Router ID	OSPF router address or ID number.	See page 11-20.
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 12-20 and page 12-16.
BGP timers	Configured BGP timed events.	See page 12-18 and page 12-19.
BGP IGP Lockstep	Status of the BGP Interior Gateway Protocol (IGP) lockstep setting.	See page 12-20.
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 3-23.

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 3-28.
Alternate Server	Alternate RADIUS authentication server.	See page 3-27.
Accounting Server	Radius accounting server.	See page 3-25.
Alt. Acct. Server	Alternate RADIUS accounting server.	See page 3-25.
ChoiceNet Server	ChoiceNet server.	See page 3-30.
Alt. ChNet Server	Alternate ChoiceNet server.	See page 3-30.
PPP Authentication	Configured authentication—PAP and CHAP.	See page 3-16.
ISDN Switch Type	ISDN switch type.	See page 8-9 and page 9-6.
ISDN MSN	ISDN multiple subscriber number (MSN) setting.	See page 8-4.
ISDN numberauto	Automatic determination of ISDN number plan and type for a received call.	See page 8-5.
ISDN numberplan	ISDN number plan.	See page 8-6.
ISDN numbertype	ISDN number type.	See page 8-7.
End Point Disc	The Multichassis PPP endpoint discriminator.	See page 9-5.
Disabled Modules	Disabled ComOS modules.	See page 2-31.

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, <i>Size:Number</i> : <ul style="list-style-type: none">• <i>Size</i>—size in bytes (for example, 64).• <i>Number</i>—number of fragments of that size (for example, 1). To determine the total amount of 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. The output shows the total number of buffers, buffers in use by network packets, and available buffers. Each buffer is 128 bytes.
System bbufs	Equivalent to system nbufs on PortMaster Office Routers with T1 interfaces. Buffer size is increased to 1600 bytes.

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 such as the SNMP table that are not loaded 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	The 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 *Handle* - 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	<p>Number of times the interface was reset since reboot, due to any of the following:</p> <ul style="list-style-type: none"> • More than 16 collisions when transmitting 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 buffer to be sent from the interface.

show S0

This command shows the current status and configuration for the port. This command can be used for asynchronous, synchronous, ISDN, and parallel ports on the PortMaster.

show S0

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 2-22.
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	<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 <i>DCD</i> and <i>CTS</i> indicate that the DCD and CTS signals on the port are asserted (high).</p> <p>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>.</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 5-42.
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.

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
-----	---	-----	-----	---	-----	-----
080009A8CEAA80CGNPJA8CEA	30C	COA86000:	080009A8CEAA:	400C	2	ether0
NOVELL	4	00001701:	000000000001:	0451	2	ether0

Explanation

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

show sessions

This command shows current use of ports.

show sessions

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 <i>V</i> 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 2-22.
Start	Time in minutes since the session started.
Idle	Time in minutes that the session has been idle.

show syslog

This command shows 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
```

Explanation

This example displays the default settings. These default settings can be changed with the **set syslog** command (see page 3-21).

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 filter|host|location|modem|netmask|snmp|subinterface|user

filter	See the following example and page 15-26.
host	See page 16-3.
location	See page 14-28.
modem	See page 5-53.
netmask	See page 10-31.
subinterface	See page 4-16.
snmp	See page 3-39.
user	See page 13-24.

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 15-2 on page 15-11 for a list of the port numbers 20 through 1647 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.

<i>comos</i>	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 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 Remote Access 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, ChoiceNet, and SNMP 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 2-21
- **show global**—see page 2-27

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.

Table 3-1 Global Configuration

Command Syntax	
clear alarm	- see page 3-33
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 3-5

Table 3-1 Global Configuration (Continued)

Command Syntax	
set default on off broadcast listen	- see page 10-18
set dhcp-server <i>Ipaddress</i>	- see page 3-6
set domain <i>String</i> none	- see page 3-7
set gateway <i>Ipaddress</i> [<i>Metric</i>]	- see page 10-12
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 3-18
set pots on off	- see page 3-18
set reported_ip <i>Ipaddress</i>	- see page 3-19
set serial-admin on off	- see page 3-20
set syslog <i>Logtype</i> {[disabled] [<i>Facility.Priority</i>]}	- see page 3-21
set telnet <i>Tport</i>	- see page 3-23
set user-netmask on off	- see page 10-13

Table 3-1 Global Configuration (Continued)

Command Syntax	
show alarms	- see page 3-38
show all	- see page 2-21
show global	- see page 2-27
show pots	- see page 3-24

Global Commands

These commands are used to configure everything on the PortMaster except for interfaces, routing protocols, and tables.

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.



Note – 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 3-18

set user destination - page 13-6

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.

3.8

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.

Usage

ComOS 3.8 and later supports the call-check feature to enable services without authenticating the user at the point of entry. Call-check is off by default. Use the **show global** command find out if call-check is enabled on your PortMaster.

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 does one of the following:

- 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
- Allows the creation of a netdata clear channel TCP connection to the destination specified in the RADIUS accept record

Call-check enables the PortMaster—via RADIUS—to check the telephone number of a caller before answering the call. The PortMaster can then hang up and call the user back with no charge incurred for connecting the user in the first place. Alternatively, the PortMaster can reject the call to limit the number of users who can call a given number, such as an 800 number, or to prevent certain users from calling the number.

You can also use call-check to support virtual points of presence (POPs) by redirecting a call. If a caller dials one number, you can authenticate normally. If a caller dials a different number, you can accept the call and forward the caller information through a netdata (TCP clear) connection to an IP address and port of your choosing, where another process handles the user.

Additionally, you can 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.

Example

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

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, the PortMaster prompts the user to authenticate with CHAP. 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 14-8

set pap - page 3-16

show global - page 2-27

set dhcp-server

This command configures a PortMaster to forward a Dynamic Host Configuration Protocol (DHCP) request from a dial-in client of a cable modem to be forwarded to the specified DHCP server.

set dhcp-server *Ipaddress*

Ipaddress IP address or 39-character hostname.

Usage

In ComOS version 3.7.2 and later, this command is used to support Cable Modem Telephone Return Interface Specification (CMTRIS) developed by Multimedia Cable Network System (MCNS) Partners Limited. This specification requires that a cable modem using the telephone interface as an upstream channel be able to request and receive the cable interface address and configuration information using a DHCP request.

ComOS modifies the received DHCP request by removing the broadcast address and replacing it with the DHCP server's address. This enables the DHCP server to direct the response to the dial-in client of the cable modem. The DHCP server sends configuration information to the dial-in client of the cable modem to be used to configure the cable interface.

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

For more information about using this command, refer to the PortMaster Configuration Guide.

To view DHCP relaying information, use the command **set console**, followed by the command **set debug 0x81**.

To disable DHCP reply information, set the IP address to 0.0.0.0.



Note – This command does not support DHCP requests from the Ethernet or requests from a PortMaster 2Ei or Office Router OR-U.



Note – The PortMaster router does not allow for the forwarding of a packet to the broadcast address 255.255.255.255.

See Also

set console - page 2-19

set debug Hex - page 17-5

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 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 namesvc - page 3-14
set nameserver - page 3-13

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
```

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

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

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 5-22
set S0 service_device - page 5-43
set S0 service_login - page 5-44
set user host - page 13-10
set user service - page 13-22

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 4-7
set Ether0 ipxnet - page 4-8
set location ipxnet - page 14-14
set S0 ipxnet - page 5-26
set W1 ipxnet - page 6-14
show modules - page 2-31

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:0101010101 1  
IPX Gateway set to tyche:0101010101, 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. Set *Ipaddress* to 0.0.0.0 to deselect the host.

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.



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 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 3-21

set maximum pmconsole

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

set maximum pmconsole *Number*

Number The 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, the maximum number of connections should be set 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**

See Also

set serial-admin - page 3-20

set telnet - page 3-23

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. Set *Ipaddress* to 0.0.0.0 to deselect the name server.

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 prompts the user to authenticate with PAP. 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 3-5).

Example

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

See Also

set chap - page 3-5
show global - page 2-27

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*

<i>Number</i>	The number of IP addresses to allocate to the pool. The valid range is from 0 to 64.
---------------	---

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**.

To display the status of the analog PHONE port, enter the command **set pots** with no parameters.

Example

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

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

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. Set *Ipaddress* to 0.0.0.0 to disable the command.

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 13-14

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: <div><div>admin-logins</div><div>!root and administrative logins.</div></div> <div><div>user-logins</div><div>Nonadministrative logins. You might want to disable this type of logging if you already use RADIUS accounting.</div></div> <div><div>packet-filters</div><div>Packets that match filter rules with the log keyword.</div></div> <div><div>commands</div><div>Every command entered at the command line interface.</div></div> <div><div>termination</div><div>More detailed information on how user sessions terminate.</div></div>
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 3-22 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.

Example

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

See Also

set loghost - page 3-11

set telnet

This command sets the Telnet administrative port.

set telnet *Tport*

Tport Telnet administrative port—a decimal 16-bit number from 0 to 65535. Default is 23.

Usage

This command allows the administrator to use the Telnet protocol to maintain the PortMaster. The value is a number from 0 to 65535. If set to 0, the PortMaster disables the Telnet administration function. Ports numbered 10000 through 10100 are reserved for outbound users and should 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 2-41

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.

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 3-25
set alternate_auth_server <i>Ipaddress</i> [<i>Uport</i>]	- see page 3-27
set authentication_server <i>Ipaddress</i> [<i>Uport</i>]	- see page 3-28
set secret <i>String</i>	- see page 3-29

The following commands configure the PortMaster as a RADIUS client. For RADIUS server configuration information, see the *RADIUS 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.
- Ipaddress*

IP address or 39-character hostname running a RADIUS accounting server on UDP port 1646. Set *Ipaddress* to 0.0.0.0 to deselect the accounting 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 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 accounting server and the alternate accounting 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 3-28

set secret - page 3-29

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*]

Ipaddress RADIUS alternate authentication server IP address or 39-character hostname. Set *Ipaddress* to 0.0.0.0 to deselect the alternate authentication server.

Uport Integer between 0 and 65535 that specifies the UDP port to be used for RADIUS authentication. 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 3-28

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 authentication. 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 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 3-25
set alternate_auth_server - page 3-27
set secret - page 3-29
set \$0 security - page 5-42

set secret

This command sets the RADIUS shared secret.

set secret *String*

String 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 3-28
set \$0 security - page 5-42

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 3-30
set choicenet-secret <i>String</i>	- see page 3-31

Table 3-5 ChoiceNet Client Configuration (*Continued*)

Command Syntax	
set debug choicenet on off	- see page 17-4

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. |
| <i>Ipaddress</i> | IP address or 39-character hostname of the host running a ChoiceNet server on UDP port 1647. Set <i>Ipaddress</i> to 0.0.0.0 to deselect the ChoiceNet 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 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 3-30

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 3-32
clear alarm <i>alarm-id</i> all	- see page 3-33
delete snmphost reader writer <i>Ipaddress</i>	- see page 3-34
save snmp	- see page 3-35
set snmp on off	- see page 3-36
set snmp readcommunity writecommunity <i>String</i>	- see page 3-37
set sysname <i>String</i>	- see page 2-20
show alarms [<i>Alarm-id</i>]	- see page 3-38
show table snmp	- see page 3-39

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>	The 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 3-34
save snmp - page 3-35
set snmp - page 3-36
show table snmp - page 3-39

clear alarm

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

3.8

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

<i>Alarm-id</i>	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 3-38

delete snmpshost

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

```
delete snmpshost reader|writer Ipaddress
```

- reader** Use to delete a read host.
- writer** Use to delete a write host.
- Ipaddress** The 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 3-32

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 3-36

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 snmphost - page 3-32
save snmp - page 3-35
show modules - page 2-31
show table snmp - page 3-39

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. You should use some other 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 3-32
save snmp - page 3-35
set snmp - page 3-36
show table snmp - page 3-39

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
Age 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 3-33

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 3-35

set snmp - page 3-36

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 2-21
- **show arp** *Ether0*—see page 2-23
- **show** *Ether0*
- **show global**—see page 2-27
- **show netconns**—see page 2-32
- **show netstat**—see page 2-33
- **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 interface on all PortMaster products and—except as noted—the Ether1 interface on the IRX-211.

Ethernet subinterface commands are summarized in Table 4-2, on page 4-12.

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 4-6
set Ether0 ipxframe ethernet_802.2 ethernet_802.2_ii ethernet_802.3 ethernet_ii	- see page 4-7
set Ether0 ipxnet <i>Ipxnetwork</i>	- see page 4-8
set Ether0 netmask <i>Netmask</i>	- see page 10-7
set Ether0 ofilter <i>Filtername</i>	- see page 4-9
set Ether0 ospf accept-rip on off	- see page 11-7
set Ether0 ospf on off	- see page 11-8
set Ether0 rip on broadcast listen off	- see page 10-19
set Ether0 route-filter incoming outgoing <i>Filtername</i>	- see page 10-8
show Ether0	- see page 4-10

1. This command is available only on the Ether0 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 10-7

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 be seen by 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 4-9
show filter - page 15-25
show table filter - page 15-26

set ether0 ip

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

set ether0 ipx enabled|disabled

enabled	Enables IPX.
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 – This command should be entered 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.
<i>ethernet_802.2</i>	Use Ethernet 802.2 protocol. This is the default encapsulation used by Novell NetWare 4.0.
<i>ethernet_802.2_ii</i>	Use Ethernet 802.2_ii protocol. This encapsulation is not commonly used.
<i>ethernet_802.3</i>	Use Ethernet 802.3 protocol. This is the default encapsulation used by Novell NetWare 3.11.
<i>ethernet_ii</i>	Use 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 should 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 4-8
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

The IPX network number should be entered 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 4-7
set ipx on - page 3-9
set user ipxnet - page 13-13

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 be seen by 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 15-25
show table filter - page 15-26

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.

Because Ethernet subinterfaces are rebuilt every time a new subinterface is added, they can be viewed but not modified with the **ifconfig** command.



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

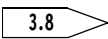
The commands in Table 4-2 configure and manage Ether0 and Ether1 for subinterfaces.

Table 4-2 Ethernet Subinterface Configuration

Command Syntax	
add subinterface <i>Name</i>	- see page 4-12
delete subinterface <i>Name</i>	- see page 4-13
set subinterface <i>Name</i> address <i>Ipaddress</i> [/NM] [Netmask]	- see page 4-14
set subinterface <i>Name</i> broadcast <i>high low</i>	- see page 4-15
set subinterface <i>Name</i> netmask	- see page 4-15
set subinterface <i>Name</i> port <i>Portlabel</i>	- see page 4-16
show location <i>Locname</i>	- see page 14-27
show table subinterface	- see page 4-16

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 4-16

delete subinterface

This command removes a subinterface entry from the table.

3.8

delete subinterface *Name*

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.

3.8

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

<i>Name</i>	Name of the subinterface configuration. Name 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
```

set subinterface broadcast

This command determines the broadcast address for the subinterface.

3.8

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.

3.8

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.

See Also

set subinterface address - page 4-14

Example

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

set subinterface port

This command associates the subinterface configuration with a physical port.

3.8

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.

3.8

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 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1-1 for the range of asynchronous ports available on each PortMaster model.

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 2-34
- **show all**—see page 2-21
- **ifconfig**—see page 2-9
- **show sessions**—see page 2-38

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.

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 5-20
set <i>S0 all hangup on off</i>	- see page 5-21
set <i>S0 all host default prompt [1 2 3 4]Ipaddress</i>	- see page 5-22
set <i>S0 all idletime Number [minutes seconds]</i>	- see page 5-23
• set <i>S0 all ifilter Filtername</i>	- see page 5-25
• set <i>S0 ipxnet Ipxnetwork</i>	- see page 5-26

Table 5-1 Asynchronous Port Configuration (Continued)

Command Syntax	
set S0 all login [network dialin dialout twoway]	- see page 5-27
• set S0 all map Hex	- see page 5-28
set S0 all message String	- see page 5-30
set S0 all modem-type ModemName	- see page 5-31
• set S0 all mtu MTU	- see page 5-32
• set S0 netmask Ipmask	- see page 5-33
set S0 all network dialin dialout twoway	- see page 5-34
set S0 all network hardwired	- see page 5-35
• set S0 all ofilter Filtername	- see page 5-36
set S0 ospf on off	- see page 11-9
set S0 all override xon rts speed parity databits on off	- see page 5-37
set S0 all parity even none odd strip	- see page 5-38
set S0 all prompt String	- see page 5-39
• set S0 protocol slip ppp x75-sync	- see page 5-40
set S0 route-filter incoming outgoing Filtername	- see page 10-8
• set S0 all rip on off broadcast listen	- see page 10-19
set S0 all rts/cts on off	- see page 5-41
set S0 all security on off	- see page 5-42
set S0 all service_device netdata portmaster rlogin telnet [Tport]	- see page 5-43
set S0 all service login netdata portmaster rlogin telnet [Tport]	- see page 5-44
set S0 all speed [1 2 3]300 600 1200 2400 4800 9600 19200 38400 57600 76800 115200	- see page 5-45
set S0 all stopbits 1 2	- see page 5-46
set S0 all termtype String	- see page 5-47
set S0 twoway Device [network dialin dialout twoway]	- see page 5-48
set S0 username autolog String	- see page 5-49

Table 5-1 Asynchronous Port Configuration (Continued)

Command Syntax	
set <i>S0</i> all xon/xoff on off	- see page 5-50
show all	- see page 2-21
show <i>S0</i>	- see page 2-34

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.
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 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1-1 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.
<i>String</i>	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 5-52

show table modem - page 5-53

attach S0

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

attach S0

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 – Speech and 3.1KHz audio services each use 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 14-22
reset nHandle - page 2-15

delete modem

This command deletes a modem entry from the modem table.

delete modem *ModemName(short)*

ModemName(short)

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 5-52

show table modem - page 5-53

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 5-25

set S0 address

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

set S0 address *Ipaddress*

Ipaddress Hostname or IP address.

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.

The following table indicates the effect of DCD assertion for each port type:

Asynchronous Port		Effect of DCD Assertion	
Type		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.
network hardwired		The port is unavailable.	The port attempts to establish a network connection.

Asynchronous Port		Effect of DCD Assertion	
Type		DCD Low—Not Asserted	DCD High—Asserted
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 5-53

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, PortMaster 4, 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, PortMaster 4 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 14-9

set S0 protocol - page 5-40

set user compression - page 13-8

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 ModemName - page 5-31

set S0 parity - page 5-38

set S0 speed - page 5-45

set S0 stopbits - page 5-46

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 39-character hostname 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 6-7

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 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 5-22

set S0 login - page 5-27

set S0 twoway - page 5-48

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|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 13-9

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 5-21
set S0 modem-type ModemName - page 5-31

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|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 14, “Locations and DLCIs,” for more information.

set S0|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 14-10

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|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|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.
Ipaddress	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.

Example

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 5-43

set S0 service_login - page 5-44

set user host - page 13-10

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|all idletime *Number* [**minutes|seconds**]

<i>Number</i>	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 examples.

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

add S0 modem - page 5-31

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|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 15-4

set S0 ofilter - page 5-36

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 4-8

set ipx on - page 3-9

set W1 ipxnet - page 6-14

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|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 5-22

set S0 service-login - page 5-44

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 14-15

set S0 protocol - page 5-40

set user map - page 13-15

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|all message *String*

String	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 5-39

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 5-3, “Modem Table Commands,” on page 5-51 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 5-53

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 5-40

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 10-7
set location netmask - page 14-19
set user netmask - page 13-18
set W1 netmask - page 6-17

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|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 5-27

set S0 twoway - page 5-48

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|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 15-4
set S0 ifilter - page 5-25

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 *ModemName* - page 5-31
set S0 parity - page 5-38
set S0 speed - page 5-45

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** should 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 *ModemName* - page 5-31
set S0 speed - page 5-45
set S0 stopbits - page 5-46

set S0|all prompt

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

set S0|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 5-22
set message - page 5-30
set S0 username - page 5-49

set S0 protocol

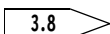
This command sets the transport protocol for a single network hardwired asynchronous port, or all network hardwired asynchronous ports.

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 17-5
set S0 compression - page 5-13
set S0 mtu - page 5-32

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 ModemName - page 5-31
set S0 xon/xoff - page 5-50

set S0|all security

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

set S0|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 3-28

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|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 5-22
set S0 login - page 5-27

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|all service_login netdata|portmaster|rlogin|telnet [*Tport*]

<i>netdata</i>	Uses the netdata login service.
<i>portmaster</i>	Uses the PortMaster login service to connect to in.pmd on the login host. This is the default.
<i>rlogin</i>	Uses remote login to connect to the login host.
<i>telnet</i>	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 5-27
set S0 modem-type *ModemName* - page 5-31
set S0 service-device - page 5-43
set telnet - page 3-23
telnet - page 2-41

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 Indicates the data terminal equipment (DTE) rate. Default is
on 9600bps.

Usage

Modern modems should 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 *ModemName* - page 5-31

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 *ModemName* - page 5-31
set S0 parity - page 5-38
set S0 speed - page 5-45

set S0|all termttype

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|all termttype *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 termttype** command.

Example

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

See Also

set S0 login - page 5-27

set S0 twoway - page 5-48

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 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 5-22

set S0 login - page 5-27

set S0 network twoway - page 5-34

set S0 service_device - page 5-43

set S0 service_login - page 5-44

set S0 username|autolog

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

set S0 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 5-30
set S0 prompt - page 5-39

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. This command should be used 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 5-41

Modem Commands

The modem table commands in Table 5-3 are used to view and configure the modem table, which stores configuration information for modems you commonly use. See also the following commands for modems attached to asynchronous ports:

- **attach S0**—see page 5-6
- **set S0 cd**—see page 5-11
- **set S0 group**—see page 5-20
- **set S0 modem-type**—see page 5-31

Table 5-3 Modem Table Commands

Command Syntax	
add modem <i>ModemName(short) ModemName(long) Speed String</i>	- see page 5-5
delete modem <i>ModemName(short)</i>	- see page 5-8
show modem <i>ModemName</i>	- see page 5-52
show table modem	- see page 5-53



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 5-53

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 5-52

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 **rest 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 2-21
- **ifconfig**—see page 2-9
- **show sessions**—see page 2-38
- **show netstat**—see page 2-33
- **show arp**—see page 2-23

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 6-8
• delete dlci ipdlci ipxdlci <i>W1</i> <i>Dlci</i>	- see page 6-8
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 6-3
• set <i>W1</i> annex-d <i>Seconds</i>	- see page 6-4
set <i>W1</i> cd on off	- see page 6-5
set <i>W1</i> compression on off stack vj	- see page 6-6
• set <i>W1</i> destination <i>Ipaddress</i> [<i>Ipmask</i>]	- see page 6-7
• set <i>W1</i> dlcilist <i>Dlci_list</i>	- see page 6-8
set <i>W1</i> extended on off	- see page 6-10
set <i>W1</i> group <i>Group</i>	- see page 6-10
set <i>W1</i> hangup on off	- see page 6-11
set <i>W1</i> idletime <i>Number</i> [<i>minutes</i> <i>seconds</i>]	- see page 6-12
• set <i>W1</i> ifilter [<i>Filtername</i>]	- see page 6-13
• set <i>W1</i> ipxnet <i>Ipxnetwork</i>	- see page 6-14
• set <i>W1</i> lmi [<i>Seconds</i>]	- see page 6-15
• set <i>W1</i> mtu <i>MTU</i>	- see page 6-16
• set <i>W1</i> netmask <i>Ipmask</i>	- see page 6-17
set <i>W1</i> network dialin dialout twoway hardwired	- see page 6-18
• set <i>W1</i> ofilter [<i>Filtername</i>]	- see page 6-19
set <i>W1</i> ospf on off	- see page 11-9

Table 6-1 Synchronous Port Configuration (Continued)

Command Syntax	
set W1 protocol slip ppp frame x75-sync	- see page 6-20
set W1 rip on off broadcast listen	- see page 10-19
set W1 route-filter incoming outgoing <i>Filtername</i>	- see page 10-8
set W1 speed 9600 14400 19200 38400 57600 76800 115200 56000 64000 1344k 1536k 2048k t1 t1e e1	- see page 6-21
show all	- see page 2-21
show W1	- see page 6-22

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 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1-1 for the range of synchronous ports available on each PortMaster model.



Note – Always set the port type to **network** for synchronous ports.

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 39-character hostname.

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*

<i>Seconds</i>	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 17-5

set w1 dlci - page 6-8

set w1 lmi - page 6-15

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.

This command should be set 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, PortMaster 4, 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, PortMaster 4, 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 14-9
set S0 compression - page 5-13
set user compression - page 13-8

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 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 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 8-10

set W1 dlci

Use these commands to add or delete data link connection identifiers (DLCIs) for Frame Relay service on a network hardwired synchronous port.

set W1 dlclist *Dlci_list*

add dlci|ipdlci|ipxdlci *W1 Dlci* **:***[Ipaddress|Ipxnode]*

delete dlci|ipdlci|ipxdlci *W1 Dlci*



Note – **set W1 dlclist** and **add dlci** perform the same function except that the command **add dlci** does not have a 244-character limitation. **ipdlci** is a synonym for **dlci**.

<i>Dlci_list</i>	Space-separated list of DLCIs. Up to a maximum of 244 characters.
<i>ipdlci</i> or <i>dlci</i>	Use for IP connections.
<i>ipxdlci</i>	Use for IPX connections.
<i>Dlci</i>	DLCI number, from 1 to 1023. You can add or delete only one DLCI number at a time.
:Ipaddress	Optional IP address of the router attached to the permanent virtual circuit (PVC) represented by the DLCI.
:Ipxnode	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 dlci** command and those created with the **add dlci W1** command.

Examples

```
Command> set w1 dlci 16 17 18
```

```
New DLCI List: 16 17 18
```

```
Command> set w1 dlci 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
```

```
Command> delete dlci w1 16
```

```
DLCI successfully deleted
```

See Also

add dlci - page 14-29

set W1 annex-d - page 6-4

set W1 lmi - page 6-15

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 referenced by each location in the location table. See page 14-10 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 14-10
set S0 group - page 5-20

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 indicates how long the PortMaster should wait 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 6-5

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 15-4

set W1 ofilter - page 6-19

show table filter - page 15-26

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 4-8

set ipx on - page 3-9

set S0 ipxnet - page 5-26

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 17-5
set W1 annex-d - page 6-4
set W1 dlci - page 6-8

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 6-20

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 10-7

set S0 netmask - page 5-33

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 5-34

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 15-4

set W1 ifilter - page 6-13

show table filter - page 15-26

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.

3.8

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 17-5
set W1 annex-d - page 6-4
set W1 lmi - page 6-15

set W1 speed

This command sets the reference speed for the synchronous port.

**set W1 speed 9600|14400|19200|38400|57600|76800|115200|
56000|64000|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 5-45

show W1

Shows the current status and configuration for the port. This command can be used for asynchronous, synchronous, ISDN, and parallel 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 2-22.
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 5-42.
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.

This chapter describes how to use the command line interface to configure the P0 parallel port 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 2-34

Summary of Parallel Port Commands

The parallel port commands in Table 7-1 configure the parallel port P0. See Table 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1, for the range of ports available on each PortMaster model.

Table 7-1 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 7-2
set p0 disabled	- see page 7-2
set p0 disconnect <i>Seconds</i> infinity	- see page 7-3
set p0 extended on off	- see page 7-4
set p0 host default prompt [1 2 3 4] <i>Ipaddress</i>	- see page 7-4
set p0 service_device netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 7-5
show all	- see page 2-21
show p0	- see page 2-34

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

This command disables the parallel port. 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 7-2

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—flow control—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** 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 39-character hostname as 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 5-22

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 7-2

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 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1-1, 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 2-19
- **set debug isdn on**—see page 17-7
- **show isdn**

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 8-1, 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 8-1 ISDN Port Commands

Command Syntax	
attach <i>S0</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 17-7
• set isdn-msn on off	- see page 8-4
set isdn-numberauto on off	- see page 8-5
set isdn-numberplan 0 1 2 7 8	- see page 8-6
set isdn-numbertype 0 1 2 4	- see page 8-7
• set isdn-switch net3 vn4 1tr6 ntt kdd	- see page 8-9
• set isdn-switch ni-1 dms-100 5ess 5ess-ptp	- see page 8-9
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 8-10
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</i> all directory dn <i>Number</i>	- see page 8-11
set <i>S10</i> all extended on off	- see page 5-19
set <i>S10</i> group <i>Group</i>	- see page 5-20
set <i>S10</i> hangup on off	- see page 5-21
set <i>S10</i> all host default prompt [1 2 3 4] <i>Ipaddress</i>	- see page 5-22
set <i>S10</i> all idletime <i>Number</i> [seconds minutes]	- see page 5-23
set <i>S10</i> all ifilter [<i>Filtername</i>]	- see page 5-25
set <i>S10</i> all login [network dialin dialout twoway]	- see page 5-27

Table 8-1 ISDN Port Commands (Continued)

Command Syntax	
set S10 all message <i>String</i>	- see page 5-30
set S10 all network dialin dialout twoway	- see page 5-34
set S10 all network hardwired	- see page 8-12
set S10 all ofilter [<i>Filtername</i>]	- see page 5-36
set S10 ospf	- see page 11-9
set S10 ofilter	- see page 5-36
set S10 all prompt <i>String</i>	- see page 5-39
set S10 all security on off	- see page 5-42
set S10 all service_device	- see page 5-43
netdata portmaster rlogin telnet [<i>Tport</i>]	
set S10 all service_login	- see page 5-44
netdata portmaster rlogin telnet [<i>Tport</i>]	
set S10 speed	- see page 8-13
• set S10 all spid <i>Number</i>	- see page 8-14
set S10 all termtype <i>String</i>	- see page 5-47
set S10 twoway Device [network dialin dialout twoway]	- see page 5-48
set S10 username autolog [<i>String</i>]	- see page 5-49
show all	- see page 2-21
show isdn [<i>dNumber</i> <i>S0</i>]	- see page 8-15
show pots	- see page 3-24
show S10	- see page 2-34

ISDN BRI Commands

These commands are used for configuring the ISDN BRI ports of the PortMaster. Table 1-1, “Configurable Ports Available for Each PortMaster Model,” on page 1-1 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 2-27

set isdn-numberauto

This command enables the PortMaster to automatically determine the ISDN number plan and number type for a received call.

3.8

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 8-6

set isdn-numbertype - page 8-7

show global - page 2-27

show isdn d0 - page 8-15

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 inform the switch about the kind of call 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 the available number plan attribute values and the current setting, enter **set isdn-numberplan** without any arguments. You can also view the current ISDN number plan and number type with 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 the change 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 8-5
set isdn-numbertype - page 8-7
show global - page 2-27
show isdn d0 - page 8-15

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 inform the switch about the kind of call being placed and where the call is to be routed. The PortMaster learns the ISDN number type automatically when the **set isdn-numberauto on** command is used, unless a specific number type is entered with the **set isdn-numbertype** command.

To display the available number type attribute values and the current setting, enter **set isdn-numbertype** without any arguments. You can also view the current ISDN number plan and number type with 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 the change 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 8-5

set isdn-numberplan - page 8-6

show global - page 2-27

show isdn d0 - page 8-15

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 8-11
set S10 spid - page 8-14

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 6-7

set S10|all dn

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 supports 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 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 8-9

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 S0|all network hardwired

Usage

ComOS 3.7 and later supports 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 8-10

show isdn d0 - page 8-15

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
```

S10	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 supports a line speed of 128Kbps for BRI ports. Only one BRI line can be configured for 128Kbps and when configured for 128Kbps, the second port 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 The ISDN port.

Number A number with 0 to 20 digits, provided by the ISDN service provider. Usually at least 9 digits long.

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. The **set all spid** command is not typically used in a BRI configuration but it can be useful when 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 8-9
set S10 dn - page 8-11

show isdn

This command shows the status of the ISDN ports.

show isdn [*dNumber*|*S0*]

- Number* 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*.

Examples

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

D	D channel associated with active session.
Ports	ISDN port numbers on the PortMaster.
State	Line status.
Change	Time since last change in status.
Start	Number of times a network termination 1 device (NT1) has attempted to bring up 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 D channel has timed out attempting to bring up the link.
Sess	Number of times PortMaster has received a connect message from the switch.
In	Number of input ISDN frames on B channel.
Out	Number of output ISDN frames on B channel.
Err	Number of cyclic redundancy check (CRC), abnormal termination, overrun, bad byte count (bbc), and lost frame errors.

```
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

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 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 register 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, and the digital modems on the PortMaster 3 and PortMaster 4. These PortMaster products can also use many of the commands common to all PortMaster models.

- For configuration information for all PortMaster products, see the *PortMaster Configuration Guide*.
- For additional configuration information and ComOS commands specific to the PortMaster 4, see the *PortMaster 4 Installation Guide*.



Note – After making any configuration changes to a line (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 ISDN PRI, T1, and E1 Diagnostic Information

To display PRI ISDN debug information on the console, use the following commands:

- **set console**—see page 2-19
- **set debug isdn on**—see page 17-7
- **set debug isdn-d frames on**—see page 17-7
- **set debug mdp-status on|off**—see page 17-9

When finished, use the following commands:

- **set debug off**—see page 17-5
- **reset console**—see page 2-15

To display line configuration or status, use the following commands:

- **show global**—see page 2-27
- **show sessions**—see page 2-38
- **show Line0**

- **show mcppp**
- **show modems**
- **show MO**

Summary of ISDN PRI, T1, and E1 Commands

The ISDN PRI, T1, and E1 configuration commands are shown in Table 9-1.

Table 9-1 PortMaster 3 Configuration Commands

Command Syntax	
attach <i>SO</i>	- see page 5-6
reset <i>MO</i>	- see page 9-4
reset <i>VO</i>	- see page 9-4
save all	- see page 2-18
set call-check on off	- see page 3-4
set debug isdn isdn-d frames termination on off	- see page 17-7
set debug mdp-status on off	- see page 17-9
set endpoint <i>Hex</i>	- see page 9-5
set isdn-switch net5 vn2 vn3 ltr6 ntt kdd ts014	- see page 9-6
set isdn-switch ni-2 dms-100 att-4ess att-5ess	- see page 9-6
set <i>Line0 line2</i> encoding b8zs ami hdb3	- see page 9-7
set <i>Line0 line2</i> framing esf d4 crc4 fas	- see page 9-8
set <i>Line0 line2</i> group <i>Cgroup</i> 56k 64k	- see page 9-8
set <i>Line0 line2</i> group <i>Cgroup</i> none channels <i>Channel-list</i>	- see page 9-9
set <i>Line0</i> isdn t1 e1 fractional isdn-fractional inband	- see page 9-10

Table 9-1 PortMaster 3 Configuration Commands (Continued)

Command Syntax	
set <i>Line0</i> line2 loopback on off	- see page 9-12
set <i>Line0</i> pcm u-law a-law	- see page 9-12
set <i>Line0</i> signaling wink immediate fxs	- see page 9-13
set <i>Line0</i> signaling r2generic mfr2	- see page 9-14
set line2 clock internal external	- see page 9-15
set line2 t1 fractional	- see page 9-10
set location <i>Locname</i> analog on off	- see page 9-16
set <i>MO</i> on off	- see page 9-16
set <i>MO</i> lastcall	- see page 9-17
set <i>SO</i> directory <i>Number</i>	- see page 9-18
show all	- see page 2-21
show <i>Line0</i>	- see page 9-19
show <i>MO</i>	- see page 9-23
show modems	- see page 9-25
show mcppp	- see page 9-26

ISDN PRI, T1, and E1 Commands

These commands are used for displaying the status of and configuring ISDN PRI, E1 or T1 lines, the T1 expansion card, digital modems, and Multichassis PPP connections.

reset M0

This command resets an internal digital modem and reloads its digital signal processor (DSP) code.

3.8

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 9-16

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 9-5

set endpoint

This command enables Multichassis PPP, which supports RFC 1990 Multilink PPP across multiple PortMaster products sharing an Ethernet.

set endpoint *Hex*

<i>Hex</i>	Endpoint discriminator—a 1 to 12-digit hexadecimal number. ComOS appends zeros if you specify less 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 endpoint 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 endpoint 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 endpoint discriminator to take effect.

Example

```
Command> set endpoint 00C005123456  
Endpoint Discriminator set to 00C005123456
```

See Also

reset *V0* - page 9-4

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. Any change you make to the switch type setting does not take effect until the PortMaster is rebooted.

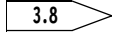
Example

```
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 .
	<i>line2</i>	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

3.8

<i>Line0</i>	line0 or line1 .
<i>line2</i>	T1 expansion card.
<i>esf</i>	Extended superframe. This is the default format for T1 lines.
<i>d4</i>	D4 framing, an alternative format for T1 lines.
<i>crc4</i>	Cyclic redundancy check 4. This is the default format for E1 lines.
<i>fas</i>	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

3.8

<i>Line0</i>	line0 or line1 .
<i>line2</i>	T1 expansion card.
<i>Cgroup</i>	Defined channel group from 1 to 63.
<i>56k</i>	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 9-10
set Line0 group channels - page 9-9

set Line0|line2 group channels

This command allows you to divide an ISD 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

3.8

<i>Line0</i>	line0 or line1 .
<i>line2</i>	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, or none to unassign channels.
<i>Channel-list</i>	Space-separated list of one or more channel numbers, from 1 through 24 for T1, or 1 through 30 for E1. The channel numbers do not have to be contiguous.

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 9-10

set Line0 group 64k - page 9-8

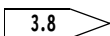
set Line0|line2

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.
3.8	isdn-fractional	Divides an ISDN line into groups specified by the set Line0 line2 group command (see page 9-9).
	fractional	Divides a channelized T1 line into groups specified by the set Line0 line2 group command (see page 9-9).
	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 9-13). For channelized E1, use the set Line0 signaling mfr2 command (see page 9-14).

Usage

ComOS releases 3.8 and later 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.



Note – The T1 card is hot-swappable. After removing the card from the PortMaster 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.



Note – T1 and E1 lines require an external clock signal provided either by the device that the PortMaster is connected to, or by the telephone company network.

set Line0|line2 loopback

This command sets a T1 or E1 line for local network loopback.

set Line0|line2 loopback on|off

3.8

<i>Line0</i>	line0 or line1 .
<i>line2</i>	T1 expansion card.
<i>on</i>	Turns on local network loopback.
<i>off</i>	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 pcm

This command sets the digital encoding method used for analog signals.

set Line0 pcm u-law|a-law

<i>Line0</i>	line0 or line1 .
<i>u-law</i>	Default method of analog-to-digital conversion used for T1 PRI lines.
<i>a-law</i>	Default method of analog-to-digital conversion used for E1 PRI lines.

Usage

This command is needed only when you are using digital modems in the PortMaster. The default settings must not be changed unless your PRI service provider instructs you otherwise.

3.8

ComOS releases 3.8 and later support the V.90 modem protocol for client modems with Lucent, Rockwell, and 3Com chipsets dialing in, and for both a-law and u-law encoding. V.90 is not supported for dial-out modems. The maximum analog dial-out speed is 33600bps for V.34, K56flex, and V.90 protocols.

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 *Line0* 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 9-10

set Line0 signaling r2generic|mfr2

This command sets inband signaling to multifrequency R2 signaling (MFR2) for a channelized E1 line.

3.8

set Line0 signaling r2generic|mfr2 Profile

<i>Line0</i>	line0 or line1 .
<i>r2generic</i>	Generic R2, the default when Line0 is set for inband signaling. Sets inband signaling to MFR2 but without tone signaling.
<i>mfr2 Profile</i>	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 release 3.8 and later 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 for 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 9-10

show Line0 - page 9-19

set line2 clock

This command sets the source for the clock signal for the T1 expansion card.

3.8

set line2 clock internal|external

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 digital service unit (DSU)/ channel service unit (CSU) 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 9-10

set location analog

This command sets the PortMaster to use an 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 MO

This command makes the digital modems on the PortMaster available or unavailable.

set MO on|off

<i>MO</i>	Any modem number from m0 to m59 . Changes to the default setting must be made to individual modems.
on	Makes the modem available for use. This is the default.
off	Busies the modem so it is unavailable.

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 9-16

set M0 lastcall

This command forces an active modem into ADMIN mode as soon as a user logs off.

set M0 lastcall

<i>M0</i>	Any modem number from m0 to m59 . Changes to the default setting must be made to individual modems.
-----------	---

Usage

ComOS releases 3.7.2c and later 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. 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 9-10
set M0 on|off - page 9-16
show M0 - page 9-23

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 Support. ComOS releases 3.8 and later 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

Shows the status of a E1 or T1 line on a PortMaster.

```
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              Violations
-----
Blue                0  Bipolar                102
Yellow              0  CRC Errors                1
Receive Carrier Loss 0  Multiframe Sync          9
Loss of Sync         0
```

Line0 is configured for inband signaling—channelized T1.

```
Command> show line0
----- line0 - T1 Inband DSO -----
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 9-8.
Encoding	Encoding method in use.	See page 9-7.
PCM	Pulse code modulation method in use.	See page 9-12.
Channel Group	Channel group number.	See page 9-9

Speed	Connect speed.	
Channels	Channel numbers.	See page 9-9.
Signaling	Type of inband signaling in use	See page 9-13 and page 9-13.
Options	Inband signaling options in use.	See page 9-13.
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.	
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 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.

show M0

M0 The digital modem number.

Example

```
Command> show m0
Card Type           Lucent Chipset
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							
Card Type	Displays the card type: <ul style="list-style-type: none"> • ADI Chipset—True Digital V.34 card • Lucent Chipset—True Digital K56flex card 						
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 or 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 modem retrain events.						
Renegotiations	Number of modem handshake renegotiation events.						
Total Calls	Total calls attempted.						
Modem Detects	Total calls where 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: <table> <tr> <td>No Modulation:</td><td>No signal modulation detected.</td></tr> <tr> <td>No Protocol:</td><td>No link-layer protocol detected.</td></tr> <tr> <td>Total Failed:</td><td>Total failed connections.</td></tr> </table>	No Modulation:	No signal modulation detected.	No Protocol:	No link-layer protocol detected.	Total Failed:	Total failed connections.
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: <table> <tr> <td>Lost Carrier:</td><td>DCD was lost, with consequent session termination.</td></tr> <tr> <td>Normal Disconnect:</td><td>Normal session termination.</td></tr> </table>	Lost Carrier:	DCD was lost, with consequent session termination.	Normal Disconnect:	Normal session termination.		
Lost Carrier:	DCD was lost, with consequent session termination.						
Normal Disconnect:	Normal session termination.						

show modems

Shows the status of all digital modems on a PortMaster.

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	UNKNWN	NONE	NONE	0	0	NORMAL

Explanation

Mdm	Digital modem number.
Port	PortMaster port assignment.
Status	ACTIVE The modem is in use. 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 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.

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 11, “OSPF Routing,” and Chapter 12, “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 10-1 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 10-1 Routing Commands

Command Syntax	
add ipxroute <i>Ipxnetwork Ipxaddress Metric Ticks</i>	- see page 10-14
add netmask <i>Ipaddress Ipmask</i>	- see page 10-23
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 10-3
add route <i>Ipaddress[/NM] Ipaddress(gw) Metric</i>	- see page 10-15
delete ipxroute <i>Ipxnetwork Ipxaddress</i>	- see page 10-16
delete netmask <i>Ipaddress</i>	- see page 10-24
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 10-3
delete route <i>Ipaddress Ipaddress(gw)</i>	- see page 10-17
reset propagation	- see page 10-6
save netmask	- see page 10-24
save route	- see page 10-17
set default <i>on off broadcast listen</i>	- see page 10-18
set <i>Ether0 S0 W1 netmask Ipmask</i>	- see page 10-7
set <i>Ether0 S0 W1 rip on off broadcast listen</i>	- see page 10-19
set <i>Ether0 S0 W1 user Username location Locname route-filter incoming outgoing Filtername</i>	- see page 10-8
set gateway <i>Ipaddress [Metric]</i>	- see page 10-12
set location <i>Locname rip on off broadcast listen</i>	- see page 10-20
set user <i>Username rip on off broadcast listen</i>	- see page 10-21

Table 10-1 Routing Commands (Continued)

Command Syntax	
set user-netmask on off	- see page 10-13
show ipxroutes	- see page 10-25
show propagation	- see page 10-26
show routes [<i>String Prefix/NM</i>]	- see page 10-28
show route to-dest <i>Ipaddress</i>	- see page 10-30
show table netmask	- see page 10-31

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 PortMaster 3, PortMaster 4, and IRX products.

add propagation *Protocol(src) Protocol(dest) Metric Filtername*

delete propagation *Protocol(src) Protocol(dest)*

<i>Protocol(src)</i>	<p>Designates the source protocol of the route. Use one of the following keywords:</p> <ul style="list-style-type: none">• rip• static• ospf• bgp
<i>Protocol(dest)</i>	<p>Designates the destination routing protocol for the route propagation. Use one of the following keywords:</p> <ul style="list-style-type: none">• rip• static• ospf• bgp
<i>Metric</i>	<p>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.</p> <p>By default, all routes propagate and the common metric is 0.</p>
<i>Filtername</i>	<p>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.</p>



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 is 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 15-4
set Ether0 ospf accept-rip on - page 11-7
set filter - page 15-6

reset propagation

This command resets the propagation rules system.

reset propagation

Usage

This command should 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 12-14

reset ospf - page 11-6

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 14-19

set user netmask - page 13-18

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 12, “Configuring BGP,” 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.
<i>incoming</i>	Inbound filter.
<i>outgoing</i>	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 10-2 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 10-2 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 10-2 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 10-3 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                                Options: Quiet, Compression
MTU: 1500                                  Async Map: 00000000
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:
```

```

Command> set user zephyr route-filter outgoing routes.out
Username: zephyr                                     Type: Dial-in Network User
Address: Negotiated                                 Netmask: 255.255.255.255
Protocol: PPP                                       Options: Quiet Compression
MTU: 1500                                           Async Map: 00000000
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

```

See Also

add filter - page 15-4
reset ospf - page 11-6
set bgp policy (advertisement) - page 12-34
set bgp policy (injection) - page 12-29

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 10-28

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 release 3.5 and later supports 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 – You should 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 10-15

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 10-16

show ipxroute - page 10-25

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 should 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 10-23
add user-netmask - page 10-13
delete route - page 10-17
show ipxroute - page 10-25

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 10-14
show ipxroutes - page 10-25

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</i> (<i>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 10-15

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



Note – 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 messages, and if the PortMaster has a default route it is advertised to RIP.

Example

Command> **set default on**

Default routing changed from off (no_broadcast,no_listen) to on (broadcast,listen)

See Also

set gateway *Ipaddress* - page 10-12

show global - page 2-27

set Ether0|S0|W1 rip

This command enables RIP on a specified interface.

set Ether0|S0|W1 rip on|off|broadcast|listen

<i>Ether0</i>	Ethernet interface.
<i>S0</i>	Network hardwired asynchronous port.
<i>W1</i>	Network hardwired synchronous port.
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 10-20

set user rip - page 10-21

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 10-18

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 13-4

set default - page 10-18

Netmask Commands

The netmask commands configure a table of 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 10-24

save netmask - page 10-24

show table netmask - page 10-31

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 10-23
save netmask - page 10-24
show table netmask - page 10-31

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 10-23

delete netmask - page 10-24

show table netmask - page 10-31

Routing Information

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 PortMaster 3, PortMaster 4, and IRIX 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 *PortMaster Routing Guide* for a description of a routing table.

show routes [*String*|*Prefix/NM*]

- String*

Displays only routes that contain the matching *String*. For example, **show routes local** shows only routes that contain the matching *String* **local** 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.

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: <table> <tr> <td>local</td><td>Route learned from an interface on the PortMaster.</td></tr> <tr> <td>rip</td><td>RIP route learned from a connected network.</td></tr> <tr> <td>ospf</td><td>OSPF route learned from an internal neighbor.</td></tr> <tr> <td>ospf/E1 ospf/E2</td><td>OSPF route learned from Type 1 external or Type 2 external routes.</td></tr> <tr> <td>ospf/N1 ospf/N2</td><td>OSPF route learned as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).</td></tr> <tr> <td>ospf/IA</td><td>OSPF route originating from another area and learned via an area border router.</td></tr> <tr> <td>bgp/D</td><td>BGP route for the default network (network 0).</td></tr> <tr> <td>bgp/E</td><td>BGP route learned from an external neighbor.</td></tr> <tr> <td>bgp/I</td><td>BGP route learned from an internal neighbor.</td></tr> </table>	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.
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.																		
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 route						
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 10-28

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 10-23
- delete netmask** - page 10-24
- save netmask** - page 10-24
- set user-netmask** - page 10-13
- show routes** - page 10-28

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 2-27
- **show memory**—see page 2-30
- **show propagation**—see page 10-26
- **ifconfig**—see page 2-9, and this chapter
- **show ospf areas**
- **show ospf links**
- **show ospf neighbors**
- **show routes**

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

Summary of OSPF Commands

OSPF commands allow you to configure the PortMaster to use the OSPF IP routing protocol.

Table 11-1 OSPF Commands

Command Syntax	
add ospf area <i>Area</i>	- see page 11-4
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 10-3
add route <i>Ipaddress/[NM] IPaddress(gw) Metric</i>	- see page 10-15
delete ospf area <i>Area</i>	- see page 11-5
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 10-3
ifconfig	- see page 2-9 and page 11-5
reset ospf	- see page 11-6
reset propagation	- see page 10-6
save ospf	- see page 11-7
set debug ospf on off	- see page 17-10
set Ether0 ospf accept-rip on off	- see page 11-7
set Ether0 ospf on off [cost Number] [hello-interval Seconds] [dead-time Seconds]	- see page 11-8
set Ether0 S0 W0 user Username location Locname route-filter in out Filtername	- see page 10-8
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]	- see page 11-9

Table 11-1 OSPF Commands (Continued)

Command Syntax	
set ospf area <i>Area</i> external on off	- see page 11-12
set ospf area <i>Area</i> md5 <i>Number String</i>	- see page 11-13
set ospf area <i>Area</i> nssa on off	- see page 11-14
set ospf area <i>Area</i> password <i>String</i>	- see page 11-15
set ospf area <i>Area</i> range <i>Prefix/NM</i> [advertise quiet off]	- see page 11-16
set ospf area <i>Area</i> stub-default-cost <i>Number</i>	- see page 11-17
set ospf enable disable	- see page 11-18
set ospf priority <i>Number</i>	- see page 11-19
set ospf router-id <i>Ipaddress Number</i>	- see page 11-20
show ospf areas	- see page 11-21
show ospf links [router network summary external nssa]	- see page 11-24
show ospf neighbor	- see page 11-27
show propagation	- see page 10-26
show routes [<i>String Prefix/NM</i>]	- see page 11-29
show table ospf	- see page 11-21

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
```

See Also

set ospf area - page 11-16

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 (BDR), 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 ffffffff00 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. The range is 0 to 15. Lower-cost routes are preferred.
<i>Number</i>	Assigned cost for the interface—a 16-bit number between 1 and 65535. The default is 1.
hello-interval Seconds	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 Seconds	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.

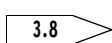
set location|S0|S10|W1|user ospf on|off

This command enables or disables the OSPF protocol and allows optional settings on any network hardwired port, location, or user.

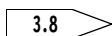
set location *Locname*|*S0*|*S10*|*W1*|**user** *Username* **ospf on|off** [**cost** *Number*]
[**hello-interval** *Seconds*] [**dead-time** *Seconds*] [**nbma|point-to-**
multipoint|wan-as-stub-ptmp]



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>	Synchronous port—configured as a network hardwired port.
<i>Username</i>	Login or network user in the user table.
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.
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 route** 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 11-24
show routes - page 11-29

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 11-14
set ospf area stub-default-cost - page 11-17

set ospf area md5

This command sets the secret for the OSPF area using the Message-Digest Algorithm (MD5) from RSA Data Security, Inc., as defined in RFC 1321.



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 11-17

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 11-12
set ospf area nssa - page 11-14

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*

<i>Ipaddress</i>	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.
<i>Number</i>	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 11-19

show ospf areas

This command shows 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**. MD5 is the Message-Digest Algorithm from RSA Data Security, Inc., as defined in RFC 1321.

Command> **show ospf areas**

Area	Network Range	Authentication			External Routes	Stub Default Cost
		Type	ID	Key		
-----	-----	-----	---	-----	-----	-----
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 11-16). 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 11-15, and the set ospf area md5 command on page 11-13.
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 11-12.	
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.

See the examples of using the **ifconfig** command on page 11-5 to show 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 11-13 for more information.

show routes

This command shows the IP routing table. See the information on routing tables in the *PortMaster Routing 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: <table><tr><td>local</td><td>Route learned from an interface on the PortMaster.</td></tr><tr><td>rip</td><td>RIP route learned from a connected network.</td></tr><tr><td>ospf</td><td>OSPF route learned from an internal neighbor.</td></tr><tr><td>ospf/E1 ospf/E2</td><td>OSPF route learned from Type 1 external or Type 2 external routes.</td></tr><tr><td>ospf/N1 ospf/N2</td><td>OSPF route learned as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).</td></tr><tr><td>ospf/IA</td><td>OSPF route originating from another area and learned via an area border router.</td></tr><tr><td>bgp/D</td><td>BGP route for the default network (network 0).</td></tr><tr><td>bgp/E</td><td>BGP route learned from an external neighbor.</td></tr><tr><td>bgp/I</td><td>BGP route learned from an internal neighbor.</td></tr><tr><td>temp</td><td>Route learned from RADIUS. Removed from the routing table when the user logs off.</td></tr></table>	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.
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, PortMaster 3, or PortMaster 4, 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 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 2-27
- **show memory**—see page 2-30
- **show propagation**—see page 10-26
- **show bgp memory**
- **show bgp next-hop**
- **show bgp path**
- **show bgp peers**
- **show bgp policy**
- **show bgp summarization**

Summary of BGP Commands

BGP commands, shown in Table 12-1, allow you to configure the PortMaster for BGP routing.

Table 12-1 BGP Commands

Command Syntax	
add delete bgp policy <i>Policyname</i> all	- see page 12-4
add propagation <i>Protocol(src) Protocol(dest) Metric Filtername</i>	- see page 10-3
add set bgp peer <i>Ipaddress(src) Ipaddress(dest) ASN</i> [assume-default [Number]] [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 12-5
add 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 12-10
delete bgp peer <i>IPaddress(dest)</i>	- see page 12-5
delete bgp policy <i>Policyname</i> all	- see page 12-4
delete bgp summarization <i>Prefix/NM</i>	- see page 12-10
delete propagation <i>Protocol(src) Protocol(dest)</i>	- see page 10-3
reset bgp [peer <i>Ipaddress</i>]	- see page 12-14
reset propagation	- see page 10-6
save bgp	- see page 12-15
set bgp as <i>ASN</i>	- see page 12-15
set bgp cluster-id <i>Ipaddress</i>	- see page 12-16
set bgp cma <i>ASN</i>	- see page 12-17
set bgp connect-retry-interval <i>Seconds</i>	- see page 12-18
set bgp enable disable	- see page 12-19

Table 12-1 BGP Commands (Continued)

Command Syntax	
set bgp hold-time <i>Seconds</i>	- see page 12-19
set bgp id <i>Ipaddress</i>	- see page 12-20
set bgp igp-lockstep on off	- see page 12-20
set bgp keepalive-timer <i>Seconds</i>	- see page 12-21
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 12-22, page 12-29, page 12-34
set bgp policy <i>Policyname</i> blank	- see page 12-42
set debug bgp on off	- see page 17-2
show bgp memory	- see page 12-42
show bgp next-hop	- see page 12-43
show bgp paths [<i>Prefix/NM</i> [verbose]]	- see page 12-45
show bgp peers [verbose packets]	- see page 12-48
show bgp policy [<i>Policyname</i>]	- see page 12-54
show bgp summarization [all]	- see page 12-55
show routes [<i>String Prefix/NM</i>]	- see page 12-57

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|delete bgp policy

These commands create or delete a BGP policy for route acceptance, injection, or advertisement.



Caution – Be careful when deleting BGP policy statements. Make sure that they are no longer needed for BGP route selection.

add|delete bgp policy *Policyname* |all

<i>Policyname</i>	Name of the policy to be created or 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. Use the **delete bgp policy** command to delete a BGP policy. Define BGP policies with the **set bgp policy** commands.

Examples

```
Command> add bgp policy admit  
New BGP policy admit successfully added
```

```
Command> delete bgp policy admit  
BGP policy admit successfully deleted
```

See Also

set bgp policy (acceptance) - page 12-22
set bgp policy (injection) - page 12-29
set bgp policy (advertisement) - page 12-34

add|set|delete bgp peer

These commands create, modify, or delete entries on the PortMaster for BGP peers, and provide options that control how policies are implemented for route selection.

```
add|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]}
```

```
delete bgp peer Ipaddress(dest)
```

add	Creates a new peer.
set	Modifies an existing peer. All settings need to be respecified.
delete	Deletes an existing peer.
<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>Polycname</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 12-22), 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	Predefined policy that you can use to permit all routes to be accepted, injected, or advertised.
<i>Polycname</i>	Name of a BGP policy statement defined by the set bgp policy command.
inject-policy	<p>Enables a BGP policy <i>Polycname</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>Polycname</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 12-22
set bgp policy (injection) - page 12-29
set bgp policy (advertisement) - page 12-34

add|set|delete bgp summarization

These commands create, modify, or delete a BGP summarization entry that indicates how internal gateway protocol (IGP) routing information from OSPF, RIP, or static routing is forwarded into BGP for advertisement to other BGP peers.

```
add|set bgp summarization Prefix/NM  
[as ASN] [cma ASN] [multi-exit-disc Number]  
[local-pref Number] [community Tag]
```

```
delete bgp summarization Prefix/NM
```

add	Creates a new BGP summarization entry.
set	Modifies an existing BGP summarization entry. All settings need to be respecified.
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.
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 *Number*

Assigns an arbitrary rating *Number* to an external route for advertisement to external or confederation-member peers only. *Number* is a 32-bit integer.

multi-exit-disc can be abbreviated as **med** 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, 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.

<i>community</i>	Advertises the 32-bit community attribute, defined by <i>Tag</i> , along with this summarization.
<i>Tag</i>	<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:
no-export	<p>Destinations only within a confederation. Advertise the route only to BGP peers within your confederation or autonomous system.</p>
no-advertise	<p>No destinations. Do not advertise this route.</p>
no-export-subconfed	<p>Internal destinations only. Advertise this route only to internal BGP peers.</p>

The restrictions imposed by these reserved community keywords do not apply to the PortMaster originating this information.

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.

Examples

```
Command> set bgp summarization 172.16.0.0/16 multi 55 as 2 as 3 as 4  
BGP summarization successfully added
```

```
Command> delete bgp summarization 172.16.0.0/16  
BGP summarization to 172.16.0.0/16 successfully deleted
```

See Also

set bgp policy - page 12-22

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.

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.

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*

<i>ASN</i>	The 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*

<i>Seconds</i>	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*

<i>Seconds</i>	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 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]]
```

<i>Polycname</i>	Name of an acceptance 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. • A maximum of 160 rules is permitted in a policy. If more rules are needed, they can be added with the include <i>Polycname</i> 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>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 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> <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

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 Number | strip` Assigns an arbitrary *Number* for the learned multiexit discriminator, overriding any that is learned from the peer. *Number* 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 Number` Assigns a degree-of-preference *Number* to a route. *Number* 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 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 polycname 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.

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.

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.

You can create any number of injection 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.

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.

<code>include</code> <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.
<code>if</code>	<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.
<code>prefix Prefix/NM</code>	<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>
<code>exactly</code>	Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.

<i>as-path 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

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 set of metrics to any IP prefix selected for advertisement before advertising it.

`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
Ipaddress

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 *Tag* to the IP prefix to be advertised.

replace

Replaces the community categories identified in the community *Tag* of the IP prefix to be advertised with new *Tag* 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.

You can create any number of 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.

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> 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 12-4
set bgp policy (acceptance) - page 12-22
set bgp policy (injection) - page 12-29
set bgp policy (advertisement) - page 12-34

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: <table><tr><td>local</td><td>Route learned from an interface on the PortMaster.</td></tr><tr><td>rip</td><td>RIP route learned from a connected network.</td></tr><tr><td>ospf</td><td>OSPF route learned from an internal neighbor.</td></tr><tr><td>ospf/E1 ospf/E2</td><td>OSPF route learned from Type 1 external or Type 2 external routes.</td></tr><tr><td>ospf/N1 ospf/N2</td><td>OSPF learned route as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).</td></tr><tr><td>ospf/IA</td><td>OSPF route originating from another area and learned via an area border router.</td></tr><tr><td>bgp/D</td><td>BGP route for the default network (network 0).</td></tr><tr><td>bgp/E</td><td>BGP route learned from an external neighbor.</td></tr><tr><td>bgp/I</td><td>BGP route learned from an internal neighbor.</td></tr></table>	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.
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> : <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/BMA/BMP</i> : + 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.

BMA	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: <table> <tr> <td>C</td><td>Identifies this peer as a confederation member peer of the PortMaster.</td></tr> <tr> <td>R</td><td>Identifies this peer as a route-reflector client of the PortMaster.</td></tr> <tr> <td>N</td><td>This peer is configured to always consider the PortMaster as the next hop for any update packet sent from this peer.</td></tr> </table>	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.
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: <table> <tr> <td>Up</td><td>Peer is in a fully established state.</td></tr> <tr> <td>Dn</td><td>Peer is not in a fully established state.</td></tr> </table>	Up	Peer is in a fully established state.	Dn	Peer is not in a fully established state.		
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 NLRIs Policy: all
Inject NLRIs Policy: all
Advertise NLRIs 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:	
	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:	
	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...:	Number of seconds that must elapse before the next timed event will occur:	<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 [*Policyname*]

Policyname	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: <table><tr><td>local</td><td>Route learned from an interface on the PortMaster.</td></tr><tr><td>rip</td><td>RIP route learned from a connected network.</td></tr><tr><td>ospf</td><td>OSPF route learned from an internal neighbor.</td></tr><tr><td>ospf/E1 ospf/E2</td><td>OSPF route learned from Type 1 external or Type 2 external routes.</td></tr><tr><td>ospf/N1 ospf/N2</td><td>OSPF route learned as Type 1 external or Type 2 external routes from not-so-stubby areas (NSSAs).</td></tr><tr><td>ospf/IA</td><td>OSPF route originating from another area and learned via an area border router.</td></tr><tr><td>bgp/D</td><td>BGP route for the default network (network 0).</td></tr><tr><td>bgp/E</td><td>BGP route learned from an external neighbor.</td></tr><tr><td>bgp/I</td><td>BGP route learned from an internal neighbor.</td></tr></table>	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.
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.																		

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 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, you should use RADIUS for user authentication rather than the user table. To use RADIUS see Chapter 3, “Global Commands,” and the *RADIUS 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 14, “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**

Summary of User Commands

The user commands in Table 13-1 configure the user table used to authenticate dial-in users. The **User Type** column in the table denotes commands for login user (L) and netuser (N). RADIUS can also be used to authenticate dial-in users; the user table is always consulted first.

Table 13-1 User Table Configuration

User Type	Command Syntax	
N	add netuser <i>Username</i> [password <i>Password</i>]	- see page 13-4
L	add user <i>Username</i> [password <i>Password</i>]	- see page 13-5
L/N	delete user <i>Username</i>	- see page 13-5
L/N	save user	- see page 13-6
N	set user <i>Username</i> address destination assigned negotiated <i>Ipaddress</i>	- see page 13-6
N	set user <i>Username</i> compression on off	- see page 13-8
L/N	set user <i>Username</i> dialback <i>Locname String none</i>	- see page 13-9
L	set user <i>Username</i> host default prompt <i>Ipaddress</i>	- see page 13-10
L/N	set user <i>Username</i> idle <i>Number</i> [minutes seconds]	- see page 13-11
L/N	set user <i>Username</i> ifilter [<i>Filtername</i>]	- see page 13-12
N	set user <i>Username</i> ipxnet <i>Ipxnetwork</i>	- see page 13-13
N	set user <i>Username</i> local-ip-address <i>Ipaddress</i>	- see page 13-14
N	set user <i>Username</i> map <i>Hex</i>	- see page 13-15
L/N	set user <i>Username</i> maxports <i>Number</i>	- see page 13-16
N	set user <i>Username</i> mtu <i>MTU</i>	- see page 13-17
N	set user <i>Username</i> netmask <i>Ipmask</i>	- see page 13-18
N	set user <i>Username</i> ofilter [<i>Filtername</i>]	- see page 13-19

Table 13-1 User Table Configuration (Continued)

User Type	Command Syntax	
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 11-9
L/N	set user <i>Username</i> password <i>Password</i>	- see page 13-20
N	set user <i>Username</i> protocol slip ppp x75-sync	- see page 13-21
N	set user <i>Username</i> rip on off broadcast listen	- see page 10-21
L/N	set user <i>Username</i> route-filter incoming outgoing <i>Filtername</i>	- see page 10-8
L	set user <i>Username</i> service netdata portmaster rlogin telnet [<i>Tport</i>]	- see page 13-22
L/N	set user <i>Username</i> session-limit <i>Minutes</i>	- see page 13-23
L/N	set user <i>Username</i> route-filter incoming outgoing <i>Filtername</i>	- see page 10-8
L/N	show table user	- see page 13-24
L/N	show user <i>Username</i>	- see page 13-25

User Commands

These commands configure the user table of the PortMaster.



Note – 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 A network username of 1 through 8 characters.

Password A 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 13-5

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 13-24

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*

Username 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

<i>Username</i>	Name of a network user.
on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression on PortMaster 3, PortMaster 4, 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 39-character hostname.

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 5-22

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.
<i>idle Number</i>	Timeout value from 0 to 240. The default value is 0.
<i>minutes</i>	Sets the idle time in minutes. This is the default.
<i>seconds</i>	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 13-23

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 the 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 15-4

set user host prompt - page 13-10

set user ofilter - page 13-19

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

The PPP protocol must be used with IPX. If you set the IPX network number to OXFFFFFFFE, 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 a numbered IP network. 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.



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 13-6

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 should be replaced. The lowest-order bit corresponds to the first ASCII character NUL and so on. Most environments should 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*

<i>Username</i>	Name of a user.
<i>Number</i>	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 14-16

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 13-21

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 10-13

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

set user ifilter - page 13-12

add filter - page 15-4

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 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 5-34

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.
<i>netdata</i>	Uses a netdata connection (TCP clear channel).
<i>portmaster</i>	Uses the PortMaster login service to connect to in.pmd on login host. This is the default.
<i>rlogin</i>	Uses the rlogin protocol to connect to the login host.
<i>telnet</i>	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 5-44

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 13-11

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 13-25

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 13-24

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

Summary of Location Commands

The location table commands in Table 14-1 are used to configure the location table, used for network dial-out.

Table 14-1 Location Table Commands

Command Syntax	
add location <i>Locname</i>	- see page 14-3
delete location <i>Locname</i>	- see page 14-4
save location	- see page 14-5

Table 14-1 Location Table Commands (Continued)

Command Syntax	
set location <i>Locname</i> analog on off	- see page 14-5
set location <i>Locname</i> automatic manual on_demand	- see page 14-6
set location <i>Locname</i> chap on off	- see page 14-8
set location <i>Locname</i> compression on off stac vj	- see page 14-9
set location <i>Locname</i> destination <i>Ippaddress</i>	- see page 14-10
set location <i>Locname</i> group <i>Group</i>	- see page 14-10
set location <i>Locname</i> high_water <i>Number</i>	- see page 14-11
set location <i>Locname</i> idletime <i>Number</i> [minutes seconds]	- see page 14-12
set location <i>Locname</i> ifilter [<i>Filtername</i>]	- see page 14-13
set location <i>Locname</i> ipxnet <i>Ipxnetwork</i>	- see page 14-14
set location <i>Locname</i> local-ip-address <i>Ippaddress</i>	- see page 14-15
set location <i>Locname</i> map <i>Hex</i>	- see page 14-15
set location <i>Locname</i> maxports <i>Number</i>	- see page 14-16
set location <i>Locname</i> mtu <i>MTU</i>	- see page 14-17
set location <i>Locname</i> multilink on off	- see page 14-18
set location <i>Locname</i> netmask <i>Ipmask</i>	- see page 14-19
set location <i>Locname</i> ofilter [<i>Filtername</i>]	- see page 14-19
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 11-9
set location <i>Locname</i> password <i>Password</i>	- see page 14-20
set location <i>Locname</i> protocol slip ppp frame_relay x75-sync	- see page 14-21

Table 14-1 Location Table Commands (Continued)

Command Syntax	
set location <i>Locname</i> rip on off broadcast listen	- see page 10-20
set location <i>Locname</i> route-filter incoming outgoing <i>Filtername</i>	- see page 10-8
set location <i>Locname</i> script v25bis <i>RuleNumber</i> "String1" "String2"	- see page 14-22
set location <i>Locname</i> telephone <i>String</i>	- see page 14-24
set location <i>Locname</i> username <i>Username</i>	- see page 14-25
set location <i>Locname</i> voice on off	- see page 14-26
show location <i>Locname</i>	- see page 14-27
show table location	- see page 14-28

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 14-4

save location - page 14-5

show table location - page 14-28

delete location

This command deletes a location from the location table.

delete location *Locname*

<i>Locname</i>	A previously created location name that is in the location table.
----------------	---

Example

Command> **delete location hq**
Location hq successfully deleted

See Also

add location - page 14-3

save location - page 14-5

show table location - page 14-28

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 PortMaster to use 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 14-26

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 14-12

set location chap

This command is used for configuring outbound CHAP authentication for a specified location.

set location *Locname* **chap on|off**

<i>Locname</i>	Location name that is in the location table.
on	CHAP authentication is required for an outbound dial.
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 3-5

set location password - page 14-20

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, PortMaster 4, 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, PortMaster 4, 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 39-character hostname 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. Assigned addresses are not supported for dial-out locations. 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 5-20

set W1 group - page 6-10

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 14-10
set location maxports - page 14-16

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 240. 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 15-4

set location ofilter - page 14-19

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

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 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 location *Locname* **local-ip-address** *Ipaddress*

Locname Location name that is in the location table.

Ipaddress IP address or 39-character hostname.

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 14-10

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 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 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, idle time is used to decide when to disconnect unused lines.

The maximum number of ports should 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 14-11

set location multilink - page 14-18

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 14-21

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 14-11
set location maxports - page 14-16

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.

You remove the filter by entering 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 15-4

set location ifilter - page 14-13

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
```

Locname Location name that is in the location table.

Password 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 14-8. 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 to set up location table scripting when dialing to a remote location.

Example

```
Command> set location denver password excalcolaur
New password successfully set for location denver
```

See Also

set location chap - page 14-8
set location script - page 14-22
set location telephone - page 14-24
set location username - page 14-25

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>	A location name that is in the location table.
slip	SLIP protocol.
ppp	PPP protocol.
frame_relay	Frame Relay subinterface.
x75-sync	X.75 protocol.

3.8

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 14-29

set location mtu - page 14-17

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 should 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 up. 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, for PPP users, 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 14-24—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 should 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 should 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 14-20
set location telephone - page 14-24
set location username - page 14-25

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 for PPP users 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.

Examples

Command> **set location denver telephone 13035551212&13035551313**
New telephone successfully set for location denver

See Also

set location password - page 14-20
set location script - page 14-22
set location username - page 14-25

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*

Locname Location name that is in the location table.

Username 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 for PPP users 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.

Example

Command> **set location denver username sanjose**
New username successfully set for location denver

See Also

set location chap - page 14-8
set location password - page 14-20
set location script - page 14-22
set location telephone - page 14-24

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 14-3
set location analog - page 14-5
show location - page 14-28

show location

This command displays configuration information for a specified location.

show location *Locname*

Locname Location name that is in the location table.

Example

```
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
```

See Also

show all - page 2-21

show S0 - page 2-34

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

DLCI Commands

The DLCI table commands in Table 14-2 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 14-2 DLCI Table Commands

Command Syntax	
add dlci <i>ipdlci</i> <i>ipxdlci</i> <i>Locname</i> <i>Dlci</i> [<i>Ipaddress</i> <i>Ipxnode</i>]	- see page 14-29
delete dlci <i>ipdlci</i> <i>ipxdlci</i> <i>Locname</i> <i>Dlci</i>	- see page 14-31
show location <i>Locname</i>	- see page 14-27

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**.

<i>ipdlci</i> or <i>dlci</i>	Use for IP connections.
<i>ipxdlci</i>	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 6-8

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.

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 14-29
delete dlci - page 6-8

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 referenced 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.

Summary of Filter Commands

The commands in Table 15-1 configure the filter table. Filters can be applied to Ethernet interfaces, users, locations, network hardwired ports, or protocols, and can be used for debugging with the **ptrace** command.



Note – The commands should be entered on one line, without any breaks. Line breaks shown here are due to the limited space available.

Table 15-1 Filter Table Configuration

Command Syntax	
add filter <i>Filtername</i>	- see page 15-4
delete filter <i>Filtername</i>	- see page 15-4
save filter	- see page 15-5
set filter <i>Filtername</i> blank	- see page 15-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress(dest)/NM</i>] [esp ah ipip ospf] [log] [notify]	- see page 15-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</i> <i>Ipaddress(dest)/NM</i>] [protocol <i>Number</i>] [log] [notify]	- see page 15-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>=ListName</i> <i>Ipaddress(dest)/NM</i> [esp ah ipip ospf] [log] [notify]	- see page 15-6
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>=ListName</i> <i>Ipaddress(dest)/NM</i> [protocol <i>Number</i>] [log] [notify]	- see page 15-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM</i> <i>=ListName</i> [esp ah ipip ospf] [log] [notify]	- see page 15-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny <i>Ipaddress/NM</i> <i>=ListName</i> [protocol <i>Number</i>] [log] [notify]	- see page 15-7
set filter <i>Filtername</i> <i>RuleNumber</i> permit deny [<i>Ipaddress/NM</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 15-9

Table 15-1 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 15-9
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 15-10
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 15-15
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 15-15
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 15-15
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 15-18
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 15-18
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 15-18
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 15-20
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 15-23
show filter ipxfilter sapfilter <i>Filtername</i>	- see page 15-25
show table filter	- see page 15-26

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 15-4

show table filter- page 15-26

save filter

This command writes 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
Removed all rules from filter test
```

See Also

delete filter - page 15-4

set filter (IP)

These commands configure a filter that controls passage of a packet through an interface.



Note – Enter this 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 to compare with the source IP address of the packet. Hostnames are not recognized.
<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). 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 is used to cause 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> .
= <i>ListName</i>	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 that 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.

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

```
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 15-4
set choicenet - page 3-30
set loghost - page 3-11

set filter (TCP)

These commands set filtering rules for TCP packets.



Note – Enter this 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
Ippaddress/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>Ippaddress</i>	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.
<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>Ippaddress(dest)</i>	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.
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 15-2 for a list of the port numbers 20 through 1647 commonly assigned to TCP and UDP services.
<i>dst</i>	Specifies that the packet destination port number be tested; see “Usage” for test criteria.
<i>established</i>	Accepts only packets being sent to an established TCP network connection, and denies packets sent to establish new TCP connections.
<i>log</i>	Packets matching the rule are logged by syslog to the loghost.
<i>notify</i>	Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword is used to cause 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.

Table 15-2 TCP and UDP Port Services

Service	Port	Protocol	Description
ftp-data	20	TCP	File Transfer Protocol (FTP) (default data)
ftp	21	TCP	FTP (control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer Protocol (SMTP) (email)
nicname	43	TCP	whois Internet directory service
nicname	43	UDP	whois Internet directory service
domain	53	TCP	Domain Name System (DNS)
domain	53	UDP	DNS
tftp	69	UDP	Trivial File Transfer Protocol (TFTP)
gopher	70	TCP	Gopher

Table 15-2 TCP and UDP Port Services (Continued)

Service	Port	Protocol	Description
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)
ntp	123	TCP	Network Time Protocol (NTP)
ntp	123	UDP	NTP
snmp	161	TCP	Simple Network Management Protocol (SNMP)
snmp	161	UDP	SNMP
snmptrap	162	TCP	SNMP system management messages
snmptrap	162	UDP	SNMP system management messages
imap3	220	TCP	Interactive Mail Access Protocol (IMAP) version 3
imap3	220	UDP	IMAP version 3
exec	512	TCP	Remote process execution
login	513	TCP	Remote login
who	513	UDP	Remote who daemon (rwhod)
cmd	514	TCP	Remote command (rsh)
syslog	514	UDP	System log facility

Table 15-2 TCP and UDP Port Services (Continued)

Service	Port	Protocol	Description
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

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 15-4
set loghost - page 3-11

set filter (UDP)

This command sets filtering rules for User Datagram Protocol (UDP) packets.



Note – Enter this 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, to compare with the destination IP address of the packet. Hostnames are not recognized.

<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>Ippaddress(dest)</i>	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.
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 15-2 for a list of the port numbers 20 through 1647 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 is used to cause 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 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

```
Command> set filter w1.in 5 permit udp src eq 53
Filter w1.in updated
```

```
Command> set filter w1.in 6 permit udp dst eq 53
Filter w1.in updated
```

See Also

add filter - page 15-4
set loghost - page 3-11

set filter (ICMP)

These commands set filtering rules for Internet Control Message Protocol (ICMP) packets.



Note – Enter this 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, to compare with the destination IP address of the packet. Hostnames are not recognized.

<i>/NM</i>	<p>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</p> <p>/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.</p>
<i>Ipaddress(dest)</i>	<p>IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.</p>
<i>Itype</i>	<p>ICMP message type to compare against the ICMP message type contained in the packet. ICMP message types are defined in RFC 1700, <i>Assigned Numbers</i>. Common ICMP types are the following:</p> <p>0—Echo reply 3—Destination Unreachable 4—Source Quench 5—Redirect 8—Echo 11—Time Exceeded 12—Parameter Problem 13—Timestamp 14—Timestamp Reply 15—Information Request 16—Information Reply</p>
<i>log</i>	<p>Packets matching the rule are logged by syslog to the loghost.</p>
<i>notify</i>	<p>Packets matching the rule are logged by syslog to the source of the packet. If you have the ChoiceNet notifier installed, this keyword is used to cause a notification pop-up to appear on your computer.</p>
<i>=ListName</i>	<p>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.</p>

Examples

Command> **set filter w1.in 1 permit icmp**
Filter w1.in updated

See Also

add filter - page 15-4
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.

<code>srchost</code>	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.
<code>Ipxnode</code>	IPX node address, a 48-bit hexadecimal value—usually the MAC address of the host.
<code>srcsocket</code>	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.
<code>eq</code> , <code>lt</code> , or <code>gt</code>	Mode of comparison of socket numbers; equal (eq), less than (lt), or greater than (gt).
<code>Ipxsock</code>	A socket number specified for the comparison, an integer from 1 to 65535.
<code>dstnet</code>	Specifies the comparison with the destination IPX network number contained in the packet. A 32-bit hexadecimal number.
<code>dsthost</code>	Specifies the comparison with the destination IPX node address contained in the packet. A 32-bit hexadecimal number.
<code>dstsocket</code>	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 15-4

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 a SAP packet that matches the filter to pass through the interface. This is the default.
deny	Stops a 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.

Example

```
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 15-4

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.
<i>Filtername</i>	Name of a filter that is in the filter table.

Example

```
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 15-25

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 System (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**

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 16-1 are used to configure the host table.

Table 16-1 Host Table Commands

Command Syntax	
add host <i>Ipaddress String</i>	- see page 16-2
delete host <i>Ipaddress String</i>	- see page 16-2
save host	- see page 16-3
show table host	- see page 16-3



Note – The PortMaster always checks the local host table before using DNS or NIS.

Description of 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.



Caution – 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 will be deleted.

Examples

```
Command> delete host chopin  
Host entry successfully deleted
```

save host

This command writes the current host table to the nonvolatile RAM of the PortMaster.

save host

Usage

The command can also be entered as **save hosts**; **save all** can also be used.

Example

```
Command> save host  
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 the debug commands used for troubleshooting PortMaster configuration or operation.

Summary of Debug Commands

The debug commands in Table 17-1 are used for PortMaster debugging sessions.

Table 17-1 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 17-2
set debug ccp-stac on off	- see page 17-3
set debug choicenet on off	- see page 17-4
set debug clock on off	- see page 17-5
set debug Hex	- see page 17-5
set debug isdn isdn-dframes isdn DO isdn-l1 DO termination v120 on off	- see page 17-7
set debug mcppp-event on off	- see page 17-8
set debug mdp-status mdp-events mdp-max on off	- see page 17-9
set debug off	- see page 17-5
set debug ospf-hello ospf-event ospf-spfcalc ospf-lsu ospf-lsa ospf-dbdesc ospf-error ospf-routing ospf-max on off	- see page 17-10



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 <i>Hex</i> debug settings—currently active on the PortMaster.

Usage

The **set debug ccp-lzs** command displays the allocation of compression data structures, error messages, and reinitializations 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-lzs on
```

To stop the debugging output, enter the following:

```
Command> set debug off  
Command> reset console
```

set debug choicenet

This command sets debug flags used for troubleshooting ChoiceNet. Debug information is displayed to the console.

set debug choicenet **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 choicenet on
```

To stop the debugging output, enter the following:

```
Command> set debug off  
Command> reset console
```


set debug (Hex and Clock)

These commands sets 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.

Hex One of the following hex codes:

- **0x0** disables the output for a *Hex* 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 *Hex* 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 2-19
traceroute - page 2-43

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|v120 on|off

isdn	Set on to show ISDN debugging information on the console.
isdn-dframes	Set on to show ISDN frame debugging information on the console. To turn off debugging, re-enter the command.
isdn <i>D0</i>	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 <i>D0</i>	Set on to show layer 1 (l1) activation tracing on a BRI line designated by the value of <i>D0</i> . Layer 1 is the physical layer of the OSI model.
isdn-v120	Set on to display debugging of the V.120 protocol exchanges in V.120 connections.
termination	Set on to display detailed port termination information.
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 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-status|mdp-events mdp-max on|off

mdp-status	Set on to display the status of the digital modems.
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.
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 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
```

Command Index

A

- add bgp peer 12-5
- add bgp policy 12-4
- add bgp summarization 12-10
- add dlci (location) 14-29
- add dlci (synchronous port) 6-8
- add filter 15-4
- add host 16-2
- add ipdlci (location) 14-29
- add ipdlci (synchronous port) 6-8
- add ipxdlci (location) 14-29
- add ipxdlci (synchronous port) 6-8
- add ipxroute 10-14
- add location 14-3
- add modem 5-5
- add netmask 10-23
- add netuser 13-4
- add ospf area 11-4
- add propagation 10-3
- add route 10-15
- add snmpghost any 3-32
- add snmpghost none 3-32
- add snmpghost reader 3-32
- add snmpghost writer 3-32
- add subinterface 4-12
- add user 13-5
- attach S0 5-6

C

- clear alarm 3-33

D

- delete bgp peer 12-5
- delete bgp policy 12-4
- delete bgp summarization 12-10
- delete dlci (location) 14-31
- delete dlci (synchronous port) 6-8
- delete filter 15-4
- delete host 16-2
- delete ipdlci (location) 14-31
- delete ipdlci (synchronous port) 6-8
- delete ipxdlci (location) 14-31
- delete ipxdlci (synchronous port) 6-8
- delete ipxroute 10-16
- delete location 14-4
- delete modem 5-8
- delete netmask 10-24
- delete ospf area 11-5
- delete propagation 10-3
- delete route 10-17
- delete snmpghost reader 3-34
- delete snmpghost writer 3-34
- delete subinterface 4-13
- delete user 13-5
- 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) 11-5

P

ping 2-11
pmlogin 2-12
ptrace 2-13
ptrace extended 2-13

Q

quit 2-5

R

reboot 2-15
references ix
 books x
 RFCs ix
reset all 2-15
reset bgp 12-14
reset console 2-15
reset dialer 2-15
reset Handle 2-15
reset MO 9-4
reset nic 2-15
reset Number 2-16
reset ospf 11-6
reset p0 2-15

reset propagation 10-6
reset S0 2-15
reset V0 9-4
reset W1 2-15
rlogin 2-17

S

save all 2-18
save bgp 2-18, 12-15
save console 2-18
save Ether0 2-18
save filter 2-18, 15-5
save global 2-18
save host 2-18, 16-3
save location 2-18, 14-5
save netmask 2-18, 10-24
save ospf 2-18, 11-7
save P0 2-18
save ports 2-18
save route 2-18, 10-17
save S0 2-18
save snmp 2-18, 3-35
save user 2-18, 13-6
save W1 2-18
set accounting 3-25
set all access 5-9
set all cd 5-11
set all databits 5-14, 5-17
set all dialback_delay 5-17
set all directory 8-11
set all dn 8-11
set all dtr_idle 5-18
set all extended 5-19
set all group 5-20
set all hangup 5-21
set all host default 5-22

set all host Ipaddress 3-8, 5-22
 set all host prompt 5-22
 set all idletime 5-23
 set all ifilter 5-25
 set all login network dialin 5-27
 set all login network dialout 5-27
 set all login network twoway 5-27
 set all map 5-28
 set all message 5-30
 set all modem-type 5-31
 set all mtu 5-32
 set all network dialin 5-34
 set all network dialout 5-34
 set all network hardwired 5-35, 8-12
 set all network twoway 5-34
 set all ofilter 5-36
 set all override 5-37
 set all parity 5-38
 set all prompt 5-39
 set all rts/cts 5-41
 set all security 5-42
 set all service_device netdata 5-43
 set all service_device portmaster 5-43
 set all service_device rlogin 5-43
 set all service_device telnet 5-43
 set all service_login netdata 5-44
 set all service_login portmaster 5-44
 set all service_login rlogin 5-44
 set all service_login telnet 5-44
 set all speed 5-45
 set all spid 8-14
 set all stopbits 5-46
 set all termtype 5-47
 set all xon/xoff 5-50
 set alternate_auth_server 3-27
 set assigned_address 3-3
 set authentication_server 3-28
 set bgp as 12-15
 set bgp cluster-id 12-16
 set bgp cma 12-17
 set bgp connect-retry-interval 12-18
 set bgp disable 12-19
 set bgp enable 12-19
 set bgp hold-time 12-19
 set bgp id 12-20
 set bgp igp-lockstep 12-20
 set bgp keepalive-timer 12-21
 set bgp peer 12-5
 set bgp policy (acceptance) 12-22
 set bgp policy (advertisement) 12-34
 set bgp policy (injection) 12-29
 set bgp policy blank 12-42
 set bgp summarization 12-10
 set call-check 3-4
 set chap 3-5
 set choicenet 3-30
 set choicenet-secret 3-31
 set console 2-19
 set debug bgp-decision-process 17-2
 set debug bgp-errors 17-2
 set debug bgp-fsm 17-2
 set debug bgp-keepalives 17-2
 set debug bgp-max 17-2
 set debug bgp-notifications 17-2
 set debug bgp-opens 17-2
 set debug bgp-packets 17-2
 set debug bgp-updates 17-2
 set debug ccp-stac 17-3
 set debug choicenet 17-4
 set debug clock 17-5
 set debug Hex 17-5
 set debug isdn 17-7

set debug isdn D0 17-7
set debug isdn-dframes 17-7
set debug isdn-l1 D0 17-7
set debug isdn-v120 17-7
set debug mcppp-event 17-8
set debug mdp-events 17-9
set debug mdp-max 17-9
set debug mdp-status 17-9
set debug off 17-5
set debug ospf-dbdesc 17-10
set debug ospf-error 17-10
set debug ospf-event 17-10
set debug ospf-hello 17-10
set debug ospf-lsa 17-10
set debug ospf-lsu 17-10
set debug ospf-max 17-10
set debug ospf-routing 17-10
set debug ospf-spfcalc 17-10
set debug termination 17-7
set default broadcast 10-18
set default listen 10-18
set default off 10-18
set default on 10-18
set dhcp-server 3-6
set domain 3-7
set endpoint 9-5
set Ether0 address 4-3
set Ether0 broadcast 4-4
set Ether0 ifilter 4-5
set ether0 ip 4-6
set ether0 ipx 4-6
set Ether0 ipxframe 4-7
set Ether0 ipxnet 4-8
set Ether0 netmask 10-7
set Ether0 ofilter 4-9
set Ether0 ospf 11-8
set Ether0 ospf accept-rip 11-7
set Ether0 ospf cost 11-8
set Ether0 ospf dead-time 11-8
set Ether0 ospf hello-interval 11-8
set Ether0 rip broadcast 10-19
set Ether0 rip listen 10-19
set Ether0 rip on 10-19
set Ether0 route-filter 10-8
set filter (ICMP) 15-18
set filter (IP) 15-6, 15-7
set filter (IPX) 15-20
set filter (SAP) 15-23
set filter (TCP) 15-9, 15-10
set filter (UDP) 15-15
set gateway 10-12
set host 3-8
set ipx 3-9
set ipxfilter 15-20
set ipxgateway 3-10
set isdn-msn 8-4
set isdn-numberauto 8-5
set isdn-numberplan 8-6
set isdn-numbertype 8-7
set isdn-switch (BRI) 8-9
set isdn-switch (PRI) 9-6
set Line0 e1 9-10
set Line0 encoding 9-7
set Line0 fractional 9-10
set Line0 framing 9-8
set Line0 group 9-8
set Line0 group channels 9-9
set Line0 inband 9-10
set Line0 isdn 9-10
set Line0 isdn-fractional 9-10
set Line0 loopback 9-12
set Line0 pcm 9-12

set Line0 signaling 9-13
set Line0 signaling mfr2 9-14
set Line0 signaling r2gen 9-14
set Line0 t1 9-10
set line2 clock 9-15
set line2 encoding 9-7
set line2 fractional 9-3, 9-10
set line2 framing 9-8
set line2 group 9-8
set line2 group channels 9-9
set line2 loopback 9-12
set line2 t1 9-3, 9-10
set location analog 9-16, 14-5
set location automatic 14-6
set location chap 14-8
set location compression 14-9
set location destination 14-10
set location group 14-10
set location high_water 14-11
set location idletime 14-12
set location ifilter 14-13
set location ipxnet 14-14
set location local-ip-address 14-15
set location manual 14-6
set location map 14-15
set location maxports 14-16
set location mtu 14-17
set location multilink 14-18
set location netmask 14-19
set location ofilter 14-19
set location on_demand 14-6
set location ospf 11-9
set location ospf cost 11-9
set location ospf dead-time 11-9
set location ospf hello-interval 11-9
set location ospf nbma 11-9
set location ospf point-to-multipoint 11-9
set location ospf wan-as-stub-ptmp 11-9
set location password 14-20
set location protocol 14-21
set location rip broadcast 10-20
set location rip listen 10-20
set location rip on 10-20
set location route-filter 10-8
set location script 14-22
set location telephone 14-24
set location username 14-25
set location v25bis 14-22
set location voice 14-26
set loghost 3-11
set M0 9-16
set M0 lastcall 9-17
set maximum pmconsole 3-12
set nameserver 3-13
set namesvc 3-14
set netbios 3-15
set ospf area external 11-12
set ospf area md5 11-13
set ospf area nssa 11-14
set ospf area password 11-15
set ospf area range 11-16
set ospf area stub-default-cost 11-17
set ospf disable 11-18
set ospf enable 11-18
set ospf priority 11-19
set ospf router-id 11-20
set p0 device 7-2
set p0 disabled 7-2
set p0 disconnect 7-3
set p0 extended 7-4
set p0 host 7-4
set p0 service_device netdata 7-5

set p0 service_device portmaster 7-5
set p0 service_device rlogin 7-5
set p0 service_device telnet 7-5
set pap 3-16
set password 3-17
set pool 3-18
set pots 3-18
set reported_ip 3-19
set S0 access 5-9
set S0 address 5-10
set S0 autolog 5-49
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 9-18
set S0 dtr_idle 5-18
set S0 extended 5-19
set S0 group 5-20
set S0 hangup 5-21
set S0 host 5-22
set S0 host default 5-22
set S0 host prompt 5-22
set S0 idletime 5-23
set S0 ifilter 5-25
set S0 ipxnet 5-26
set S0 login 5-27
set S0 login network dialin 5-27
set S0 login network dialout 5-27
set S0 login network twoway 5-27
set S0 map 5-28
set S0 message 5-30
set S0 modem-type 5-31
set S0 mtu 5-32
set S0 netmask 5-33, 10-7
set S0 network dialin 5-34
set S0 network dialout 5-34
set S0 network hardwired 5-35
set S0 network twoway 5-34
set S0 ofilter 5-36
set S0 ospf 11-9
set S0 ospf cost 11-9
set S0 ospf dead-time 11-9
set S0 ospf hello-interval 11-9
set S0 ospf nbma 11-9
set S0 ospf point-to-multipoint 11-9
set S0 ospf wan-as-stub-ptmp 11-9
set S0 override 5-37
set S0 parity 5-38
set S0 prompt 5-39
set S0 protocol 5-40
set S0 rip broadcast 10-19
set S0 rip listen 10-19
set S0 rip on 10-19
set S0 route-filter 10-8
set S0 rts/cts 5-41
set S0 security 5-42
set S0 service_device netdata 5-43
set S0 service_device portmaster 5-43
set S0 service_device rlogin 5-43
set S0 service_device telnet 5-43
set S0 service_login netdata 5-44
set S0 service_login portmaster 5-44
set S0 service_login rlogin 5-44
set S0 service_login telnet 5-44
set S0 speed 5-45
set S0 stopbits 5-46

set S0 termtype 5-47	set user dialback 13-9
set S0 twoway 5-48	set user host 13-10
set S0 twoway network dialin 5-48	set user idle 13-11
set S0 twoway network dialout 5-48	set user ifilter 13-12
set S0 twoway network twoway 5-48	set user ipxnet 13-13
set S0 username 5-49	set user local-ip-address 13-14
set S0 xon/xoff 5-50	set user map 13-15
set S10 destination 8-10	set user maxports 13-16
set S10 directory 8-11	set user mtu 13-17
set S10 dn 8-11	set user netmask 13-18
set S10 network hardwired 8-12	set user-netmask 10-13
set S10 ospf 11-9	set user ofilter 13-19
set S10 ospf cost 11-9	set user ospf 11-9
set S10 ospf dead-time 11-9	set user ospf cost 11-9
set S10 ospf hello-interval 11-9	set user ospf dead-time 11-9
set S10 ospf nbma 11-9	set user ospf hello-interval 11-9
set S10 ospf point-to-multipoint 11-9	set user ospf nbma 11-9
set S10 ospf wan-as-stub-ptmp 11-9	set user ospf point-to-multipoint 11-9
set S10 speed 8-13	set user ospf wan-as-stub-ptmp 11-9
set S10 spid 8-14	set user password 13-20
set sapfilter 15-23	set user protocol 13-21
set secret 3-29	set user rip broadcast 10-21
set serial-admin 3-20	set user rip listen 10-21
set snmp 3-36	set user rip on 10-21
set snmp readcommunity 3-37	set user route-filter 10-8
set snmp writecommunity 3-37	set user service 13-22
set subinterface address 4-14	set user session-limit 13-23
set subinterface broadcast 4-15	set W1 address 6-3
set subinterface port-name 4-16	set W1 annex-d 6-4
set syslog 3-21	set W1 cd 6-5
set sysname 2-20	set W1 compression 6-6
set telnet 3-23	set W1 destination 6-7
set user address 13-6	set W1 dlci 6-8
set user callback 13-9	set W1 extended 6-10
set user compression 13-8	set W1 group 6-10
set user destination 13-6	set W1 hangup 6-11

set W1 idletime 6-12
set W1 ifilter 6-13
set W1 ipxnet 6-14
set W1 lmi 6-15
set W1 mtu 6-16
set W1 netmask 6-17, 10-7
set W1 network dialin 6-18
set W1 network dialout 6-18
set W1 network hardwired 6-18
set W1 network twoway 6-18
set W1 ofilter 6-19
set W1 ospf 11-9
set W1 ospf cost 11-9
set W1 ospf dead-time 11-9
set W1 ospf hello-interval 11-9
set W1 ospf nbma 11-9
set W1 ospf point-to-multipoint 11-9
set W1 ospf wan-as-stub-ptmp 11-9
set W1 protocol 6-20
set W1 rip broadcast 10-19
set W1 rip listen 10-19
set W1 rip on 10-19
set W1 route-filter 10-8
set W1 speed 6-21
show alarms 3-38
show all 2-21
show arp 2-23
show bgp memory 12-42
show bgp next-hop 12-43
show bgp paths 12-45
show bgp peers 12-48
show bgp peers packets 12-48
show bgp peers verbose 12-48
show bgp policy 12-54
show bgp summarization 12-55
show Ether0 4-10
show files 2-24
show filter 15-25
show global 2-27
show ipxfilter 15-25
show ipxroutes 10-25
show isdn 8-15
show isdn d0 8-15
show isdn S0 8-15
show Line0 9-19
show location 14-27
show M0 9-23
show mcppp 9-26
show memory 2-30
show modem 5-52
show modems 9-25
show modules 2-31
show netconns 2-32
show netstat 2-33
show ospf areas 11-21
show ospf links 11-24
show ospf neighbor 11-27
show pots 3-24
show propagation 10-26
show routes 10-28, 11-29, 12-57
show route to-dest 10-30
show S0 2-34
show sap 2-37
show sapfilter 15-25
show sessions 2-38
show syslog 2-39
show table 2-40
show table bgp 12-48
show table filter 2-40, 15-26
show table host 16-3
show table location 14-28
show table modem 5-53

show table netmask 10-31
show table ospf 11-21
show table snmp 3-39
show table subinterface 4-16
show table user 13-24
show user 13-25
show W1 6-22

T

telnet 2-41
tftp get 2-42
traceroute 2-43

V

version 2-44

Subject Index

A

- access filter 5-9, 5-25
- access override 5-9
- accounting server daemon 3-26
- accounting server, RADIUS 3-25
- adding
 - BGP peer 12-5
 - BGP policy 12-4
 - BGP summarization 12-10
 - DLCI to DLCI table 6-8, 14-29
 - filter to filter table 15-4
 - host to host table 16-2
 - IPX route 10-14
 - location to location table 14-3
 - modem to modem table 5-5
 - netmask to netmask table 10-23
 - netuser to user table 13-4
 - OSPF area 11-4
 - propagation 10-3
 - SNMP host 3-32
 - static route to IP route table 10-15
 - subinterface 4-12
 - user to user table 13-5
- administrative logins
 - disabling 3-20
 - enabling 3-20
 - using serial ports 3-20
- administrative password 1-4
- advertising network routes 11-16
- alarms 3-33, 3-38
- A-law encoding 9-12
- analog modems, enabling on PortMaster 3 9-16, 14-5
- analog port, enabling 3-18
- Annex-D polling interval 6-4
- area border router 11-4
- ARP tables for interface 2-23
- assigned base address 3-3
- assigned pool size 3-18
- asynchronous
 - access override 5-47
 - callback delay 5-17
 - carrier detect signal 5-11
 - configuring ports 5-1
 - data bits 5-10
 - device service 5-47
 - displaying port data 5-1
 - extended mode 5-15
 - hardware flow control 5-47
 - hardwired network 5-35
 - input filter 5-10
 - local IP address 5-10
 - login message 5-30
 - login prompt 5-39
 - login service 5-47
 - modem pools 5-20
 - modem selection 5-47
 - output filter 5-10
 - parity checking 5-46
 - port groups 5-20
 - RTS/CTS 5-47
 - stop bits 5-46
 - TCP/IP header compression 5-51
 - terminal type 5-47
 - transport protocol 5-10
- asynchronous port commands
 - description 5-5
 - summary 5-2
- asynchronous port types, description 5-4
- attached devices, to PortMaster 5-6
- authentication
 - CHAP 3-5

- PAP 3-16
- RADIUS 3-28
- RADIUS, alternate 3-27
- autonomous system
 - export summary information to 12-10
 - setting identifier 12-15

B

- backbone area 11-4
- backup router 11-19
- BACP 8-11, 9-19
- bandwidth on demand 8-11, 9-19
- BAP 8-11, 9-19
- Basic Rate Interface. See ISDN
- basic routing configuration 10-1
- baud rate 5-45, 8-13
- BBS 5-18
- BGP
 - adding peers to routing table 12-5
 - clearing a policy list 12-42
 - CMAS 12-10, 12-17
 - community 12-24, 12-31, 12-36, 12-56
 - community information 12-12
 - confederation member autonomous system.
 - See BGP, CMAS
 - confederation member, setting ID 12-17
 - connection retry interval 12-18
 - creating policy 12-4
 - defining an acceptance policy rule 12-22
 - defining an advertisement policy rule 12-34
 - defining an injection policy rule 12-29
 - degree of preference 12-22, 12-46
 - deleting a policy 12-4
 - displaying information 12-1
 - displaying memory usage 12-42
 - displaying next hop information 12-43
 - displaying path information 12-45
 - displaying peer information 12-48
 - displaying policy information 12-54
 - displaying route summaries 12-55
 - enabling or disabling 12-19
 - hold time 12-19

- keepalive timer 12-21
- local preference 12-34, 12-46
- lockstep feature 12-20
- multiexit discriminator 12-22, 12-34, 12-47
- multihome routing 12-7
- peer 12-5
- reducing numbers of advertised routes 12-28
- resetting 12-14
- route reflector setup 12-16
- route summarization 12-10, 12-13
- saving changes 12-15
- setting autonomous system identifier 12-15
- setting identifier 12-20
- BGP commands summary 12-2
- BGP community, setting identifier tag 12-24, 12-31, 12-36
- BGP policy
 - clearing 12-42
 - creating 12-4
 - defining acceptance rule 12-22
 - defining advertisement rule 12-34
 - defining injection rule 12-29
 - deleting 12-4
- bidirectional communications 5-18
- Border Gateway Protocol. See BGP
- BRI. See ISDN
- broadcast routing 10-19
- bulletin board service 5-18

C

- cable modem 3-6
- Cable Modem Telephone Return Interface
 - Specification 3-6
- callback delay 5-17
- callback login user
 - location 13-9
 - telephone number 13-9
- callback telephone number 13-9
- call-check 3-4
- carrier detect signal. See DCD
- Challenge Handshake Authentication Protocol.

- See CHAP
- channel rate 9-25
- channelized E1 9-14
- channelized T1 9-11, 9-13
- CHAP
 - authentication 2-20, 3-5
 - configuration 14-8
- ChoiceNet
 - authentication 3-30
 - client configuration 3-29
 - commands 3-29
 - debugging 17-4
 - secret 3-31
 - server 3-30
 - server configuration 3-30
 - shared secret 3-31
- clocking
 - E1 9-11
 - internal and external 9-15
 - T1 9-11
 - T1 card 9-15
- cluster ID for route reflector 12-16
- CMTRIS 3-6
- command line interface
 - introduction to 1-1
 - starting 1-4
- command line values, summary 1-7
- COMMAND status 2-22
- ComOS
 - displaying functional modules 2-31
 - erasing 2-6
 - version 2-44
- compression, Van Jacobson and Stac LZS 5-13, 6-6, 13-8, 14-9
- configuring a modem 5-6
- CONNECTING status 2-22
- cost setting
 - default, for OSPF stub area 11-17
 - Ethernet interface 11-8, 11-9

D

- data link connection identifier. See DLCI
- data over voice 3-19
- databits 5-14
- DCD 5-11, 6-5
- dead time, Ethernet interface 11-8, 11-10
- debug commands, summary 17-1
- debugging
 - adjacency formation between OSPF neighbors 17-10
 - ChoiceNet events 17-4
 - clearing all debug settings 17-2, 17-6
 - complete OSPF information 17-10
 - digital modems 17-9
 - from a terminal session 2-13
 - hexadecimal commands 17-5
 - I/O events 17-5
 - interactivity between ComOS and nonvolatile RAM 17-5
 - ISDN information 17-7
 - link state acknowledgment packets 17-10
 - link state update packets 17-10
 - LMI and Annex-D requests and acknowledgments 17-5
 - Multichassis PPP 17-8
 - OSPF database and routing table exchanges 17-10
 - OSPF errors in configuration 17-10
 - OSPF events 17-10
 - OSPF hello packets 17-10
 - RIP routing table updates 17-5
 - routing 10-30
 - Stac LZS messages 17-3
 - Telnet negotiation options 17-6
 - termination causes 17-5
 - updates to the ARP cache 17-6
- dedicated network connection 5-35, 8-13
- degree of preference, BGP
 - displaying 12-46
 - for acceptance 12-22
- deleting
 - BGP peer 12-5

- BGP policy 12-4
- BGP summarization 12-10
- DLCI from DLCI table 6-8, 14-31
- filter from filter table 15-4
- host from host table 16-2
- location from location table 14-4
- modem from modem table 5-8
- netmask from netmask table 10-24
- OSPF area 11-5
- propagation 10-3
- SNMP host 3-34
- static route from IP route table 10-17
- static route from IPX route table 10-16
- subinterface 4-13
- timestamping debug messages 17-5
- user from user table 13-5
- designated router 11-19
- device designation 5-16
- device service
 - netdata 5-43, 7-5
 - PortMaster 5-43, 7-5
 - rlogin 5-43, 7-5
 - Telnet 5-43, 7-5
- DHCP request forwarding 3-6
- dial group 5-20
- dial script 14-22
- dialback. See callback
- dial-in network 6-18
- dialing to a network location 2-4
- dial-out network 6-18
- digital encoding 9-12
- digital modems
 - ADMIN mode for hot swap 9-17
 - debugging 17-9
 - display status 2-31
- directory number 8-11, 9-5
- disabling security 5-42
- disconnecting a dial-in user 5-23
- DISCONNECTING status 2-22
- DLCI
 - adding to location 14-29
 - adding to synchronous port 6-8

- deleting 6-8, 14-31
 - feature 14-29
 - list 6-4, 6-10, 6-15
- DLCI table commands 14-28
- DNS 3-8, 3-14
- document conventions xii
- domain name 3-5
- Domain Name System. See DNS
- DOV 3-18
- DTR 5-18
- DTR idle 5-18
- DTR signal 5-18, 5-21
 - dropped 5-21
- Dynamic Host Configuration Protocol 3-6

E

- E & M wink start protocol 9-13
- E1 lines
 - encoding method 9-7
 - framing format 9-12
 - pulse code modulation 9-12
 - setting use 9-10
 - signaling for channelized E1 9-14
- endpoint discriminator, setting for Multichassis PPP 9-5
- erasing nonvolatile RAM 2-6
- ESTABLISHED status 2-22
- establishing login sessions 5-44
- Ethernet
 - 802.2 protocol 2-9, 4-7
 - 802.2_ii protocol 2-9, 4-7
 - 802.3 protocol 2-9, 4-7
 - configuration values 4-10
 - configuring for OSPF 11-8
 - enable IP protocol 4-6
 - enable IPX protocol 4-6
 - II protocol 2-9, 4-7
 - output filter 4-9
- Ethernet commands
 - description 4-3
 - subinterface commands 4-12

- summary 4-2
- Ethernet interface
 - configuring 4-1
 - displaying configuration 4-1
- Ethernet subinterface
 - adding 4-12
 - deleting 4-13
 - displaying configuration 4-12
 - IP address 4-14
 - port 4-16
- exiting the command line interface 2-5
- extended mode 5-19, 6-10
- external clocking 9-15
- external routes, propagating 11-12

F

- file statistics 4-11
- filter table
 - displaying data 2-40
 - saving changes 15-5
- filter table commands
 - description 15-4
 - summary 15-2
- filters
 - adding 15-4
 - configuring ICMP 15-18
 - configuring IP 15-6
 - configuring IPX 15-20
 - configuring SAP 15-23
 - configuring TCP 15-9
 - configuring UDP 15-15
 - deleting 15-4
 - displaying content 15-25
 - displaying data 15-1
 - emptying 15-6
 - for dial-in locations 5-25
 - for dial-out locations 5-25
 - for locations 14-13, 14-19
 - for routes 10-8
 - for users 13-12, 13-19
 - using in ptrace 2-13
- Flash RAM. See nonvolatile RAM

- foreign exchange station 9-13
- fractional E1
 - enabling 9-10
 - grouping channels 9-9
- fractional ISDN
 - enabling 9-10
 - grouping channels 9-9
- fractional T1
 - enabling 9-10
 - grouping channels 9-9
- Frame Relay 6-8, 6-20, 14-21, 14-29
 - subinterfaces 14-29
- FXS loop start protocol 9-13

G

- gateway address 10-3, 10-12
- general commands 2-1
 - summary 2-1
- global commands
 - summary 3-1
- global settings 2-27
 - displaying 3-1
- group number 5-20, 6-10, 14-11

H

- hardware flow control 5-41
- hardwired network 6-18
- hello interval for Ethernet interface 11-8, 11-10
- help commands 2-7
- high-water mark 14-11, 14-16
- host
 - alternate 3-8
 - default 3-8, 3-21, 5-22
 - device 5-20
 - device service 3-8, 5-22
 - for login sessions 3-8, 5-22
 - login 5-20
 - override parameters 5-47
 - prompt 5-22
- host table
 - adding host 16-2

- configuring 16-1
- deleting host 16-2
- displaying 16-1
- saving 16-3
- summary of commands 16-1
- hostname lookups 3-7
- HOSTNAME status 2-22
- hot-swappable modem 9-17
- hot-swappable T1 card 9-11

I

ICMP

- echo request packets 2-11
- time expired packets 2-43

ICMP filter, configuring 15-18

IDLE status 2-22

idle time

- asynchronous port 5-23
- location 14-12
- synchronous port 6-12
- user 13-11

ifconfig 2-9

IGP routes, using to advertise to an external BGP

- peer 12-20

imed 12-26

in.pmd daemon 5-16, 5-44, 7-2

inband signaling

- E & M wink start protocol 9-13
- FXS loop start protocol 9-13

INITIALIZING status 2-22

input filter

- asynchronous 5-10
- location 14-13
- synchronous 6-18
- user 13-12

internal clocking 9-15

Internet Control Message Protocol. See ICMP

Internet Network Information Center 12-15

InterNIC, supplier of autonomous system

- numbers 12-15

IP address

- assigned pool size 3-18
- asynchronous 5-10
- base 3-3
- ChoiceNet server 3-30
- default 5-22
- Ethernet 4-3
- gateway 10-12
- loghost 3-11
- network user 13-6
- pool 3-3
- RADIUS accounting server 3-25
- RADIUS authentication server 3-28
- remote router 5-15
- reported 3-19
- synchronous 6-3

IP broadcast address 4-4

IP filter, configuring 15-6

IP netmask

- asynchronous 5-33
- synchronous 6-19
- user 13-18

IPX

- frame type 4-7
- gateway 3-10
- NetBIOS 3-15

IPX filter, configuring 15-20

IPX network

- Ethernet 4-5
- location 14-14
- synchronous 6-14
- user 13-13

IPX route table

- adding routes 10-14
- deleting routes 10-16
- displaying 10-25

ISDN

- automatic number plan determination 8-5
- configuring BRI ports 8-1
- debugging 17-7
- description of BRI commands 8-4
- directory number for B channels 9-5
- displaying BRI port data 8-1

- displaying PRI port data 9-1
- displaying status of BRI ports 8-15
- encoding method for PRI line 9-7
- framing format for PRI line 9-12
- leased line 8-12
- number plan 8-6
- number type 8-7
- pulse code modulation for PRI line 9-12
- setting fractional lines 9-10
- setup of PRI line 9-10
- summary of BRI commands 8-1
- summary of PRI commands 9-2
- supported BRI switches 8-9
- supported PRI switches 9-6

L

leased line ISDN 8-12

lines

- analog to digital 9-12
- channels 9-9
- displaying 9-19
- encoding 9-7
- framing 9-8
- groups 9-8
- loopback 9-12
- setting 9-10
- setting E1 9-10
- setting fractional 9-10
- setting inband 9-10
- setting T1 9-10

listen routing 10-19

LMI polling interval 6-15

Local Management Interface 6-15

local preference, BGP

- displaying 12-46
- for advertisement 12-34

location

- automatic dial scripting 14-24
- CHAP configuration 14-8
- configuring 14-6
- destination address 14-10
- dial script 14-22

- displaying 14-27
- filters 14-13, 14-19
- force voice call 14-26
- high-water mark 14-11
- idle time 14-12
- input filter 14-13
- IPX network 14-14
- local IP address 14-14
- maximum dial-out ports 14-16
- MTU 14-17
- multilink 14-17
- netmask 14-19
- output filter 14-19
- password 14-20
- port groups 14-10
- protocol 14-21
- routing 10-20
- Stac LZS compression 14-9
- TCP/IP header compression 14-9
- telephone number for dial-out 14-24
- username 14-25

location password 14-20

location table

- adding locations 14-3
- configuring 14-1
- deleting locations 14-4
- displaying 14-1
- saving changes 14-5

location table commands summary 14-1

lockstep, matching advertised route to BGP peer
12-20

loghost address 3-11

login

- host 5-22
- message 5-30
- prompt 5-22, 5-30, 5-39, 13-10
- service 5-22

loopback, enabling on T1 or E1 lines 9-12

Lucent technical support, contacting xii

M

maximum transmission unit. See MTU

MCNS 3-6
MCPPP. See Multichassis PPP
MD5 authentication 11-13
MED. See multiexit discriminator, BGP
memory 2-30
memory usage for BGP 12-43
MFR2 signaling 9-14
modem card, replacing 9-17
modem initialization string 5-5
modem name
 long 5-5
 short 5-5, 5-52
modem switch 9-5
modem table
 adding modem 5-5
 configuration 5-51
 deleting modem 5-8
 displaying 5-53
modems, digital. See digital modems
modems, resetting 9-4
MSN 8-4
MTU
 location 14-17
 synchronous port 6-5
 user 13-17
Multichassis PPP
 debugging 17-8
 display of neighbors 9-26
 enabling on a PortMaster 3 9-5
 resetting a virtual port 9-4
multiexit discriminator, BGP
 displaying 12-47
 input for acceptance 12-22
 output for advertisement 12-34
Multifrequency R2 signaling 9-14
multihome routing 12-7
multiline load-balancing 13-17, 14-17, 14-18
Multilink PPP 13-16, 14-17
Multilink V.120 13-16
Multimedia Cable Network System 3-6
multiple subscriber network 8-4

N

name server 3-19
name service, selecting 3-19
negotiated address 13-7
netdata service 5-43, 5-44
netmask
 adding 10-23
 deleting 10-24
 hardwired asynchronous port 5-33
 hardwired synchronous port 6-19
 location 14-19
 network hardwired port 5-15
 saving configuration 10-24
 setting for specified interface 10-7
 subinterface 4-15
netmask table
 description of commands 10-22
 displaying 10-31
network
 connections 2-32
 hardwired asynchronous port 5-25, 5-36
 routes 2-34, 10-28, 11-29, 12-57
 statistics 2-32
network hardwired port
 MTU 5-28, 5-32
 netmask 5-33
Network Information Service. See NIS
network interface statistics, display 2-33
network service
 netdata 5-44
 PortMaster 5-44
 rlogin 5-44
 Telnet 5-44
network type
 dial-in 6-18
 dial-out 6-18
 hardwired 6-18
 two-way 6-18
NIS 3-8, 3-14
nonvolatile memory. See nonvolatile RAM
nonvolatile RAM
 debugging 17-5

- erasing 2-6
- NO-SERVICE status 2-23
- not-so-stubby area 11-14
- Novell NetWare
 - Version 3.11 2-9, 4-7
 - Version 4.0 2-9, 4-7
- NSSA 11-14

O

- omed 12-39
- online help 2-7
- Open Shortest Path First. See OSPF
- OSPF
 - adding area 11-4
 - advertising router 11-26
 - asynchronous interface 11-9
 - authentication key 11-21, 11-22
 - configuring 11-1
 - debugging 17-10
 - deleting area 11-5
 - displaying configured areas 11-21
 - displaying information 11-1
 - displaying neighbors 11-27
 - displaying summary of links 11-24
 - enabling or disabling 11-9, 11-18
 - Ethernet interface 11-8
 - examples of ifconfig output 11-5
 - external routes 11-23
 - link ID 11-26
 - MD5 authentication 11-13
 - NSSA 11-14
 - priorities of designated and backup routers 11-19
 - range and type of route propagation 11-16
 - RIP routing 11-7
 - route propagation 11-12, 11-16
 - router ID 11-20
 - saving changes 11-7
 - stub area 11-12
 - stub area default cost 11-17
 - stub area default route 11-17
 - synchronous interface 11-9

- transit area 11-12
- Type 1 external routes 11-14
- Type 2 external routes 11-7, 11-14
- OSPF area
 - adding 11-4
 - default route 11-12
 - deleting 11-5
 - network range 11-23
 - range 11-16
- OSPF commands
 - description of 11-4
 - summary 11-2
- OSPF Ethernet interface
 - cost 11-8, 11-9
 - dead time 11-8, 11-10
 - enabling 11-8
 - hello interval 11-8, 11-10
- output filter
 - asynchronous 5-10
 - Ethernet 4-9
 - location 14-19
 - synchronous 6-19
 - user 13-19

P

- PAP
 - authentication 3-16
 - configuration 3-16
- parallel port
 - configuration 7-1
 - device 7-5
 - device service 7-5
 - disabling 7-2
 - displaying configuration 7-1
 - extended mode 7-4
 - host 7-4
- parallel port commands
 - description 7-2
 - summary 7-1
- parity checking 5-38
- password
 - setting location 14-20

- setting user 13-20
- PASSWORD status 2-22
- peer, BGP 12-5
- permanent network connection 5-35, 8-12
- PHONE port
 - displaying 3-24
 - setting 3-18
- ping 2-11
- PMVision vii
- Point-to-Point Protocol. See PPP
- policy, creating for BGP 12-4
- port idle time 5-23
- port session information 2-38
- PortMaster
 - administrative password 1-4
 - debug commands 17-5
 - in.pmd daemon 5-16, 7-2
 - IP broadcast address 4-4
 - login service 2-12, 5-43, 5-44
 - rebooting 1-6
 - resetting ports 2-20
 - shared device 5-17
 - system console 2-19
 - uptime 2-44
- PortMaster 3
 - channel rate 9-25
 - digital modem status 9-6, 9-23, 9-25
 - displaying diagnostics 9-1
 - displaying line status 9-19
 - E1 inband signaling 9-14
 - enabling analog modem service 9-16, 14-5
 - enabling modems 9-5
 - enabling Multichassis PPP support 9-5
 - encoding method 9-7
 - framing format 9-12
 - line use 9-10
 - Multichassis PPP status 9-26
 - network loopback 9-12
 - pulse code modulation 9-12
 - switch type 9-6
 - T1 inband signaling 9-13
- PPP

- asynchronous control map 5-28, 13-15, 14-15
- connections 5-32
- negotiated address 13-7
- negotiation 3-19
- protocol 5-40, 6-20, 13-21, 14-21

PRI. See ISDN

Primary Rate Interface. See ISDN

printer port. See parallel port

propagating external routes 11-12

propagation rules, displaying 10-26

propagation, resetting 10-14

ptrace 2-13

Q

quitting the command line interface 2-5

R

RADIUS

- accounting server 3-25
- authenticating server, primary 3-28
- authenticating server, secondary 3-27
- client configuration 3-25
- filters 5-25
- port-limit attribute 13-17
- security 5-42
- shared secret 3-29

reboot 2-15

remote login 2-17

reported IP address 3-19

resetting modems 9-4

resetting OSPF interface 11-6

resetting ports 2-20

RIP routing 10-18

- enabling on specified interface 10-19

rlogin service 5-43, 5-44

route filter 10-8

- effects 10-9

route gateway 10-12

route propagation 11-12, 11-16

route reflector setup 12-16

route table

- adding routes 10-15
- deleting routes 10-17
- saving 10-15
- route, tracing 2-15, 10-30
- routing information, displaying 10-1
- routing options, default for RIP 10-18

S

- SAP
 - configuring filters 15-23
 - PortMaster information 2-37
- save command 2-20
- saving configurations 2-19
- script for dialing 14-22
- secret
 - ChoiceNet 3-31
 - RADIUS 3-29
- security level 5-42
- security, enabling 5-42
- Serial Line Internet Protocol. See SLIP
- Service Advertising Protocol. See SAP
- service profile identifier 8-14
- session time limit 13-23
- shared secret
 - ChoiceNet 3-31
 - RADIUS 3-29
- Simple Network Management Protocol. See SNMP
- SLIP
 - connections 5-32
 - notification 3-19
 - protocol 5-40, 6-20, 13-21, 14-21
- SNMP
 - alarms 3-33, 3-38
 - configuration 3-32
 - host, deleting 3-34
 - host, specifying 3-32
 - parameters, saving 3-35
 - read/write strings 3-37
 - support, enabling 3-36
- SNMP table, displaying 3-39

- software flow control 5-50
- SPID number 8-14
- Stac LZS compression 5-13, 6-6, 13-8, 14-9
 - debugging 17-3
- static routing commands 10-14
- status
 - COMMAND 2-22
 - CONNECTING 2-22
 - DISCONNECTING 2-22
 - ESTABLISHED 2-22
 - HOSTNAME 2-22
 - IDLE 2-22
 - INITIALIZING 2-22
 - NO-SERVICE 2-23
 - PASSWORD 2-22
 - USERNAME 2-22
- stop bits 5-46
- stub area
 - default route to 11-17
 - defining 11-12
- subinterface, Ethernet 4-12
- summarization 12-10
- switches
 - supported for ISDN BRI 8-9
 - supported for ISDN PRI 9-6
- synchronous
 - Annex-D polling interval 6-4
 - carrier detect signal 6-5
 - destination address 6-14
 - DLCI list 6-10
 - extended mode 6-5
 - hardwired network 8-12
 - input filter 6-18
 - IPX network 6-14
 - LMI polling interval 6-15
 - local IP address 6-3
 - modem pools 6-10
 - MTU 6-5
 - netmask 6-19
 - network type 6-18
 - output filter 6-19
 - port groups 6-10

- port idle time 6-12
- reference speed 6-21
- synchronous port commands
 - description 6-3
 - summary 6-2
- synchronous ports
 - configuring 6-1
 - displaying data 6-1
- syslog
 - displaying current settings 2-39
 - facilities and priorities 3-21
 - log types 3-21
 - setting loghost 3-11
 - settings for logged events 3-21
- system name parameter (sysname) 2-20

T

- T1 expansion card
 - encoding 9-7
 - framing 9-8
 - hot-swapping 9-11
 - setting fractional lines 9-10
- T1 lines
 - encoding method 9-7
 - framing format 9-12
 - pulse code modulation 9-12
 - setting use 9-10
- TCP filter, configuring 15-9
- TCP port services 15-11
- technical support, contacting xii
- Telnet
 - address 2-18
 - setting administrative port 3-18
- Telnet login service 5-43, 5-44
- terminal type 5-47
 - login 5-47
 - two-way 5-47
- testing a location configuration 2-4
- TFTP, retrieving file from host 2-42
- timeout value
 - asynchronous ports 5-23

- location 14-12
- parallel port 7-3
- synchronous 6-12
- user 13-11
- tracing a route 2-15
- transit area 11-12
- transport protocol 5-40
- Trivial File Transfer Protocol 2-42
- two-way network 6-18
 - connections 5-16, 5-34, 5-48
- two-way operation 5-48

U

- UDP filter, configuring 15-15
- UDP port services 15-11
- U-law encoding 9-12
- user
 - destination address 13-22
 - idle timeout 13-11
 - input filter 13-12
 - IPX network 13-13
 - local IP address 13-14
 - login host 13-10
 - login service 13-22
 - maximum dialout ports 13-16
 - MTU 13-17
 - netmask 13-18
 - network IP address 13-22
 - output filter 13-19
 - password 13-20
 - session time limit 13-23
 - Stac LZS compression 13-8
 - TCP/IP header compression 13-8
 - transport protocol 13-21
- user commands, summary 1-4
- user configuration 13-25
- user login mode 5-49
- user table 13-24
 - adding login users 13-5
 - adding network users 13-4
 - configuring 13-1

- deleting users 13-5
- displaying data 13-1
- saving changes 13-6
- setting user password 13-20
- user table commands summary 13-2
- USERNAME status 2-22
- users in user table 13-24

V

- V.90 support 9-13
- Van Jacobson TCP/IP header compression 5-13,
6-6, 13-8, 14-9
- variable-length subnet masks 10-13
- virtual port, resetting for Multichassis PPP 9-4
- VLSM 10-13

X

- X.75 protocol 5-40, 13-21, 14-21
