PortMaster® 4

Command Line Reference

Copyright and Trademarks

Disclaimer

Contents

About This Reference

The *PortMaster 4 Command Line Reference* provides ComOS® operating system commands for the PortMaster® 4 Integrated Access Concentrator from the Remote Access Business Unit of Lucent Technologies, Inc.

This command reference is one of three manuals that make up the comprehensive *PortMaster 4 User Manual*:

- *PortMaster 4 Installation Guide*

- *PortMaster 4 Configuration Guide*

- *PortMaster 4 Command Line Reference*

Consult the contents and indexes in each of these three manuals for detailed lists of topics and specific page references.

See the additional manuals listed under "PortMaster Documentation" for configuration, maintenance, and troubleshooting information common to all PortMaster products.

Audience

This reference is designed to be used by qualified system administrators and network managers. Knowledge of basic networking concepts is required.

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 Configuration Guide*

  This guide provides a comprehensive overview of networking and configuration for PortMaster products.

- PortMaster hardware installation guides

  These guides contain complete hardware installation instructions. An installation guide is shipped with each PortMaster.

- *PortMaster Routing Guide*

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

- *PortMaster Troubleshooting Guide*

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

- *RADIUS for UNIX Administrator's Guide*

  This guide provides complete installation and configuration instructions for Lucent RADIUS software for UNIX operating systems.

- *RADIUS for Windows NT Administrator's Guide*

  This guide provides complete installation and configuration instructions for Lucent RADIUS software for Microsoft Windows NT.

Additional References

RFCs

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

RFC 768, *User Datagram Protocol*
RFC 791, *Internet Protocol*
RFC 792, *Internet Control Message Protocol*
RFC 793, *Transmission Control Protocol*
RFC 854, *Telnet Protocol Specification*
RFC 950, *Internet Standard Subnetting Procedure*
RFC 1058, *Routing Information Protocol*
RFC 1112, *Host Extensions for IP Multicasting*
RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*
RFC 1157, *A Simple Network Management Protocol (SNMP)*
RFC 1166, *Internet Numbers*
RFC 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 1723, *RIP Version 2*
RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
RFC 1812, *Requirements for IP Version 4 Routers*
RFC 1814, *Unique Addresses are Good*
RFC 1818, *Best Current Practices*
RFC 1824, *Requirements for IP Version 4 Routers*
RFC 1825, *Security Architecture for the Internet Protocol*
RFC 1826, *IP Authentication Header*
RFC 1827, *IP Encapsulating Payload*
RFC 1828, *IP Authentication Using Keyed MD5*
RFC 1829, *The ESP DES-CBC Transform*
RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1878, *Variable Length Subnet Table for IPv4*
RFC 1918, *Address Allocation for Private Internets*
RFC 1962, *The PPP Compression Control Protocol (CCP)*
RFC 1965, *Autonomous System Confederations for BGP*
RFC 1966, *BGP Route Reflection, An Alternative to Full Mesh IBGP*
RFC 1974, *PPP Stac LZS Compression Protocol*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 1997, *BGP Communities Attribute*
RFC 2003, *IP Encapsulation within IP*
RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
RFC 2125, *The PPP Bandwidth Allocation Protocol (BAP), The PPP Bandwidth Allocation Control Protocol (BACP)*
RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*
RFC 2139, *RADIUS Accounting*
RFC 2153, *PPP Vendor Extensions*
RFC 2328, *OSPF Version 2*
RFC 2400, *Internet Official Protocol Standards*
RFC 2453, *RIP 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.	• Enter **version** to display the version number. • Press **Enter**. • Open the **permit_list** file.
Italic font	Identifies a command-line placeholder. Replace with a real name or value.	• **set** *Ether0* **address** *Ipaddress* • Replace *Area* with the name of the OSPF area.
Square brackets ([ ])	Enclose optional keywords and values in command syntax.	• **set nameserver** [**2**] *Ipaddress* • **set** *S0* **destination** *Ipaddress* [*Ipmask*]

Convention	Use	Examples
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	**set syslog** *Logtype* {[**disabled**] [*Facility.Priority*]}
Vertical bar (|)	Separates two or more possible options in command syntax.	· **set** *S0*|*W1* **ospf on**|**off** · **set** *S0* **host default**|**prompt**|*Ipaddress*

Document Advisories

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

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

Warning – means danger. You might do something—or fail to do something—that results in personal injury or equipment damage.
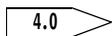
4.0   Means this command, keyword, or feature was introduced in the ComOS version shown.

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/tech/training/index.html**,s

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.

Introduction 1

You use the ComOS commands to configure, monitor, and debug the PortMaster 4 via the command line interface. The PortMaster 4 runs on ComOS releases 4.0 and later.

For more detailed information on how to use these commands, see the *PortMaster 4 Configuration Guide*, the *PortMaster Routing Guide*, and the *PortMaster Troubleshooting Guide*.

You can also configure the PortMaster 4 with the PMVision™ graphical user interface (GUI) for Microsoft Windows, UNIX, and other platforms supporting the Java Virtual Machine (JVM). Access PMVision online help for more information.

Note – You must use the command line interface to configure certain ComOS features.

Accessing the Command Line Interface

Refer to the *PortMaster 4 Installation Guide* for information on attaching to a console before attempting to configure your PortMaster with the command line interface.

To access the command line interface:

1. **Connect via Telnet to the PortMaster 4 or connect to a console port—C0 or C1—and log in as follows:**

   Login: **!root**

   Hit return twice to get to a **Command** prompt.

Note – If you are unable to log in to your PortMaster, refer to the *PortMaster 4 Installation Guide*.

2. **Configure your PortMaster with commands described in this reference.**

   For detailed configuration instructions, see the *PortMaster 4 Configuration Guide* and the *PortMaster Routing Guide* and *PortMaster Troubleshooting Guide*.

PortMaster 4 Management Commands 2

This chapter describes the commands you use to manage the PortMaster 4, to access the boards installed in the slots of the PortMaster 4 for configuration, and to display general information about boards and slots. The PortMaster 4 runs on ComOS releases 4.0 and later.

Note – After making any configuration changes to a PortMaster 4 slot, you must use the **reset slot***Slotnumber* command for the changes to take effect.

Table 2-1 lists commands for managing the PortMaster 4. Definitions of general administration commands and **show** commands follow the table. For debug commands and other **show** command definitions, see the pages indicated in the table.

Table 2-1   PortMaster 4 Management Commands

Command Syntax	
!!	- see page 2-4
copy *Subdirectory*/*Filename*(*source*) *Subdirectory*/*Filename*(*destination*)	- see page 2-4
dial *Locname* [**-x**]	- see page 2-6
done, quit, exit	- see page 2-7
erase all-flash	- see page 2-7
erase file *String*	- see page 2-7
help [*CommandName*]	- see page 2-8
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**]	- see page 2-9
ping [*Ipaddress*]	- see page 2-10
ptrace [*Filtername*|*Filtername* **extended**|**dump** *Bytes*]	- see page 2-11
reboot	- see page 2-13
reset all|*CO*|*SO*|*W1*|**console**|**dialer**|**nic**|**n***Handle*|**d***Number*| **ospf**|**bgp**|**slot***Slotnumber*	- see page 2-13
rlogin *Ipaddress*	- see page 2-15

Table 2-1   PortMaster 4 Management Commands *(Continued)*

Command Syntax	
save all|global|console|filter|host|location|netmask|ports|route|snmp|user|ospf|bgp	- see page 2-15
set console *C0*	- see page 2-16
set debug clock on|off	- see page 14-6
set debug *Hex*|**off**	- see page 14-6
set debug comport on|off *S0*	- see page 14-4
set debug flash on|off	- see page 14-5
set debug mdp-status|mdp-events|mdp-max on|off	- see page 14-9
set slot*Slotnumber* **on|off**	- see page 2-17
set sysname [*String*]	- see page 2-18
set view *Slotnumber*	- see page 2-18
show all	- see page 2-19
show arp *Interface*	- see page 2-21
show bgp memory	- see page 9-31
show bgp next-hop	- see page 9-32
show bgp paths [*Prefix*/*NM* [**verbose**]]	- see page 9-33
show bgp peers [**verbose**|**packets**]	- see page 9-36
show bgp policy [*Policyname*]	- see page 9-40
show bgp summarization [**all**]	- see page 9-41
show boards	- see page 2-21
show *Ether0*	- see page 4-12
show files [**verbose**]	- see page 2-23
show filter *Filtername*	- see page 12-18
show global	- see page 2-26
show ipxroutes	- see page 7-23
show isdn [**d***Number*|*S0*]	- see page 15-19
show *Line0*	- see page 15-20

Table 2-1   PortMaster 4 Management Commands *(Continued)*

Command Syntax	
show location *Locname*	- see page 11-21
show *M0*	- see page 15-23
show memory	- see page 2-30
show modems	- see page 15-23
show modem *ModemName(short)*	- see page 5-39
show modules	- see page 2-31
show netconns	- see page 2-32
show netstat	- see page 2-32
show ospf areas	- see page 8-15
show ospf links [**router**|**network**|**summary**|**external**|**nssa**]	- see page 8-18
show ospf neighbor	- see page 8-20
show propagation	- see page 7-24
show routes [*String*|*Prefix/NM*]	- see page 7-24, page 8-22, page 9-42
show route to-dest *Ipaddress*	- see page 7-26
show *S0*	- see page 2-34
show sap	- see page 2-36
show sessions	- see page 2-37
show slots	- see page 2-38
show syslog	- see page 2-41
show table filter|**host**|**location**|**modem**|**netmask**|**snmp**|**user**	- see page 2-41
show user *Username*	- see page 10-19
show *W1*	- see page 6-17
telnet *Ipaddress* [*Tport*]	- see page 2-42
tftp get [**comos**|**config**|**nostop**] *Ipaddress String*	- see page 2-43
traceroute [*Ipaddress*]	- see page 2-44
version	- see page 2-44

PortMaster 4 Management Commands

ComOS releases 4.0 and later support the following management commands for the PortMaster 4.

!!

This command repeats the previous command.

```
!!
```

Usage

You can also enter !! and a keyword such as when using the **help** command**.** See the examples on page 2-8.

See Also

`help` - page 2-8

copy

This command copies files from one directory to another in the nonvolatile file system.
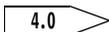
4.0 > `copy /Subdirectory/Filename(source) /Subdirectory/Filename(destination)`

`Subdirectory`	Path to the file.
`Filename(source)`	Name of the file to be copied. Filenames and directories cannot exceed 16 characters.
`Filename(destination)`	Name to give the copied file. Filenames and directories cannot exceed 16 characters.

Usage

The manager board's nonvolatile RAM file system has a shared directory and directories for each board in the PortMaster 4.

Use the **copy** command to copy files between the subdirectories in the PortMaster 4 or to copy files in the same directory. To verify that you have successfully copied files, use the **show files** command before and after using the **copy** command.

Note – Entire subdirectories cannot be copied.

Example

This example copies the SNMP file from the directory of the manager board to the shared directory. The copied file is highlighted in this example.

```
Command> show files
File Name     Length
----------------------------
ComOS-pm4     525602
/manager
confdata      2812
snmp          65
/shared
global        324
lan           293908
m2c_1.2a      73214
m2d_1.2a      131072
quadt1        327452
/slot10
confdata      124
              -------------
Total         1373437

Command> copy /manager/snmp /shared/snmp2
Command> show files
File Name               Length
----------------------------
ComOS-pm4               525602
/manager
confdata                2812
snmp                    65
/shared
global                  324
lan                     293908
m2c_1.2a                73214
m2d_1.2a                131072
quadt1                  327452
snmp2                   65
/slot10
confdata                124
                        -------------
Total                   1373437
```

See Also

show files - page 2-23

dial

This command initiates dialing to a network location.

> **dial** *Locname* [**-x**]

Locname	Name of location to dial.
-x	Displays send and expect strings during dialing. Also resets some debugging values previously set with **set debug**.

Usage

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

Example

```
Command> set console

Command> dial loc1 -x
Starting dial to location loc1 using S1
send them (atdt5551212\r)
expect    (CONNECT)
atdt5551212\r\r\nCONNECTgot it
send them (\r)
expect    (Login:)
 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 2-13
set console - page 2-16
set debug - page 14-6

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 4.

> **erase all-flash|file** *String*

all-flash	Erases all the nonvolatile RAM in the PortMaster 4, including ComOS.
file	Erases a specified file from nonvolatile RAM.
String	The name of the file to be erased; see **show files** on page 2-23 for filenames.

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.

help

These commands provide online help for the PortMaster 4 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 releases 3.8 and later support context-sensitive help. Entering a question mark (?) at any point in the command line and pressing **Return** generates a list of keywords or values that can be entered at that point.

Examples

```
Command> 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
ipxroute - Add an IPX route to the static routing table
route - Add a route to the static routing table
location - Add a new Dialnet dial-out location
snmphost - Add a host to the SNMP access list
netuser - Add a SLIP or PPP user to the password table
user - Add a login user to the password table
```

```
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
```

ifconfig

This command displays configuration values for all interfaces.

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

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

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

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

Usage

The **ifconfig** command allows you to view the active configuration of all network interfaces. You cannot use **ifconfig** to make configuration changes on ComOS 4.0 and ComOS 4.1.

Note – The PortMaster 4 supports IPX protocols on ComOS releases 4.1 and later.

Examples

```
Command> ifconfig
ether0: flags=16<IP_UP,IPX_DOWN,BROADCAST,OSPF>
inet 172.16.110.68 netmask ffffff0 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 ffffff00 broadcast 192.168.55.255 mtu 1500
```

See Also

ifconfig - page 8-4
ping - page 2-10
traceroute - page 2-44

ping

This command sends Internet Control Message Protocol (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. Because it 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), **ping** also displays the IP address of a host name. On a PortMaster 4, the output also displays the elapsed time for the ICMP reply.

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

Example

```
Command 1> ping www.lucent.com
www.lucent.com (172.16.200.3) is alive - round trip=15 ms
```

See Also

ptrace - page 2-11
set reported_ip - page 3-21
traceroute - page 2-44

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*|*Filtername* **extended**|**dump** *Bytes*]

Filtername	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 hexadecimal dump of the contents of an Ethernet frame for any packet specified.
Bytes	Number of bytes in the hex dump—between 0 and 1514.

Usage

For more information about filters, see "Filter Commands" on page 12-3.

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>
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 12-3
set console - page 2-16
set filter - page 12-5 to page 12-12
show filter - page 12-18
show table filter - page 12-18

reboot

This command restarts the software using the currently saved configuration.

> **reboot**

Usage

You must reboot the system manager card for a changed IP address, IPX address, or ISDN switch type to take effect, or for an upgrade loaded earlier into nonvolatile RAM to be used.

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

reset

This command shuts down and immediately restarts a physical or virtual port or all ports on the PortMaster 4.

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

> **reset all**|*C0*|*S0*|*W1*|**console**|**dialer**|**nic**|**n**Handle|**d**Number|**propagation** |**ospf**|**bgp**|**slot**Slotnumber

all	Resets all ports.
C0	Any asynchronous port. 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.
S0	Any ISDN primary rate interface.
W1	Any synchronous WAN 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.
nHandle	Network identifier. Enter this value as **n** immediately followed (no space) by a number from the first column of the **show netconns** output. See page 2-32 for an example display.

d*Number*	ISDN channel.
ospf	See page 8-5.
bgp	See page 9-8.
slot*Slotnumber*	Resets a board in a specified slot—physical or virtual. Table 2-2 lists the slots in the PortMaster 4. No output is generated from this command.
	Slotnumber is an integer between 0 and 16.
propagation	See page 7-5.

Usage

Table 2-2   PortMaster 4 Slot Numbers

Slot Number	Use
0 through **9**	Physical slot numbers. Identifies the board or module installed in the slot.
4	Physical slot number. Identifies a manager module, which consists of a manager board and an Ethernet board.
10 through **16**	Virtual slot numbers assigned to Ethernet boards or other accessory boards. Slot 10 is reserved for Ether1. For example, although Ether1 is physically in slot 4, the PortMaster assigns it a virtual slot number so it can be monitored separately from the manager card in slot 4. Similarly, although you can configure Ether1 from the manager view (slot 4), you must use **reset slot10** to activate Ether1 settings.

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

Command-1> reset slot1
Command-1>
```

See Also

save console - page 2-15
set console - page 2-16
set view - page 2-18

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

telnet - page 2-42

save

This command saves configuration information to the nonvolatile memory of the PortMaster 4, regardless of what view is set.

Note – You must use the command **save ports** to save changes made to any port.

**save all|global|console|filter|host|location|netmask|
ports|route|snmp|user|ospf|bgp**

all	All configuration changes.	
global	Global configuration changes.	See Chapter 3.
console	Console port setting.	See page 2-16.
filter	Filter configuration changes.	See Chapter 12.
host	Host table settings.	See Chapter 13.
location	Location table settings.	See Chapter 11.
netmask	Netmask table settings.	See Chapter 7.
ports	All ports.	

route	Static route table settings.	See Chapter 7.
snmp	SNMP table settings.	See Chapter 3.
user	User table settings.	See Chapter 10.
ospf	OSPF configuration.	See Chapter 8.
bgp	BGP configuration.	See Chapter 9.

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. To save changes made to any port, use the **save ports** command.

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 14-6
show files - page 2-23

set console

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

> **set console** *C0*

C0   Console port.

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 2-13
save console - page 2-15
set debug - page 14-6

set slot

This command turns the power on or off for a specific slot.

`4.0` ▷ **set slot***Slotnumber* **on|off**

Slotnumber	Integer between 0 and 9 that identifies a physical slot in the PortMaster 4 chassis. Leave no space between the keyword **slot** and the slot number. See Table 2-2 on page 2-14 for slot number values.
on	Turns on the board or module in the specified slot.
off	Turns off the board or module in the specified slot, except slot number 4, the manager module.

Note – To turn off a board or module, you must first **save all.**

Usage

Entering **save all** after setting a slot on or off sets the autostart configuration for that slot.

Note – After turning a module off, wait 3 seconds before turning it back on.

Examples

1. The following example turns off the slot or module in slot 3 but does not affect the autostart configuration:

    Command> **set slot3 off**
    slot3 disabled

2. The following example turns off the module in slot 3 and sets the autostart configuration so that the module is not turned on the next time the PortMaster 4 is restarted:

    Command> **set slot3 off**
    slot3 disabled

    Command> **save all**

set sysname

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

> **set sysname** [*String*]

String   Name of up to 16 characters. No default.

Usage

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

Example

```
Command> set sysname pm4
System Name Successfully changed
```

See Also

set chap - page 3-7
set snmp - page 3-34

set view

This command provides configuration access to the specified slot and displays its status.

> ⬗ 4.0 ⬗   **set view** *Slotnumber*

Slotnumber   Integer between 0 and 16 that identifies a physical or virtual slot in the PortMaster 4. See Table 2-2 on page 2-14 for slot number values.

Usage

Setting the view to a slot allows you to configure or display the status of a board or module in the slot. Entering **set console** after setting this view displays console messages for this board only. The view number appears in the command prompt.

Setting the view to slot 4, the slot containing the manager module, allows you to configure and display the status individual boards installed in the PortMaster 4. Similarly, entering **set console** from the manager view displays console messages for all boards. No view number appears in the prompt for the manager view, which is the default view.

Setting the view to a virtual slot lets you configure the board assigned to that slot—the Ethernet board in the manager module is assigned to slot 10, for example. However, you can also configure the Ethernet boards from any view.

Note – The **save all** command saves the configuration for the entire chassis regardless of what view is set.

Example

```
Command 2> set view 5
View changed from 2 to 5
Command 5>
```

show all

This command shows a summary status of all ports on the PortMaster 4, or of all ports on a particular board or module if the view is set to its slot.

> **show all**

Example

The following example is from the manager module of a PortMaster 4. In this example, only two slots are active, slot 0 and slot 1.

If your view is set to a board or module other than the manager module, the output displays port information only for the selected line board.

```
Command> show all
C0     9600     off                 Login     COMMAND       356        29969      0
C1     115200   off                 Login     USERNAME      0          1321       0
*************Slot 0*****************
Port   Speed    Mdm    Host     Type       Status        Input      Output     Pend
----   -----    ----   -------- --------   -----------   -------    --------   ----
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
.
.
.
S96    9600     OFF             Login/     NO-SERVICE    0          0          0
*************Slot 1*****************
Port   Speed    Mdm    Host     Type       Status        Input      Output     Pend
----   -----    ----   -------- --------   -----------   -------    --------   ----
S0     9600     OFF             Login/     NO-SERVICE    0          0          0
```

```
S1     9600    OFF              Login/    NO-SERVICE    0        0        0
S2     9600    OFF              Login/    NO-SERVICE    0        0        0
S3     9600    OFF              Login/    NO-SERVICE    0        0        0
S4     9600    OFF              Login/    NO-SERVICE    0        0        0
.
.
.
S96    9600    OFF              Login/    NO-SERVICE    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	Login or device host for the port.
Type	Type of operation for which port is configured.
Status	Current port state. See Table 2-3 on page 2-20 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 2-3   Port Status Messages

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

show arp

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

> **show arp** *Interface*

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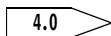
For Frame Relay, the output shows the mapping from IP address to data link connection identifier (DLCI), and includes the Q.922 value for the DLCI.

See Also

ifconfig - page 2-9

show boards

This command displays general information about the boards installed in the PortMaster 4.

4.0 >   **show boards**

Usage

Use the **show boards** command to display the status of all boards in the PortMaster 4. The PortMaster 4 stores configuration files for a board in a subdirectory named after the slot number the board occupies. If you move a board from one slot to another, and turn on the board, the board uses the configuration stored for the new slot, allowing you to replace a failed board without re-entering configuration information.

The output of this command is the same from any view.

Example

Command> **show boards**

```
ID    Type              Directory    Uptime   Boot   Hello   State    OS
02    Quad T1           slot2        16:21    1      10      Active   4.0
04    System Manager    Manager      1days    1      0       Active   4.0
10    Ethernet          slot10       1days    1      30      Active   4.0
```

Explanation

ID
Board identification number—matches the slot number that the board occupies, except for the Ethernet board and other accessory boards, which are assigned a virtual slot number.

Type
Type of board in each slot:

Quad T1
Contains four T1 line ports and 98 modems, or four T1 line ports only. The T1 line ports can be configured for PRI, channelized T1, fractional T1, fractional ISDN, or T1. See "ISDN PRI, T1, and E1 Commands" on page 15-3.

Tri E1
Contains three E1 line ports and 98 modems or three E1 line ports only. The E1 line ports can be configured for PRI, channelized E1, fractional E1, fractional ISDN, or E1. See "ISDN PRI, T1, and E1 Commands" on page 15-3

System Manager
Contains a 10Mbps Ethernet connection and two asynchronous ports.

Ethernet
One of the following Ethernet connections:

- The 10/100Mbps Ethernet connection with a media-independent interface (MII) connection in virtual slot 10 that is physically in slot 4.

- Single standalone Ethernet board with one 10/100Mbps Ethernet connection and one MII connection

- Dual standalone Ethernet module with two 10/100Mbps Ethernet connections and two MII connections.

T3 Mux board
Board that demultiplexes T3 bandwidth into 28 DS-1 channels and terminates them on T1 lines.

Directory
Subdirectory reserved for the board.

Uptime
Elapsed time, in seconds, since the last startup.

Boot
Number of times the board has been started.

Hello	Elapsed time, in seconds, since a hello packet was received from the board. The boards in the PortMaster 4 send hello packets every 30 seconds, so any number greater than 30 indicates a problem.
State	One of the following board states:

	Present	The board has been detected but not identified by the system manager.
	Active	The board is present and operational.
	Config	The board is not active.
	Empty	No board is present.

OS	Version of ComOS that the board is running. Each board has its own ComOS that can be viewed via the **show files** command.

show files

This command shows the files in the nonvolatile directories of the manager board and optionally performs a check on them.

> **show files** [**verbose**]

files	Shows the files in the nonvolatile directories of the manager board and the length of each file in bytes.
verbose	Performs a file system check on the nonvolatile directories of the manager board to ensure that they are not corrupt and that if problems are detected, they are automatically fixed.

`4.0`

Usage

The PortMaster 4 stores configuration files for a board in a subdirectory named after the slot number the board occupies. If you move a board from one slot to another, and turn on the board, the board uses the configuration stored for the new slot, allowing you to replace a failed board without re-entering configuration information.

The PortMaster 4 performs a check on the nonvolatile directories of the system manager whenever the **show files verbose** command is used or when the PortMaster 4 is started. The output of this command is displayed to the command line interface. The results of the check at startup is sent to the console.

Filenames and directories cannot exceed 16 characters. The number of files and subdirectories in directories is limited by the size of nonvolatile RAM.

Examples

```
Command> show files
File Name        Length
---------------  -------
ComOS-pm4        531650
/manager
bgp_peer         168
confdata         2860
ospfarea         176
snmp             24
/shared
filters          54
global           337
ipxfilt          26
lan              485476
m2c_1.2a         73214
m2d_1.2a         131072
quadt1           323379
sapfilt          26
/slot10
confdata         72
lan3             435460
/slot3
confdata         10064
                 -------
Total            1994158
```

Explanation

ComOS-pm4	Manager module binary file.
/manager	Indicates that the files immediately following are subdirectories of **manager**.
bgp_peer	BGP configuration information.
confdata	Configuration binary file.
ospfarea	OSPF binary file.
snmp	SNMP binary file.
/shared	Indicates that the files immediately following are subdirectories of **shared**.
filters	Filter binary file.
lan	Ether1—10/100 Ethernet—binary file.
m2c_1.2a	Modem binary file.

m2d_1.2a	Modem binary file.
quadt1	Quad T1 binary file.
sapfilt	SAP filter.
/slot10	Indicates that the files immediately following are subdirectories of Ether1.
confdata	Configuration information.
lan3	Ethernet information.
/slot3	Indicates that the files immediately following are subdirectories of the board or module in slot 3.
confdata	Slot 3 board configuration binary file.

```
Command> show files verbose
Flash type Am29F016 with 8192K of memory in 128 cells and 8064 nodes
     2 directory nodes in 2 cells
     6710 empty nodes in 107 cells
     5 released nodes in 2 cells
     1347 data nodes 0 unreferenced nodes 0 missing nodes
      0 cells being erased 0 bad cells

File Name          Length
------------------ -------
     ComOS-pm4     525602
/manager
     confdata      2812
     snmp          65
/shared
     global        324
     lan           293908
     m2c_1.2a      73214
     m2d_1.2a      131072
     quadt1        327452
/slot10
     confdata      124
/slot3
     confdata      18864
                   -------
Total              1373437
```

Explanation

Cell   The nonvolatile memory of the manager board is divided into 64KB cells. Each cell holds 63 nodes.

Node   Each node is 1036 bytes in length and consists of a block and its header. In the PortMaster 4, data is contained in 1KB blocks. Each block contains a 12-byte header.

A node is one of the following types:

Directory node	Node containing information about the file system, such as directory names, filenames, file lengths, and directory structures.
Empty node	Node that is ready to accept data.
Released node	Node containing data that is no longer being used. A released node cannot become an empty node until all the other nodes in the cell are also released.
Data node	Node containing data belonging to a file.
Unreferenced node	Node containing data for a file that does not exist, indicating that the nonvolatile file system has been corrupted.
Missing node	The sum of all the counters—directory nodes, empty nodes, data nodes, unreferenced nodes, and released nodes—must equal the total number of nodes. If these values do not match, the difference is noted as missing nodes. The presence of missing nodes indicates a problem.

Bad cell   Cell with a header containing unexpected or incorrect information.

show global

This command shows system-wide configuration values.

> **show global**

Examples

1. The following example shows output from the default (manager) view of a PortMaster 4 running ComOS 4.0:

```
Command> show global
        System Name:  pm4
       Default Host:  0.0.0.0
    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 (default)
            BGP ID[AS]:  0.0.0.0 [0]
            BGP timers:  Connect 120 Keepalive 30 Hold 90
     BGP IGP Lockstep:   off
          Name Service:  DNS
           Name Server:  server.lucent.com
                Domain:  lucent.com
    Telnet Access Port:  23
               Loghost:  0.0.0.0
     Maximum PMconsole:  10
         RADIUS Server:  server.lucent.com
      Alternate Server:  0.0.0.0
     Accounting Server:  server.lucent.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: off
      ISDN Switch Type:  DMS-100
              ISDN MSN:  off
       Disabled Modules: SNMP
```

2. The following example shows output when the view is set to slot 1 on a PortMaster 4 running ComOS 4.0:

```
Command 1> show global
           System Name:  pm4
          Default Host:  0.0.0.0
       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 (default)
            BGP ID[AS]:  0.0.0.0 [0]
            BGP timers:  Connect 120 Keepalive 30 Hold 90
     BGP IGP Lockstep:   off
          Name Service:  DNS
           Name Server:  server.lucent.com
                Domain:  lucent.com
    Telnet Access Port:  23
               Loghost:  0.0.0.0
     Maximum PMconsole:  10
         RADIUS Server:  server.lucent.com
      Alternate Server:  0.0.0.0
     Accounting Server:  server.lucent.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: off
       ISDN Switch Type:  DMS-100
               ISDN MSN:  off
        Disabled Modules:  SNMP
       Slot 1 Parameters:
       Assigned Address:  0.0.0.0
       ISDN Switch Type:  dms-100
```

3. The following example shows output from the default (manager) view of a
    PortMaster 4 running ComOS 4.1.

```
  Command> show global
             System Name:  pm4
            Default Host:  0.0.0.0
         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 (default)
             BGP ID[AS]:  0.0.0.0 [0]
             BGP timers:  Connect 120 Keepalive 30 Hold 90
       BGP IGP Lockstep:  off
           Name Service:  DNS
            Name Server:  server.lucent.com
                 Domain:  lucent.com
      Telnet Access Port:  23
                 Loghost:  0.0.0.0
      Maximum PMconsole:  10
           Shutdown Temp:  60C/140F
            Chassis type:  MSM_RAC
           RADIUS Server:  192.168.96.8 1645
         Alternate Server:  192.168.96.7 1645
     Tertiary Auth Server:  0.0.0.0
       Accounting Server:  192.168.96.8 1645
       Alt. Acct. Server:  192.168.96.7 1645
     Tertiary Acct. Server:  0.0.0.0
         ChoiceNet Server:  192.168.96.9
         Alt. ChNet Server:  0.0.0.0
      PPP Authentication:  PAP: on      CHAP: off
         Disabled Modules:  SNMP
```

Explanation

File	Contents	
System Name	SNMP system name.	See page 2-18.
Default Host	Host used for login services.	See page 5-15.
Alternate Hosts	Alternate host.	See page 5-15.
IP Gateway	Default route gateway address.	See page 7-11.
Gateway Metric	Metric for the default route.	See page 7-11.
Default Routing	Default routing options for all interfaces.	See page 7-16.
OSPF Priority	OSPF priority assigned to the router.	See page 8-14.
OSPF Router ID	OSPF router address or ID number.	See page 8-15.
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 9-12 and page 9-9.
BGP timers	Configured BGP timed events.	See page 9-10 and page 9-11.
BGP IGP Lockstep	Status of the BGP Interior Gateway Protocol (IGP) lockstep setting.	See page 9-12.
Name Service	Service—Network Information Service (NIS) or Domain Name System (DNS)—used for resolving hostnames.	See page 3-18.
Name Server	Name server IP address or hostname.	See page 3-17.
Domain	Domain name used with hostname lookups.	See page 3-9.
Telnet Access Port	Administrative Telnet port.	See page 3-25.
Loghost	Host to which **syslog** messages are sent.	See page 3-16.
Maximum PMconsole	Maximum number of concurrent connections for management applications permitted into the PortMaster.	See page 3-17.
Shutdown Temp	Maximum internal temperature set for the PortMaster 4.	See page 3-22.
Chassis Type	Type of chassis.	See page 3-7.
Assigned Address	Base address in the assigned address pool.	See page 3-5.
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 3-28.
Tertiary Auth Server	Third RADIUS authentication server.	See page 3-28.
Accounting Server	RADIUS accounting server.	See page 3-27.
Alt. Acct. Server	Alternate RADIUS accounting server.	See page 3-27.
Tertiary Acct. Server	Third RADIUS accounting server.	See page 3-27.
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 3-19.
ISDN Switch Type	ISDN switch type.	See page 15-5.
ISDN MSN	ISDN multiple subscriber network.	
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
System blocks 460 - 49 used, 411 available
```

Explanation

System memory *nnnnnn* bytes	Total memory installed in the system.
nnnnnn used	Highest amount of system memory ever used by the system.
nnnnnn available	Memory remaining in the free large heap. If this value is greater than zero, the system has never run out of memory.
64:1, 96:1, 1152:1, and so on	Memory fragments, *Size:Number*: • *Size*—size in bytes (for example, 64). • *Number*—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 blocks   Memory block usage.

show modules

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

show modules

Example

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

Explanation

Module   The functional module.

State   Module state:

• **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.lucent.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 the receive queue.
Send-Q	Number of packets in the 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 *UDP* for UDP sockets.

See Also

reset r*Handle* - page 2-13

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 the last reboot.
Ierrs	Number of input errors counted since the last reboot. All input errors cause the error counter to increase. Examples of input error sources are as follows:

- PPP frame header errors.
- Frame too large or too small.
- Frame alignment errors.
- CRC errors.

Opkts	Number of valid packets sent since the last reboot.
Oerrs	Number of output errors counted since the last reboot. All output errors cause the error counter to increase. Examples of output error sources are as follows:

- Transmission prevented because of excess collisions.
- Out-of-window collision—collision occurring outside a normal time slot.

Collis	Number of collisions since the last reboot.
Resets	Number of times the interface was reset since reboot, due to any of the following:

- 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 a buffer to be sent from the interface.

show *C0|S0*

This command shows the current status and configuration of asynchronous console ports and synchronous ISDN Primary Rate Interface (PRI) ports on the PortMaster.

> **show** *C0|S0*

C0	C0 or C1—asynchronous console port.
S0	Synchronous ISDN PRI.

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 2-3 on page 2-20.
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	Number of abnormal termination errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—**framing errors/device errors**:
	Framing errors—This count increments when the receiver chip reports either a framing error or an abnormal termination.
	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.
CRC Errors	Number of cyclic redundancy check (CRC) errors occurring since last reboot.
Overrun Errors	Number of overrun errors occurring since last reboot.
Frame Errors	Number of frame errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—**short frame errors/large frame errors**:
	Short frame errors—This count increments when a short frame is received.
	Large frame errors—This count increments when a packet is too large and must be dropped.
Modem Status	Status of external modems.
	The plus signs (+) on *DCD* and *CTS* indicate that the DCD and CTS signals on the port are asserted (high).
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 5-29.
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 or hosts defined for the specified port.

Terminal Type	The terminal type selected.
Login Prompt	The user login prompt.
Idle Timeout	The idle time in minutes before a port is reset.

See Also

show W1 - page 6-17

show sap

Shows the active Service Advertising Protocol (SAP) table.

> **show sap**

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Example

```
Command> show sap
Server                          Svc   Network     Host            Sock    Hops    Interface
----------------------------    ---   ---------   --------------  ---     -----   ---------
080009A8CEAA80CGNPIA8CEA        30C   COA86000:   080009A8CEAA:   400C    2       ether0
NOVELL                          4     00001701:   000000000001:   0451    2       ether0
```

Explanation

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

show sessions

This command shows current use of ports on a selected board.

> **show sessions**

Usage

To display information about the ports of a specific board or module in a PortMaster 4, you must first use the command **set view**. By default, the view is set to slot 4—the manager module.

Example

The following example shows output from the default (manager) view of a PortMaster 4 with two active slots:

```
Command> show sessions
Port    User    Host/Inet/Dest   Type      Dir   Status         Start    Idle
----    ----    --------------   --------   ---   -------------   ---      --
C0      test1                    Login     In    COMMAND        0
C1                               Login     In    USERNAME       0
*****************Slot0**************
S0                               Login     In    USERNAME       0        0
S1                               Device    Out   ESTABLISHED    1:23     1:23
S2                               Device    Out   ESTABLISHED    3        3
S3                               Log/Net   In    USERNAME       0        0
S4                               Login     In    USERNAME       0        0
S9                               Login     In    USERNAME       0        0
S10                              Log/Net   In    NO-SERVICE     0        0
.
.
.
S95                              Log/Net   In    NO-SERVICE     0        0
*****************Slot1**************
S0                               Log/Net   In    NO-SERVICE     0        0
S1                               Log/Net   In    NO-SERVICE     0        0
S2                               Log/Net   In    NO-SERVICE     0        0
S3                               Log/Net   In    NO-SERVICE     0        0
S4                               Log/Net   In    NO-SERVICE     0        0
S9                               Log/Net   In    NO-SERVICE     0        0
S10                              Log/Net   In    NO-SERVICE     0        0
.
.
.
```

S95		Log/Net	In	NO-SERVICE	0	0

Explanation

Port	Console, WAN, or ISDN, asynchronous port 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 2-3 on page 2-20.
Start	Time in minutes since the session started.
Idle	Time in minutes that the session has been idle.

show slots

This command displays general information about the physical slots in the PortMaster 4 and information about the PortMaster 4 chassis.

> 4.0   **show slots**

Example

The output of this command is the same from any view. The following example is from a PortMaster 4 running ComOS 4.1:

```
Command> show slots
AC Power:       Top: Working       Middle: Working Bottom: Removed
Max Power: 800W,  Allocated: 520 W, Left: 280W
DC Power:       Primary DC: Off      Secondary DC: Off
Fan Status:     1: On 2: On 3: On 4: On
--------------------------------------------------------------------------
                Chassis slot entries
--------------------------------------------------------------------------
Slot    State     Board      Config Serial Number  Power    Temp        Rev
  00     Empty                On                    0W       n/a
  01     ACTIVE    Quad T1    On     slot1          200W     34C/86F
  02     ACTIVE    Quad T1    On     3C00006        80W      34C/86F      B
  03     ACTIVE               On                    0W       n/a
  04     ACTIVE    Manager    On     Manager        80W      n/a
  05     EMPTY                On                    0W       n/a
  06     EMPTY    Ethernet    On     slot6          80W      37C/95F
```

07	EMPTY	Triple E1	On	3D00405	80W	33C/86F	B
08	EMPTY		On		0W	n/a	
09	EMPTY		On		0W	n/a	

Explanation

AC Power   Shows if the AC power supplies are working.

The maximum power available to the PortMaster 4 from the three AC power supplies is 1200W. If a power supply fails or is disabled, an SNMP alarm is generated.

Before it turns on a board, the PortMaster 4 determines how much power a board requires. If enough power is available, the board is turned on; if not, the board is left without power and an SNMP alarm is generated. If the PortMaster 4 experiences wattage drop and is unable to run all installed boards, it shuts down boards until sufficient power is available. Boards are shut down by type, and then by slot number. High slot numbers are shut down before low slot numbers. The manager module never shuts down because of a shortage of power.

Max Power   Maximum power—in watts—available to the PortMaster 4.

  Allocated   Power allotted to the boards.

  Left   Available power.

DC Power   Shows if DC power is on or off.

Fan Status   Status—on or off—of the four fans of the PortMaster 4.

If any fan fails, an SNMP alarm is generated. Fan failure does not cause boards to shut down. For information about hot-swapping a failed fan, see the *PortMaster 4 Installation Guide*.

Slot   Slot number—an integer between 0 and 9—that specifies a physical location in the PortMaster 4 chassis. See Table 2-2 for slot number values.

State   One of the following states for each slot in the PortMaster 4:

  Present   Board or module is detected but not identified by the system manager. No code has been loaded.

  Active   Board or module is present and operational.

  Config   Board or module is not active.

  Empty   No board or module is present.

Board   One of the following board types occupying a slot:

  Quad T1   Contains either four ISDN Primary Rate Interface (PRI) or T1 line ports and 98 modems, or four T1 line ports only.

  Tri E1   Contains either three ISDN PRI or E1 line ports and 98 modems, or three E1 line ports only.

  Manager   Manager module that contains a 10Mbps Ethernet connection and two asynchronous ports.

	Ethernet	Single interface standalone Ethernet board with one 10/100Mbps Ethernet connection and one MII connection, or a dual standalone Ethernet module with two 10/100Mbps Ethernet connectors and two MII connections.
	T3 Mux	Demultiplexes T3 bandwidth into 28 DS-1 channels and terminates them on Quad T1 lines.

Config   Shows if the board is configured or not.

Serial Number   Serial number of the board in each slot. The manager board displays **Manager** because it cannot read its own serial number.

The serial number of the board is stored in the serial EPROM (SEP) located on each board. The EPROM also contains the type of board, the amount of power to be budgeted for the board, the temperature of the board, and the serial number and revision number of the board.

If the EPROM driver is unable to interpret the programmed information, it shows the board type as **unknown**.

Power   Number of watts allotted for the board. When a board is originally detected, the manager module reads this information from the board itself. If the information is unavailable, the manager module allocates 80W for the board.

Ether1—the 10/100Mbps Ethernet connection physically in slot 4—is powered by the manager board. It does not shut down when the power is low.

Temp   Board temperature in degrees Celsius. ComOS 4.1 also displays the temperature in degrees Fahrenheit. The manager module samples board temperature every 10 seconds. If the board temperature exceeds 45°C (113°F), the manager module generates an SNMP alarm. See **show alarms** on page 3-36. To manually set a shutdown temperature, use the **set shutdown temp** command.

If the temperature exceeds 50°C (122°F), the manager module generates another SNMP alarm as the board is shut down. To turn on the board again, use the **set slot** command.

The manager board and the Ethernet board on the manager module do not shut down from excessive heat.

Rev   Board version number.

See Also

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 3-23).

See Also

set loghost - page 3-16

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|user**

filter	See the following example and page 12-18.
host	See page 13-3.
location	See page 11-22.
modem	See page 5-40.
netmask	See page 7-27.
snmp	See page 3-37.
user	See page 10-18.

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

Usage

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

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

Example

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

See Also

rlogin - page 2-15
set telnet - page 3-25

tftp get

This command retrieves a file of configuration commands or a ComOS image from a TFTP server using the Trivial File Transfer Protocol (TFTP) and moves it to the nonvolatile RAM of the PortMaster.

> **tftp get** [**comos**|**config**|**nostop**] *Ipaddress String*

comos	Downloads a ComOS image that has been translated via **uuencode** to ASCII for the transmission over the Internet. This is the default. If no keyword is specified, the PortMaster tries to download this ComOS image.
config	Downloads a text file containing command line interface commands. If any one of the commands produces an error, the TFTP transmission is terminated.
nostop	Downloads a text file containing command line interface commands. If any one of the commands produces an error, the TFTP transmission is terminated the TFTP transmitting will continue.
Ipaddress	IP address or hostname—up to 39 characters—of the TFTP server.
String	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 decrementing 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 2-10
ptrace - page 2-11

version

This command displays the ComOS software version number, PortMaster hardware platform, 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
Lucent PortMaster PM-4 ComOS 4.0
System uptime is 29 minutes
```

Global Settings　　3

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.

Global settings allow you to set default and alternate hosts, set gateways and metrics, set the name service used by the PortMaster 4, and set the administrative password of the PortMaster 4.

Displaying Global Information

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

- **show all**—see page 2-19

- **show global**—see page 2-26

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 4, except for those commands marked with a leading bullet (•), which are global only for a specific module or board.

The following sections also cover global commands affecting the entire PortMaster 4:

- RADIUS commands - see page 3-26

- ChoiceNet commands - see page 3-29

- SNMP commands - see page 3-31.

Table 3-1　　Global Commands

Command Syntax	
add ippool *Name*|**default**	- see page 3-3
clear alarms|**alarm** *Alarm-id*|**all**	- see page 3-32
delete ippool *Name*|**default address-range** *Ipaddress*|**all**	- see page 3-4
reset ippool	- see page 3-5
• **set assigned_address** *Ipaddress*	- see page 3-5
set call-check on|**off**	- see page 3-6

Table 3-1   Global Commands *(Continued)*

Command Syntax	
set chap on|**off**	- see page 3-7
set chassis pm4|**msm-rac**	- see page 3-7
set default on|**off**|**broadcast**|**listen**	- see page 7-16
set dhcp-server *Ipaddress*	- see page 3-8
set domain *String*|**none**	- see page 3-9
set gateway *Ipaddress* [*Metric*]	- see page 7-11
set host [**1**|**2**|**3**|**4**] *Ipaddress*	- see page 3-10
set ippool *Name*|**default** *Ipaddress/NM*|*Ipaddress Netmask* [*Gateway*]	- see page 3-10
set ippool *Name* **default-gateway** *Gateway*	- see page 3-12
set ipx on|**off**	- see page 3-13
set ipxgateway *Network*|*Node Metric*	- see page 3-14
• **set isdn-switch**	- see page 15-5
set local-ip-address [**1**|**2**|**3**|**4**] *Ipaddress*	- see page 3-14
set loghost *Ipaddress*	- see page 3-16
set maximum pmconsole *Number*	- see page 3-17
set nameserver [**1**|**2**] *Ipaddress*	- see page 3-17
set namesvc dns|**nis**	- see page 3-18
set netbios on|**off**	- see page 3-19
set pap on|**off**	- see page 3-19
set password [*Password*]	- see page 3-20
• **set pool** *Number*	- see page 3-21
set reported_ip *Ipaddress*	- see page 3-21
set serial-admin on|**off**	- see page 3-22
set shutdown-temp *Number*	- see page 3-22
set syslog *Logtype* {[**disabled**] [*Facility.Priority*]}	- see page 3-23
set telnet *Tport*	- see page 3-25

Table 3-1 Global Commands *(Continued)*

Command Syntax	
set user-netmask on|off	- see page 7-11
show alarms	- see page 3-36
show all	- see page 2-19
show global	- see page 2-26
show table ippool	- see page 3-25

Global Commands

These commands are used to configure global settings on the PortMaster or on a particular module or board.

add ippool

This command adds a named IP pool to the IP pool table.

 4.1   **add ippool** *Name*|**default**

Name	Name of the IP pool—a string of up to 31 characters.
default	Adds a default IP pool to the IP pool table.

Usage

The PortMaster 4 supports named IP pools on ComOS 4.1 and later releases. Named IP pools provide a global range of multiple dynamically assigned IP addresses within the PortMaster 4.

You can assign a gateway address to each range in a named IP pool, or assign a default gateway address for the entire named IP pool. Because you cannot create user profiles for IP pools in PortMaster user tables, you can only configure named IP pools using RADIUS.

To activate changes to a named IP pool configuration, use the **reset ippool** command.

Note – To use IP pools, you must also add a corresponding RADIUS attribute to the RADIUS dictionary file. See the *PortMaster 4 Configuration Guide* for more information.

Example

```
Command> add ippool shelbyville
IP pool shelbyville successfully added
```

See Also

delete ippool - page 3-4
reset ippool - page 3-5
set ippool - page 3-10
set ippool default - page 3-12
show table ippool - page 3-25

delete ippool

This command deletes an IP address from the specified named IP pool or the entire named IP pool.

| 4.1 | **delete ippool** *Name* **address-range** *Ipaddress*\|**all** |

Name	Name of the IP pool in the IP pool table—a string of up to 31 characters.
default	Deletes the default IP pool from IP pool table.
Ipaddress	IP address or range of IP addresses from the named IP pool.
all	Deletes the entire named IP pool.

Usage

The PortMaster 4 supports named IP pools on ComOS 4.1 and later releases.

To activate changes to a named IP pool configuration, use the **reset ippool** command.

Examples

```
Command> delete ippool address-range livermore 192.168.1.0
Range 192.168.1.0 in livermore successfully deleted

Command> del ippool livermore all
Pool livermore successfully deleted
```

See Also

add ippool - page 3-3
reset ippool - page 3-5
set ippool - page 3-10
set ippool default - page 3-12
show table ippool - page 3-25

reset ippool

This command activates changes to a named IP pool configuration and converts IP address ranges as routes for propagation through routing protocols.

> 4.1   **reset ippool**

Usage

The PortMaster 4 supports named IP pools on ComOS 4.1 and later releases.

After you enter the **reset ippool** command, the new routing protocols can take a short while to replace the old routes.

Example

```
Command> reset ippool
IP Pool reset
```

See Also

add ippool - page 3-3
delete ippool - page 3-4
set ippool - page 3-10
set ippool default - page 3-12
show table ippool - page 3-25

set assigned_address

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

Note – You must first use the **set view** command to select a board for configuration.

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 reset the slot after setting or changing the base IP address.

Example

```
Command 1> 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 3-21
set user destination - page 10-5

set call-check

This command provides the choice of supporting or disabling the RADIUS call-check feature on the PortMaster 4 products that support ISDN PRI or in-band signaling.

set call-check on|off

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

Caution – To support the call-check feature, you must configure RADIUS 2.1 Call-Check profiles; otherwise, the PortMaster issues a busy signal to every call. See the *RADIUS for UNIX Administrator's Guide* for more information.

Usage

The call-check feature enables user 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.

Example

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

See Also

set l2tp - page 17-4
set l2tp-lac - page 17-7

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 allows the user to negotiate CHAP as the authentication protocol. This is the default.
off	CHAP authentication is disabled.

Usage

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

Example

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

See Also

set location chap - page 11-6
set pap - page 3-19
show global - page 2-26

set chassis

This command identifies the chassis to the PMVision application as either a PortMaster 4 or an AnyMedia™ MultiService Module (MSM).

4.1 >   **set chassis pm4|msm-rac**

pm4	Identifies the chassis as a PortMaster 4. This is the default.
msm-rac	Identifies the chassis as an MSM.

Usage

The PortMaster 4 supports the **set chassis** command on ComOS 4.1 and later releases. To configure the PortMaster 4 in an MSM chassis using PMVision, you must first set the chassis to **msm-rac**.

If set to **msm-rac**, the PortMaster 4 displays the chassis type when you use the command **show global**. No additional chassis information is provided if you set the chassis to **pm4**.

Note – Use the **save all** command to save changes to nonvolatile RAM.

See Also

show global - page 2-26

set dhcp-server

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

> **set dhcp-server** *Ipaddress*

Ipaddress	IP address or 39-character hostname—except for 255.255.255.255. You cannot forward a DHCP packet to the broadcast address.

Usage

This command is used to support the 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 address 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 4 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.

See Also

set console - page 2-16
set debug *Hex* **-** page 14-6

set domain

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

> **set domain** *String*|**none**

String	Domain name. Maximum of 31 characters.
none	Disables the domain feature.

Usage

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

Example

```
Command> set domain lucent.com
Domain changed from   to lucent.com
```

See Also

set namesvc - page 3-18
set nameserver - page 3-17

set host

This command sets the default IP address or hostname for login sessions on the PortMaster 4.

> **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 *C0* **host** - page 5-15
set *C0* **service_device** - page 5-30
set *C0* **service_login** - page 5-31
set user host - page 10-8
set user service - page 10-17

set ippool

This command adds a range of IP addresses to a named IP pool and assigns it an optional gateway address.
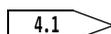
> 4.1 >   **set ippool** *Name*|**default** *Ipaddress/NM*|*Ipaddress Netmask* [*Gateway*]

Name   Name of the IP pool in the IP pool table—a string of up to 31 characters.

default	Sets the PortMaster 4 to use the default IP pool in the IP pool table. The PortMaster 4 assigns a user an address from the IP range of the default IP pool only if both of the following are true:

• The Named-IP-Pool attribute is not configured in RADIUS.

• The Quad T1 or Tri E1 board's assigned IP range is set to 0.0.0.0.

See the *PortMaster 4 Configuration Guide* for more information.

Ipaddress/NM	Specifies the range of named IP pool addresses.

Ipaddress	Base IP address in dotted decimal notation for the range. The PortMaster 4 increments this IP address by 1 when assigning IP addresses to users.
/NM	Integer between 1 and 30. Because the PortMaster does not use the first and last addresses specified in a range, you cannot use the masks **31** and **32** because they contain two hosts or fewer.

Ipaddress Netmask	Alternate method of specifying a named IP pool range.

Ipaddress	Base IP address in dotted decimal notation for the range.
Netmask	Netmask in dotted decimal notation.

Gateway	Optional gateway IP address for the specified range in the IP pool expressed in dotted decimal notation.

When the PortMaster receives a packet from a user with an assigned gateway address, the PortMaster forwards the packet to this gateway address instead of consulting its routing table.

If no gateway is specified for the range, the PortMaster uses the default address assigned to the IP pool. If no default address is set for the IP pool, the PortMaster consults its routing table.

Usage

The PortMaster 4 supports named IP pools on ComOS 4.1 and later releases. Up to eight ranges can be assigned to any single named IP pool. The PortMaster 4 assigns address ranges—except the first and last addresses—to users, using the first ranges before the latter ranges. Each range has a base address associated with it and is incremented to assign addresses. The number of addresses in a range is determined by the netmask.

To activate changes to a named IP pool configuration, you must use the **reset ippool** command.

Examples

1. The following example uses the format *Ipaddress*/*NM* to assign the of IP addresses of a range. Note that the 24-bit mask assigns 254 available IP addresses—the first and last addresses are not assigned to users.

   Command> **set ippool livermore address-range 192.168.1.0/24 10.34.56.78**
   Range 192.168.1.0/24 256 with gateway 10.34.56.78 add to livermore

2. The following example uses the format *Ipaddress Netmask* to assign a range of IP addresses to a named IP pool. No gateway address is specified for this range.

   Command> **set ippool livermore address-range 192.168.1.0 255.255.255.0**
   Range 192.168.1.0/24 256 with gateway 0.0.0.0 add to livermore

See Also

add ippool - page 3-3
delete ippool - page 3-4
reset ippool - page 3-5
set crossbar-ip - page 7-5
set ippool default - page 3-12
show table ippool - page 3-25

set ippool default-gateway

This command sets the default gateway address for an entire named IP pool.

4.1 >   **set ippool** *Name* **default-gateway** *Gateway*

Name	Name of the IP pool in the IP pool table—a string of up to 31 characters.
Gateway	Default gateway address for the named IP pool in dotted decimal notation.

Usage

The PortMaster 4 supports IP named pools on ComOS 4.1 and later releases.

You can assign a gateway address to each named IP pool, or assign a default gateway address for all named IP pools. The default gateway also functions as a crossbar IP address.

When a packet comes in from a user assigned a gateway address, the PortMaster forwards the packet to the gateway address instead of consulting its routing table. If a gateway address is not assigned to a range, the range uses the default gateway address of the named IP pool. If the named IP pool is not assigned a default address, then no crossbar IP is used and the PortMaster consults its routing table.

Example

Command> **set ippool shelbyville default 192.168.1.1**
Pool default gateway set to 192.168.1.1

See Also

add ippool - page 3-3
delete ippool - page 3-4
reset ippool - page 3-5
set crossbar-ip - page 7-5
set ippool - page 3-10
show table ippool - page 3-25

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

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 to make the change
take 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 11-10
set *C0* **ipxnet -** page 5-18
set *W1* **ipxnet -** page 6-11
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*

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

Usage

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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*.

Examples

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

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

set local-ip-address

This command assigns up to four local IP addresses to the PortMaster 4 that are not limited by network interface.

> ⟩4.1⟩   **set local-ip-address** [**1**|**2**|**3**|**4**] *Ipaddress*

1|**2**|**3**|**4**	Sets the local IP address for the PortMaster 4. The default local IP address is 1.
Ipaddress	IP address or hostname—up to 39 characters. Setting the IP address to 0.0.0.0 clears the local IP address.

Usage

The PortMaster 4 uses the local IP address as follows:

- First, the PortMaster 4 can advertise its local IP addresses as host routes through configured routing protocols such as OSPF and RIP Version 2 (RIP-2), allowing PortMaster 4 services to be referenced to a particular IP address independent of any one network interface.

- Second, the PortMaster 4 uses the local IP address to determine how it identifies itself during PPP negotiations for the IP Control Protocol (IPCP), and in the source address of an IP packet. For additional information, see the *PortMaster 4 Configuration Guide*.

If local addresses are set, the **ifconfig** command displays the logical interfaces as **local10**, **local11**, **local12**, and **local13**. To display logical interfaces, use the **ifconfig** command.

Examples

```
Command> set local-ip-address 10.112.34.17
set local-ip-address 10.112.34.17
Local IP Address (1) changed from 0.0.0.0 to 10.112.34.17


Command> set local-ip-address 2 192.168.54.6
set local-ip-address 2 192.168.54.6
Local IP Address (2) changed from 0.0.0.0 to 192.168.54.6
```

See Also

set *Ether0* **address -** page 4-3
set reported_ip - page 3-21

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 the manager module after making changes to the loghost address. You can also use the **reset n***Handle* command to reset the UDP port 514 connection.

RADIUS accounting provides a more complete method for logging usage information. Refer to the *RADIUS for UNIX Administrator's Guide* or the *RADIUS for Windows NT 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 3-23

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

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

Note – If two or more GUIs are used to configure the PortMaster 4 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 n***Handle* command to reset network handles. To view open network connections, use the **show netconns** command.

Example

```
Command> set maximum pmconsole 2
Maximum PMconsole sessions changed from 0 to 10
```

See Also

set serial-admin - page 3-22
set telnet - page 3-25

set nameserver

This command sets the name server IP address.

set nameserver [**1**|**2**] *Ipaddress*

1	Sets the primary name server. This is the default.
2	Sets an alternate name server.
Ipaddress	IP address in dotted decimal notation.

Usage

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

Example

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

See Also

set domain – page 3-9
set namesvc – page 3-18

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 3-9
set nameserver – page 3-17

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

Note – The PortMaster 4 supports IPX protocols on ComOs 4.1 and later releases.

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 3-13

set pap

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

> **set pap on|off**

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

Usage

With PAP set to **off**, the default is to support CHAP. If you do not want to support CHAP authentication, you must disable CHAP (see page 3-7).

Example

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

See Also

set chap - page 3-7
show global - page 2-26

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.

Note – You must first use the **set view command** to select a board for configuration.

> **set pool** *Number*

Number   Number of IP addresses to allocate to the pool.
                    The valid range on a PortMaster 4 is from 0 to 96.

Usage

After you set or change the pool size of IP addresses, you must reset the slot 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 3-5

set reported_ip

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

> **set reported_ip** *Ipaddress*

Ipaddress   IP address.

Usage

The IP address of any PortMaster product can be used with this command. This feature is valuable for sites that require a number of PortMaster products to appear as a single IP address to other networks. With PPP, this information is placed in the startup message, and the PortMaster products 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 10-11

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 left (on) position.

Example

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

set shutdown-temp

This command manually sets the threshold temperature for all the boards and modules of the PortMaster 4.
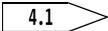
> 4.1

> **set shutdown-temp** *Number*

Number   Shutdown temperature—integer between 30°C and 90°C
                  (86°F and 194°F).

Usage

The PortMaster 4 supports the **set shutdown-temp** command on ComOS 4.1 and later releases.

Each board on the PortMaster 4 has a temperature sensor. The PortMaster 4 shuts down a board or module when the temperature of the board or module reaches the set threshold temperature.

To view the **shutdown-temp** setting, use the **show global command**.

For additional information about PortMaster 4 temperature management, see the *PortMaster 4 Installation Guide*. If the shutdown temperature is not set, the PortMaster 4 begins turning boards off when it reaches an internal temperature of 50°C (122°F) until the temperature goes below 45°C (113°F). Boards are turned off in order of slot number, with the highest-numbered slot being turned off first.

To turn on a board that has been turned off, use the **set slot on** command.

See Also

set slot - page 2-17

set syslog

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

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

Logtype	Sets logging for the following five areas. Use the following keywords:

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

disabled	Turns off logging for the *Logtype* specified.
Facility.Priority	Sets the facility and priority to be assigned to **syslog** messages. See Table 3-2 on page 3-24 and Table 3-3 on page 3-24 for *Facility* and *Priority* keywords. Enter the *Facility* and *Priority* 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 3-3 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 3-16

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 must not be used for this function.

The maximum number of concurrent Telnet sessions on the PortMaster 4 is 20.

Example

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

See Also

set maximum pmconsole - page 3-17
set serial-admin - page 3-22
telnet - page 2-42

show table ippool

This command displays the named IP pool configuration.

show table ippool

Example

```
Command> show table ippool
Name: livermore               Default Gateway: 10.23.45.56

Address/netmask               Gateway
------------------             --------------------
192.168.1.0/29                0.0.0.0
192.168.2.253/30              0.0.0.0
192.168.3.50/25               0.0.0.0
10.4.5.0/24                   192.168.222.3
```

Explanation

Name	Name of IP pool.
Default Gateway	Default gateway for the specified named IP pool.
Address/netmask	Range of the named IP pool.
Gateway	Specified gateway address for the named IP pool range.

See Also

add ippool - page 3-3
delete ippool - page 3-4
reset ippool - page 3-5
set ippool - page 3-10
set ippool default - page 3-12

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. ChoiceNet client commands begin on page 3-29, and SNMP commands begin on page 3-31.

Table 3-4   RADIUS Client Configuration

Command Syntax	
set accounting [**1**|**2**|**3**] *Ipaddress* [*Uport*]	- see page 3-27
set authentication_server [**1**|**2**|**3**] *Ipaddress* [*Uport*]	- see page 3-28
set secret *String*	- see page 3-29

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

set accounting

This command designates a host as the primary, secondary, or tertiary RADIUS accounting server.

> **set accounting** [**1**|**2**|**3**] *Ipaddress* [*Uport*]

1	Designates the primary RADIUS server. This is the default.
2	If present, designates a host as the alternate accounting server.
3	If present, designates a host as the tertiary accounting server.
Ipaddress	IP address or 39-character hostname running a RADIUS accounting server on UDP port 1646.
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.

`4.1` ▷

Usage

You can designate a primary RADIUS accounting server and up to two alternates, but you must assign a different iP address to each server. The accounting server daemon must be present on the host for the RADIUS accounting server to function correctly. Set *Ipaddress* to 0.0.0.0 to deselect the accounting server.

The PortMaster 4 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 authentication_server

This command sets the primary, secondary, or tertiary RADIUS authentication server.

set authentication_server [**1**|**2**|**3**] *Ipaddress* [*Uport*]

1	Designates the primary authentication server. This is the default.
2	If present, designates a host as the secondary authentication server.
3	If present, designates a host as the tertiary authentication server.
Ipaddress	IP address or 39-character hostname for a host running a RADIUS authentication server on UDP port 1645.
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.

4.1

Usage

Set *Ipaddress* to 0.0.0.0 to deselect the primary authentication server. For more information about setting up a RADIUS authentication server, refer to the *RADIUS for UNIX Administrator's Guide* or the *RADIUS for Windows NT Administrator's Guide*.

You can also use the **set alternate_auth_server** command to set the secondary authentication server.

Examples

```
Command> set authentication 1 10.0.0.3
Authentication Server changed from 0.0.0.0 1645 to 10.0.0.3 1645

Command> set authentication 1 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 3-27
set *CO* **security** - page 5-29
set secret - page 3-29

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 *CO* **security** - page 5-29

ChoiceNet Client Commands

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

Table 3-5   ChoiceNet Client Configuration

Command Syntax	
set choicenet [**1**|**2**] *Ipaddress* [*Uport*]	- see page 3-30
set choicenet-secret *String*	- see page 3-30
set debug choicenet on|**off**	- see page 14-4

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.
Ipaddress	IP address or 39-character hostname of the host running a ChoiceNet server on UDP port 1647.
Uport	Integer between 0 and 65535 that specifies the UDP port to be used for ChoiceNet. 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.

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

Examples

```
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|*Ipaddress*	- see page 3-31
clear alarms|alarm {*Alarm-id*|**all**}	- see page 3-32
delete snmphost reader|writer|*Ipaddress*	- see page 3-33
save snmp	- see page 3-34
set snmp on|off	- see page 3-34
set snmp readcommunity|writecommunity *String*	- see page 3-35
set sysname *String*	- see page 2-18
show alarms [*Alarm-id*]	- see page 3-36
show table snmp	- see page 3-37

add snmphost

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

> **add snmphost reader\|writer any\|none\|***Ipaddress*

reader	Adds a read-and-trap 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.
Ipaddress	IP address or hostname—up to 39 characters—of the read or write host.

Usage

The specification of read-and-trap host and write host 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-and-trap host 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 3-33
save snmp - page 3-34
set snmp - page 3-34
show table snmp - page 3-37

clear alarms

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

    clear alarms|alarm {*Alarm-id*|**all**}

alarms	Clears all alarms.
alarm *Alarm-id*	Clears a specific instance of an alarm. Use the **show alarms** command to display alarm ID numbers.
alarm all	Clears all alarms.

Usage

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

Example

```
Command> show alarms
Alarm Id    Age        Severity    Alarm Message
--------    ------     ---------   -----------------------------------
4001608     3days:11   0           slot 1 T1 line(0) down


Command> clear alarm all
Command> show alarms
Alarm Id    Age        Severity    Alarm Message
```

See Also

show alarms - page 3-36

delete snmphost

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

delete snmphost reader|writer *Ipaddress*

reader	Use to delete a read-and-trap host.
writer	Use to delete a write host.
Ipaddress	IP address or hostname of the read-and-trap 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 3-31

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 3-34

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 3-31
save snmp - page 3-34
show modules - page 2-31
show table snmp - page 3-37

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. If possible, 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 3-31
save snmp - page 3-34
set snmp - page 3-34
show table snmp - page 3-37

show alarms

This command displays instances of SNMP traps—notifications of certain events—that have occurred on the entire PortMaster 4.

> **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 the following:

- Nonfunctioning T1, E1, or T3 lines

- Modem failure

- Removal of AC power supplies

- Availability of DC power

- Fan failure

- Overheated line board slots

- Lack of power to line board slots

- Blown fuse

You can enter this command from any view.

Examples

```
Command> show alarms
Alarm Id     Age        Severity     Alarm Message
--------     ------     ---------    -------------------------------------
4763864      3 days     0            T1 line(0) down
```

```
Command> show alarm 4001608
---------------------- Alarm Details -------------------------
Alarm Id: 4001608            Alarm Message: slot 1 T1 line(0) down
Age in minutes: 3days        Alarm repeated: 1 times
Severity: 0                  Reported: SNMP
```

See Also

clear alarms - page 3-32

show table snmp

This command shows the settings in the SNMP table.

> **show table snmp**

Usage

The SNMP table contains the settings for the SNMP read and write communities. View the table to ensure that these communities are set to prevent unauthorized users from changing configuration information.

Example

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

See Also

save snmp - page 3-34
set snmp - page 3-34

Ethernet Interface 4

This chapter describes how to use the command line interface to configure the Ethernet interfaces of the PortMaster 4. The PortMaster 4 manager module comes with two routable Ethernet interfaces, a 10BaseT Ether0 and 10/100BaseT Ether1.

4.1 ▷ ComOS releases 4.1 and later also support a standalone Ethernet board with one 10/100BaseT interface (Ether0) and a standalone dual Ethernet module with two 10/100BaseT interfaces (Ether30 and Ether31). A PortMaster 4 can have only one dual Ethernet module, and it must be installed in slot 3. No new commands are required to support the standalone Ethernet board and module.

For additional information about installing and configuring the Ethernet ports of the PortMaster 4, refer to the *PortMaster 4 Installation Guide* and *PortMaster 4 Configuration Guide*.

Detailed command definitions follow a command summary table.

Commands for configuring subinterfaces on Ether0 are also summarized and defined in this chapter.

Note – To activate any changes to the configuration of Ether0—the 10BaseT interface on the manager module—you must use **reboot**. For all other Ethernet interfaces, you must use the appropriate **reset slot** command.

Displaying Ethernet Information

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

- **ifconfig**—see page 2-9
- **show all**—see page 2-19
- **show arp** *Ether0*—see page 2-21
- **show** *Ether0*
- **show global**—see page 2-26
- **show igmp**
- **show netconns**—see page 2-32
- **show netstat**—see page 2-32

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 Ethernet interfaces on the PortMaster 4. Ethernet subinterface commands are summarized in Table 4-2, on page 4-15.

Table 4-1   Ethernet Configuration Commands

Command Syntax	
reboot	- see page 2-13
reset slot*Slotnumber*	- see page 2-13
save ports	- see page 2-15
set *Ether0* **address** *Ipaddress* [*/NM*]|[*Ipmask*]	- see page 4-3
set *Ether0* **broadcast high**|**low**	- see page 4-5
set *Ether0* **crossbar-ip** *Ipaddress*	- see page 7-5
set *Ether0* **ifilter** [*Filtername*]	- see page 4-5
set ether0 ip enabled|**disabled** [1]	- see page 4-6
set ether0 ipx enabled|**disabled** [1]	- see page 4-7
set *Ether0* **ipxframe** **ethernet_802.2**|**ethernet_802.2_ii**|**ethernet_802.3**| **ethernet_ii**	- see page 4-7
set *Ether0* **ipxnet** *Ipxnetwork*	- see page 4-8
set *Ether0* **mproxy address** *Ipaddress*|**port** *Tport*|**src-address** *Ipaddress*|**src-netmask** *Netmask*|**slot** *Seconds*| **number** *Number*|**timeout** *Seconds*|**alarm** *Number*	- see page 4-9
set *Ether0* **mproxy on**|**off**	- see page 4-10
set *Ether0* **netmask** *Ipmask*	- see page 7-7
set *Ether0* **ofilter** [*Filtername*]	- see page 4-11
set *Ether0* **ospf accept-rip on**|**off**	- see page 8-6
set *Ether0* **ospf on**|**off**	- see page 8-6
set *Ether0* **rip on**|**off**|**broadcast**|**listen**|**v2** {**broadcast**|**multicast**|**on**|**v1-compatibility**}	- see page 7-17
set *Ether0* **route-filter incoming**|**outgoing** [*Filtername*]	- see page 7-8

Table 4-1   Ethernet Configuration Commands *(Continued)*

Command Syntax
set view   - see page 2-18
show *Ether0*   - see page 4-12
show igmp   - see page 4-14

Ethernet Commands

These commands affect the Ethernet interfaces of the PortMaster 4—Ether0, Ether1, and the standalone Ethernet module and boards. All Ether0 commands can be used for Ether1 and the standalone Ethernet module and boards, except as noted in this section. You can configure the Ethernet interfaces from any view.

Lucent recommends that network traffic—**syslog**, **traceroute**, **telnet**, DNS, ChoiceNet, RADIUS, and TFTP—be configured using *Ether1*.

set *Ether0* address

This command sets the IP address of the Ethernet interface.

      set *Ether0* **address** *Ipaddress* [*/NM*]|[*Ipmask*]

Ether0	One of the following Ethernet interfaces:

ether0	10BaseT interface on the manager module.
ether1	10/100BaseT interface on the manager module.
ether00	Single 10/100BaseT Ethernet interface on the standalone Ethernet board in slot 0.
ether10	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 1.
ether20	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 2.
ether30	Single 10/100BaseT Ethernet interface on a standalone Ethernet board or the first Ethernet interface on a dual Ethernet module in slot 3.
ether31	Second 10/100BaseT Ethernet interface on a dual standalone Ethernet module in slot 3.
ether50	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 5.
ether60	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 6.

4.1 ▷

ether70	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 7.
ether80	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 8.
ether90	Single 10/100BaseT Ethernet interface on a standalone Ethernet board in slot 9.

Note – You must configure Ether0 or Ether1 with an IP address for the standalone Ethernet board or dual Ethernet module to function.

Ipaddress	IP address or hostname.
/NM	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.
Ipmask	Optional netmask expressed in dotted decimal notation. Enter a space between the IP address and the netmask.

Usage

Each 10/100BaseT Ethernet interface on the PortMaster 4 has an alternative media-independent interface (MII) for connection to fiber and copper media. ComOS uses the MII if both it and the RJ-45 interface are connected.

Note – To activate any changes to the configuration of Ether0—the 10BaseT interface on the manager module—you must **reboot**; for all other Ethernet interfaces you must use the appropriate **reset slot** command.

If you change the IP address of an 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

reset slot - page 2-13
set *Ether0* **netmask** - page 7-7
set reported-ip - page 3-21

set *Ether0* **broadcast**

This command determines which broadcast address the PortMaster will use.

> **set** *Ether0* **broadcast high|low**

4.1 > *Ether0*	For a list of configurable Ethernet interfaces, see page 4-3.

Note – You must configure Ether0 or Ether1 with an IP address for the standalone Ethernet board or dual Ethernet module to function.

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. For the PortMaster 4, Lucent recommends that you connect *Ether0* and *Ether1* to separate Ethernet segments.

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*]

4.1 > *Ether0*	For a list of configurable Ethernet interfaces, see page 4-3.

Note – You must configure Ether0 or Ether1 with an IP address for the standalone Ethernet board or dual Ethernet module to function.

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 4 Configuration Guide* for more information on how to construct a filter. If the filter is changed, this command must be re-entered for the changes to take effect on the Ethernet interface.

You need not reboot the interface nor the PortMaster to activate the filter. To remove the filter, enter 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 4-11
show filter – page 12-18
show table filter – page 12-18

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.

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.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Example

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

See Also

set ipx on - page 3-13

set *Ether0* ipxframe

This command sets the IPX frame type.

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

> **set** *Ether0* **ipxframe ethernet_802.2|ethernet_802.2_ii**
> **|ethernet_802.3|ethernet_ii**

Ether0   Ethernet interface.

ethernet_802.2   Use Ethernet 802.2 protocol. This is the default
                              encapsulation used by Novell NetWare 4.0.

ethernet_802.2_ii	Use Ethernet 802.2_ii protocol. This encapsulation is not commonly used.
ethernet_802.3	Use Ethernet 802.3 protocol. This is the default encapsulation used by Novell NetWare 3.11.
ethernet_ii	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 must match those of your IPX network.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 3-13

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 must be entered in hexadecimal format, as shown in the example. You must enable IPX before using this command.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 3-13
set user ipxnet - page 10-10

set *Ether0* **mproxy**

This command enables the PortMaster 4 to monitor Internet Group Management Protocol (IGMP) multicast traffic from a heartbeat group of multicast routers.

> 4.1

set *Ether0* **mproxy address** *Ipaddress*|**port** *Tport*|**src-address** *Ipaddress*|
src-netmask *Netmask*|**slot** *Seconds*|**number** *Number*|**timeout** *Seconds*|
alarm *Number*

Ether0	**ether0** or **ether1**.
address *Ipaddress*	Broadcast address that identifies a multicast group—in dotted decimal notation.
port *Tport*	TCP port—an integer between 1 and 65535—on which the PortMaster 4 listens for a heartbeat.
src-address *Ipaddress*	IP address of the heartbeat source in dotted decimal notation, or the hostname—a string of up to 39 characters.
src-netmask *Netmask*	Netmask for the heartbeat source in dotted decimal notation.
slot *Seconds*	Length of a time slot in seconds—an integer between 0 and 120.
number *Number*	Number of time slots—an integer between 1 and 6.
timeout *Seconds*	Period of multicast host inactivity after which the PortMaster 4 disconnects the host. **timeout** is an integer between 60 and 600.
alarm *Number*	Minimum number of slots that must receive a heartbeat—an integer between 1 and 6. Otherwise, the PortMaster 4 sends an SNMP alarm.

Usage

The PortMaster 4 supports the multicast heartbeat feature on ComOS 4.1 and later releases.

This command sets time slots during which a multicast-enabled hosts must receive multicast traffic for the heartbeat group. Use this command to detect problems with multicast traffic by keeping track of multicast messages from the heartbeat group. If the number of slots receiving a heartbeat is lower than the set **alarm** value, the PortMaster 4 sends an SNMP alarm.

To activate new configuration settings, you must first use the **reboot** command.

Note – The PortMaster 4 does not currently support this command on the standalone Ethernet boards.

Example

Command> **set ether1 mproxy address 244.0.0.99 port 2000 src-address 192.168.20.1 src-netmask 255.255.255.255 slot 120 number 5 timeout 360 alarm 3**

See Also

set *Ether0* **mproxy on|off** - page 4-10
show igmp - page 4-14

set *Ether0* mproxy on

This command enables the Ethernet interface to listen for Internet Group Management Protocol (IGMP) broadcasts and send multicast broadcasts.

> 4.1

      set *Ether0* **mproxy on|off**

Ether0	**ether0** or **ether1**.
on	Enables the PortMaster 4 to listen for IGMP broadcasts from multicast-enabled hosts in its multicast group on the specified Ethernet interface.
	Setting multicast proxy routing **on** also enables the PortMaster 4 to broadcast the IGMP member report for all other multicast-enabled hosts in its multicast group to other multicast routers
off	Disables multicast proxy routing on the specified interface.

Usage

The PortMaster 4 supports IGMP multicast proxy on ComOS 4.1 and later releases.

To enable dial-in clients for multicast, you must configure corresponding RADIUS attributes. For more information about enabling users for multicast proxy, see the latest ComOS release notes.

To display multicast proxy heartbeat settings, use the **show** *Ether0* command.

Note – The PortMaster 4 does not currently support this command on the standalone Ethernet boards.

See Also

show *Ether0* - page 4-12
show igmp - page 4-14
set igmp - page 4-9

set *Ether0* ofilter

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

> **set** *Ether0* **ofilter** [*Filtername*]

| 4.1 | *Ether0* | For a list of configurable Ethernet interfaces, see page 4-3. |

Note – You must configure Ether0 or Ether1 with an IP address for the standalone Ethernet board or dual Ethernet module to function.

| *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 4 Configuration Guide* for more information on how to construct a filter. If the filter is changed, you must be re-enter this command for the changes to take effect on the Ethernet interface.

You need not reset nor reboot the interface or the PortMaster to activate the filter. To remove the filter, enter 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 12-18
show table filter - page 12-18

show *Ether0*

This command 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:c0:05:10:00:65
                Routing:  RIP (Broadcast, Listen (On))
           Input Filter:
          Output Filter:
        OSPF Accept RIP:  off
              OSPF Cost:  1
    OSPF Hello Interval:  10
         OSPF Dead Time:  40

Command> show ether1
        Ethernet Status:  IP - Enabled              IPX - Disabled
         Interface Addr:  192.168.97.25
                Netmask:  255.255.255.0
      Broadcast Address:  192.168.97.0
            IPX Network:  00000000
         IPX Frame Type:  ETHERNET_802.2
       Ethernet Address:  00:c0:05:11:00:65
                Routing:  RIP Off (Quiet)
              Multicast:  Enabled
    Multicast Heart Beat:  231.31.31.31
       Heart Beat slots:  5           Heart Beat Slot length 60 sec
      Heart Source Addr:  192.168.99.99/54    Heart Alarm Threshold: 3
             V1 Timeout:  300
           Input Filter:
          Output Filter:
        OSPF Accept RIP:  off
              OSPF Cost:  1
    OSPF Hello Interval:  10
         OSPF Dead Time:  40
```

Explanation

Ethernet Status	Shows IP 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.
Ethernet Address	The Ethernet hardware MAC address.
Routing	• **Broadcast**—the PortMaster broadcasts route information on the local Ethernet. • **Listen**—the PortMaster listens for route information from other routers on the local Ethernet.
Multicast Heart Beat	Broadcast address that identifies a multicast group.
Heart Beat slots	Number of time slots.
Heart Source Addr	IP address of the heartbeat source.
V1 Timeout	Period of IGMP v1 host inactivity after which the PortMaster 4 disconnects the host.
Heart Beat Slot length	Length of time slot in seconds.
Heart Alarm Threshold	Minimum number of slots that must receive a heartbeat.
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.
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.

show igmp

This command displays current dynamic multicast groups, including local and dial-in client group members.

> 4.1 > **show igmp**

Usage

The PortMaster 4 supports IGMP multicast proxy on ComOS 4.1 and later releases.

The PortMaster 4 displays a dynamic group table only—static groups cannot be added.

Example

The following example shows that IGMP multicast is enabled on Ether1. Its multicast broadcast address is 224.0.0.1. It listens for multicast broadcasts on 224.0.0.99.

```
Command 1> show igmp
multicast Source: ether1


Group: 224.0.0.1
        ether1
Group: 224.0.0.99
        ether1
```

See Also

set *Ether0* **mproxy** - page 4-9
set *Ether0* **mproxy on** - page 4-10

Ethernet Subinterface Commands

The PortMaster 4 supports the configuration of Ether0 on the manager module for multiple IP subnets. The MAC address for the subinterfaces is the same as that 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 – RIP, OSPF, packet filtering, and route propagation are not supported on Ethernet subinterfaces.

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

Table 4-2   Ethernet Subinterface Configuration

Command Syntax	
add subinterface *Name*	- see page 4-15
delete subinterface *Name*	- see page 4-16
set subinterface *Name* **address** *Ipaddress* [*/NM*]|[*Netmask*]	- see page 4-16
set subinterface *Name* **broadcast high**|**low**	- see page 4-17
set subinterface *Name* **netmask** *Netmask*	- see page 4-17
set subinterface *Name* **port** *Portlabel*	- see page 4-18
show location *Locname*	- see page 11-21
show table subinterface	- see page 4-18

add subinterface

This command adds a subinterface entry to the subinterface table.

> **add subinterface** *Name*

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

Usage

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

Example

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

See Also

show table subinterface - page 4-18

delete subinterface

This command removes a subinterface entry from the table.

> **delete subinterface** *Name*

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

Usage

You must use *Name* exactly as it is shown in the output of the **show table subinterface** command.

Example

Command> **delete subinterface net2**

set subinterface address

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

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

Name	Name of the subinterface configuration. Name can contain up to 11 characters.
Ipaddress	IP address or 39-character hostname.
/NM	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.
Netmask	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.

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

Name	Name of the subinterface configuration. *Name* can contain 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 4-5

set subinterface netmask

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

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

Name	Name of the subinterface configuration. *Name* can contain 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 used in the **set subinterface address** command.

See Also

set subinterface address - page 4-16

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.

> **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.**

Example

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

show table subinterface

This command displays the subinterface table.

> **show table subinterface**

Example

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

net2          192.168.55.6     255.255.255.0    192.168.55.255    ether0
```

Asynchronous Ports   5

This chapter describes how to use the command line interface to configure asynchronous ports. The PortMaster 4 comes with two asynchronous console ports on the manager module—C0 and C1.

Note – To configure the asynchronous ports, you must first access the system manager module using the **set view** command**.**

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.

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

Displaying Asynchronous Port Information

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

- **show** *C0*—see page 2-34

- **show all**—see page 2-19

- **ifconfig**—see page 2-9

- **show sessions**—see page 2-37

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 Commands

Command Syntax
add modem *ModemName* (*short*) **"***ModemName* (*long*)**" "***Speed***"**   - see page 5-37 *String*

Table 5-1   Asynchronous Port Configuration Commands *(Continued)*

Command Syntax	
attach *C0*	- see page 5-4
delete modem *ModemName*(*short*)	- see page 5-38
reset *C0*	- see page 2-13
save ports	- see page 2-15
set *C0*|**all access on**|**off**	- see page 5-6
• **set** *C0* **address** *Ipaddress*	- see page 5-6
set *C0*|**all cd on**|**off**	- see page 5-7
• **set** *C0* **compression on**|**off**|**stac**|**vj**	- see page 5-9
set *C0*|**all databits 5**|**6**|**7**|**8**	- see page 5-10
• **set** *C0* **destination** *Ipaddress* [*Ipmask*]	- see page 5-10
set *C0* **device** *Device* [**network dialin**|**dialout**|**twoway**]	- see page 5-11
set *C0*|**all dialback_delay** *Seconds*	- see page 5-12
set *C0*|**all dtr_idle on**|**off**	- see page 5-13
set *C0* **extended on**|**off**	- see page 5-13
set *C0*|**all group** *Group*	- see page 5-14
set *C0*|**all hangup on**|**off**	- see page 5-15
set *C0*|**all host default**|**prompt**|[**1**|**2**|**3**|**4**]*Ipaddress*	- see page 5-15
set *C0*|**all idletime Number** [**minutes**|**seconds**]	- see page 5-16
• **set** *C0*|**all ifilter** *Filtername*	- see page 5-17
• **set** *C0* **ipxnet** *Ipxnetwork*	- see page 5-18
set *C0*|**all login** [**network dialin**|**dialout**|**twoway**]	- see page 5-19
• **set** *C0*|**all map** *Hex*	- see page 5-20
set *C0*|**all message** *String*	- see page 5-21
set *C0*|**all modem-type** *ModemName*	- see page 5-21
• **set** *C0*|**all mtu** *MTU*	- see page 5-22
• **set** *C0* **netmask** *Ipmask*	- see page 5-23
set *C0*|**all network dialin**|**dialout**|**twoway**	- see page 5-23

Table 5-1   Asynchronous Port Configuration Commands *(Continued)*

Command Syntax	
set *C0*|**all network hardwired**	- see page 5-23
• set *C0*|**all ofilter** [*Filtername*]	- see page 5-25
set *C0* **ospf on**|**off**	- see page 8-7
set *C0*|**all override xon**|**rts**|**speed**|**parity**|**databits on**|**off**	- see page 5-25
set *C0*|**all parity even**|**none**|**odd**|**strip**	- see page 5-26
set *C0*|**all prompt** *String*	- see page 5-27
• set *C0* **protocol slip**|**ppp**|**x75-sync**	- see page 5-28
• set *C0*|**all rip on**|**off**|**broadcast**|**listen**|**v2** {**broadcast**|**multicast**|**on**|**v1-compatibility**}	- see page 7-17
set *C0* **route-filter incoming**|**outgoing** [*Filtername*]	- see page 7-8
set *C0*|**all rts/cts on**|**off**	- see page 5-28
set *C0*|**all security on**|**off**	- see page 5-29
set *C0*|**all service_device netdata**|**portmaster**|**rlogin**|**telnet** [*Tport*]	- see page 5-30
set *C0*|**all service_login netdata**|**portmaster**|**rlogin**|**telnet** [*Tport*]	- see page 5-31
set *C0*|**all speed** [**1**|**2**|**3**] **300**|**600**|**1200**|**2400**|**4800**|**9600**| **19200**|**38400**|**57600**|**76800**|**115200**	- see page 5-32
set *C0*|**all stopbits 1**|**2**	- see page 5-33
set *C0*|**all termtype** [*String*]	- see page 5-33
set *C0* **twoway** *Device* [**network dialin**|**dialout**|**twoway**]	- see page 5-34
set *C0* **username**|**autolog** *String*	- see page 5-35
set *C0*|**all xon/xoff on**|**off**	- see page 5-36
show all	- see page 2-19
show *C0*	- 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.

attach *C0*

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

> **attach** *C0*

C0   **c0** or **c1**—asynchronous console port.

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 external 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.

at&n1—Speech service.

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

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

Example

To communicate directly to an analog modem attached to asynchronous port C0, and configure the modem with the AT command **at&f1s0=1&w**, use the **attach** command as follows:

```
Command> attach C0
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 5-37
reset n*Handle* - page 2-13
set location script - page 11-18

set *C0*|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 *C0*|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 4 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 c0 access on**
Access Enhancement for port C0 changed from off to on

See Also

set *C0* ifilter - page 5-17

set *C0* address

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

> **set *C0* address** *Ipaddress*

Ipaddress	Hostname or IP address.

Usage

If the local IP address is set to 0.0.0.0, the PortMaster uses the *Ether1* 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 c0 address 192.168.7.2
Port C0 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 3-21

set *C0*|all cd

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

> **set** *C0*|**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.
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 c0 cd on
CD required for port C0 changed from off to on
```

See Also

add modem - page 5-37
show table modem - page 5-40

set *C0* compression

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

> **set *C0* compression on|off|stac|vj**

on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression.
off	Disables compression.
stac	Enables Stac LZS data compression only.
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 c0 compression on
Compression for port C0 changed from off to on
```

See Also

set location compression - page 11-6
set *C0* protocol - page 5-28
set user compression - page 10-6

set *C0*|all databits

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

> **set *C0*|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 c0 databits 8
Data bits for port C0 changed from 7 to 8
```

See Also

set *C0* modem-type *ModemName* - page 5-21
set *C0* parity - page 5-26
set *C0* speed - page 5-32
set *C0* stopbits - page 5-33

set *C0* destination

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

> **set *C0* destination** *Ipaddress* [*Ipmask*]

Ipaddress	IP address in dotted decimal notation 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 c0 destination 255.255.255.255
Port C0 destination changed from 0.0.0.0 to 255.255.255.255
```

See Also

set *W1* **destination** - page 6-8

set *C0* 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** *C0* **device** *Device* [**network dialin**|**dialout**|**twoway**]

Device	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** *C0* **host** command.

* Define the method used to connect the user to the port and device by selecting a device service with the **set** *C0* **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 c0 device /dev/ttyp0**
Port type for port C0 changed from User Login to Host Device(/dev/ttyp0)

See Also

set *C0* **host** - page 5-15
set *C0* **login** - page 5-19
set *C0* **twoway** - page 5-34

set *C0*|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** *C0*|**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 c0 dialback_delay 5**
Dialback delay for port C0 changed from 0 to 5

See Also

set user dialback - page 10-7

set *C0*|all dtr_idle

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

> **set *C0*|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 4 Configuration Guide* for more information.

Example

Command> **set c0 dtr_idle off**
DTR Idle for port C0 changed from on to off

See Also

set *C0* hangup - page 5-15
set *C0* modem-type *ModemName* - page 5-21

set *C0*|all extended

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

> **set *C0*|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** *C0* command provides more detailed output.

Example

Command> **set c0 extended on**
Extended mode for port C0 changed from off to on

set *C0*|all group

This command assigns asynchronous ports to external modem pools for use by dial-out locations. A group number is assigned to each location in the location table. Refer to Chapter 11, "Locations and DLCIs," for more information.

    set *C0*|**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 c0 group 2**
Group number for port C0 changed from 0 to 2

See Also

set location group - page 11-7

set *CO*|**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 *CO*|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 c0 hangup on**
DTR Hangup for port C0 changed from off to on

See Also

reset *C0* - page 2-13
set dtr_idle - page 5-13

set *CO*|**all host**

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

set *CO*|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.

Usage

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

host:
login:
Password:

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

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

Examples

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

Command> **set c0 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 *C0* **service_device** - page 5-30
set *C0* **service_login** - page 5-31
set user host - page 10-8

set *C0*|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 *C0*|**all idletime** *Number* [**minutes**|**seconds**]

Number	Timeout value in minutes or seconds. Any value from 0 to 240. The default value is 0.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.

Usage

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

If the value is set to 2 seconds or a longer interval, the port is reset after having no traffic for the designated time.

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 also turns off the idle timer after the user logs in.

Note – The idle time special value of 1 second applies only to asynchronous ports that have modem control turned on with the **set** *C0* **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.

To simultaneously set the idle time for all asynchronous ports, use the **set all idletime** command as shown in the example.

Example

```
Command> set c0 idletime 15
Idle timeout for C0 changed from 0 minutes to 15 minutes
```

See Also

set *C0* **cd on** - page 5-7

set *C0*|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** *C0*|**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.

To remove the input filter, enter the command without a filter name.

To simultaneously set the input filter for all hardwired asynchronous, use 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 c0 ifilter c0.in
Input filter for port C0 changed from   to c0.in
```

See Also

add filter - page 12-3
set *C0* **ofilter** - page 5-25

set *C0* ipxnet

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

> **set** *C0* **ipxnet** *Ipxnetwork*

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

Usage

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 c0 ipxnet 0XC009C801
Port C0 ipxnet changed from 00000000 to 0XC009C801
```

See Also

set *Ether0* **ipxnet** - page 4-8
set ipx on - page 3-13
set *W1* **ipxnet** - page 6-11

set *C0*|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** *C0*|**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** *C0* **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** *C0* **host** command.

- Define a login service with the **set** *C0* **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 c0 login network dialin**
Port type for port C0 changed from Login to User Login/Network(dialin)

See Also

set *C0* **device** - page 5-11
set *C0* **host** - page 5-15
set *C0* **service-login** - page 5-31

set *C0*|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** *C0*|**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 must be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments set the asynchronous map to 0 (zero) to achieve maximum throughput. 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** *C0* **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 c0 map 0xc0a86000**
Async Char Map for port C0 changed from 0x0 to 0xc0a86000

See Also

set location map - page 11-12
set *C0* **protocol** - page 5-28
set user map - page 10-12

set *C0*|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 *C0*|all message** *String*

String	Login message. The maximum length 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 *C0* message** and **set *C0* prompt** must not exceed 224 characters.

Example

```
Command> set c0 message Welcome to the Network (PMI/0)
New message:
Welcome to the Network (PMI/0)
For ports: C0
```

See Also

set *C0* prompt - page 5-27

set *C0*|all modem-type

This command selects an external modem from the modem table.

> **set *C0*|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 Configuration," on page 5-37 for more information.)

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

Example

Command> **set c0 modem-type usr-v34**
Modem type for port C0 changed from to usr-v34

See Also

add modem - page 5-37
show table modem - page 5-40

set *C0*|**all mtu**

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

> **set** *C0*|**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 must 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 c0 mtu 1500**
MTU for port C0 changed from 0 to 1500

See Also

set *C0* **protocol** - page 5-28

set *C0* netmask

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

> **set** *C0* **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 c0 netmask 255.255.255.0
C0 netmask changed from 0.0.0.0 to 255.255.255.0
```

See Also

set *Ether0* **netmask** - page 7-7
set location netmask - page 11-15
set user netmask - page 10-14
set *W1* **netmask** - page 6-13

set *C0*|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** *C0*|**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 c0 network twoway**
Port type for port C0 changed from Login to Network(twoway)

See Also

set *C0* **device** - page 5-11
set *C0* **login** - page 5-19
set *C0* **twoway** - page 5-34

set *C0*|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** *C0*|**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** *C0* **destination** command.

Example

Command> **set c0 network hardwired**
Port type for port C0 changed from Login to Network(hardwired)

See Also

set *C0* **destination** - page 5-10

set *C0*|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** *C0*|**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 c0 ofilter c0.out**
Output filter for port C0 changed from   to c0.out

See Also

add filter - page 12-3
set *C0* **ifilter** - page 5-17

set *C0*|all override

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

> **set** *C0*|**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 c0 override speed on**
Host override of speed for port C0 changed from off to on

See Also

set *C0* **device** - page 5-11
set *C0* **modem-type** *ModemName* - page 5-21
set *S0* **parity** - page 5-26
set *C0* **speed** - page 5-32

set *C0*|all parity

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

>   **set** *C0*|**all parity even**|**none**|**odd**|**strip**

even	Set for 7 data bits, 1 stop bit, and even parity.
none	Set for 8 data bits, 1 stop bit, and no parity bit. This is the default.
odd	Set for 7 data bits, 1 stop bit, and odd parity.
strip	Set to strip the parity bit from the data stream when it is received by the PortMaster.

Usage

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

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

Example

```
Command> set c0 parity none
Parity for port C0 changed from even to none
```

See Also

set *C0* **databits** - page 5-10
set *C0* **modem-type** *ModemName* - page 5-21
set *C0* **speed** - page 5-32
set *C0* **stopbits** - page 5-33

set *C0*|all prompt

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

> **set** *C0*|**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 **$hostname** is included in the login prompt, the hostname for the port is substituted for the string. Use the caret symbol (^) to designate new lines. The command **set** *C0* **prompt** returns the prompt to its default setting of **$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** *C0 message* and **set** *C0 prompt* must not exceed 224 characters.

Example

```
Command> set c0 prompt $hostname login:
New Login Prompt:
$hostname login:
For ports: C0
```

See Also

set host - page 5-15
set *C0* **message -** page 5-21
set *C0* **username** - page 5-35

set *C0* protocol

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

> **set *C0* 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 c0 protocol slip**
Protocol for port C0 changed from ppp to slip

See Also

set debug - page 14-6
set *C0* compression - page 5-9
set *C0* mtu - page 5-22

set *C0*|all rts/cts

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

> **set *C0*|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 c0 rts/cts on**
RTS/CTS flow control for port C0 changed from off to on

See Also

set *C0* **modem-type** *ModemName* - page 5-21
set *C0* **xon/xoff** - page 5-36

set *C0*|all security

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

> **set** *C0*|**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. Then, 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 c0 security on**
Security for port C0 changed from off to on

See Also

set authentication_server - page 3-28

set *C0*|all service_device

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

> **set *C0*|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	Allows **rlogin** connections to this port from the network.
telnet	Allows **telnet** connections to this port from the network.
Tport	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 c0 service_device portmaster
Device Service for port C0 changed from telnet to portmaster
```

See Also

set *C0* device - page 5-11
set *C0* host - page 5-15
set *C0* login - page 5-19

set *C0*|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*]

netdata	Uses the **netdata** login service.
portmaster	Uses the PortMaster login service to connect to **in.pmd** on the login host. This is the default.
rlogin	Uses remote login to connect to the login host.
telnet	Uses Telnet to connect to the login host.
Tport	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 c0 service_login telnet**
Login service for port C0 changed from portmaster to telnet

See Also

set *C0* **login -** page 5-19
set *C0* **modem-type** *ModemName* - page 5-21
set *C0* **service-device** - page 5-30
set telnet - page 3-25
telnet - page 2-42

set *C0*|all speed

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

> **set** *C0*|**all speed [1|2|3] 300|600|1200|2400|4800|9600|19200|38400|57600|76800|115200**

1|2|3	Indicates which of the three baud rates is being set: 1, 2, or 3. Default is 1.
300|600, and so on	Indicates the data terminal equipment (DTE) rate. Default is 9600bps.

Usage

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

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

Examples

```
Command> set c0 speed 115200
Speed for port C0 (1) changed from 9600 to 115200

Command> set c0 speed 2 115200
Speed for port C0 (2) changed from UNKNWN to 115200

Command> set c0 speed 3 115200
Speed for port C0 (3) changed from UNKNWN to 115200
```

See Also

set *C0* **modem-type** *ModemName* - page 5-21

set *C0*|all stopbits

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

> **set *C0*|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 c0 stopbits 1
Stop bits for port C0 changed from 2 to 1
```

See Also

set *C0* databits - page 5-10
set *C0* modem-type *ModemName* - page 5-21
set *C0* parity - page 5-26
set *C0* speed - page 5-32

set *C0*|all termtype

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

> **set *C0*|all termtype** *String*

String   Terminal type, 0 to 15 characters.

Usage

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

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

Example

```
Command> set c0 termtype vt100
Terminal Type for port C0 changed from    to vt100
```

See Also

set *C0* **login** - page 5-19
set *C0* **twoway** - page 5-34

set *C0* 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** *C0* **twoway** *Device* [**network dialin**|**dialout**|**twoway**]

twoway	The first use of the keyword **twoway** sets the port for both user login and device sharing—combining the commands **set** *C0* **login** and **set** *C0* **device**.
	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.
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** *C0* **host** command.

- Define a login service with the **set** *C0* **service_login** command.

- Define a device service with the **set** *C0* **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 c0 twoway /dev/ttyp0**
Port type for port C0 changed from Login to TwoWay(/dev/ttyp0)

See Also

set *C0* **device** - page 5-11
set *C0* **host** - page 5-15
set *C0* **login** - page 5-19
set *C0* **network twoway** - page 5-34
set *C0* **service_device** - page 5-30
set *C0* **service_login** - page 5-31

set *C0* **username|autolog**

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

> **set** *C0* **username|autolog** [*String*]

| *String* | 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 c0 autolog** without a value *String*.

Example

Command> **set c0 autolog posales**
Username for port C0 changed from off to posales

See Also

set *C0* **message** - page 5-21
set *C0* **prompt** - page 5-27

set *C0*|all xon/xoff

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

> **set** *C0*|**all xon/xoff on**|**off**

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

Usage

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

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

Example

Command> **set c0 xon/xoff off**
Xon/Xoff flow control for port C0 changed from on to off

See Also

set *C0* **rts/cts** - page 5-28

Modem Commands

The modem table commands in Table 5-3 are used to view and configure the modem table, which stores configuration information for external modems you commonly use.

Note – ComOS 4.0 and ComOS 4.1 do not support the **add modem**, **delete modem**, **show table modem**, and **show modems** commands for external modems. If you are running ComOS 4.0 and ComOS 4.1, you cannot use the commands in this section to configure external modems on asynchronous ports C0 and C1. Instead, you can attach a previously configured modem to the C0 or C1 ports. Although you cannot display the modem's settings with the **show modem** command, it will function if properly configured.

See also the following commands for modems attached to asynchronous ports:

- **attach** *C0*—see page 5-4

- **set** *C0* **cd**—see page 5-7

- **set** *C0* **group**—see page 5-14

- **set** *C0* **modem-type**—see page 5-21

Table 5-3   Modem Table Configuration

Command Syntax
add modem *ModemName(short) ModemName(long) Speed String*   - see page 5-37
delete modem *ModemName(short)*   - see page 5-38
show modem *ModemName*   - see page 5-39
show table modem   - see page 5-40

Note – When the console diagnostic switch is in the left (on) position, the PortMaster 4 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.

add modem

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

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

ModemName(short)   Abbreviated name used to identify the external modem. *ModemName* can be up to 16 characters.

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

Usage

Note – ComOS 4.0 and ComOS 4.1 do not support this command.

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 5-39
show table modem - page 5-40

delete modem

This command deletes an external modem 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

Note – ComOS 4.0 and ComOS 4.1 do not support this command.

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

Example

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

See Also

show modem - page 5-39
show table modem - page 5-40

show modem

This command shows configuration information on individual external 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 5-37
delete modem - page 5-38
show table modem - page 5-40

show table modem

This command displays a table listing the external 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 5-37
delete modem - page 5-38
show modem - page 5-39

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 virtual synchronous port on the PortMaster 4 as follows:

- ISDN Primary Rate Interface (PRI) ports *S0* on T1 or E1 lines configured for ISDN PRI service or fractional PRI service.

- T1 or E1 serial WAN ports *W1* on T1 or E1 lines configured for full T1 or E1, fractional T1 or E1, or channelized T1 or E1 service. These ports can be used for leased line, Frame Relay, ISDN, or switched 56Kbps connections.

You must use the *W1* designation to configure a synchronous WAN port and the *S0* designation to configure an ISDN PRI port.

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

Displaying Synchronous Port Information

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

- **ifconfig**—see page 2-9

- **show all**—see page 2-19

- **show arp**—see page 2-21

- **show netstat**—see page 2-32

- **show** *S0*—see page 2-34

- **show sessions**—see page 2-37

- **show** *W1*

Summary of Synchronous Port Commands

The synchronous port commands in Table 6-1 configure synchronous ISDN 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**|**ipxdlci** *W1* Dlci [*Ipaddress*|*Ipxnode*]	- see page 6-3
•	**delete dlci**|**ipxdlci** *W1* *Dlci*	- see page 6-4
	reset *S0*|*W1*	- see page 2-13
	save ports	- see page 2-15
•	**set** *W1* **address** *Ipaddress*	- see page 6-5
•	**set** *W1* **annex-d** *Seconds*	- see page 6-5
	set *W1* **cd on**|**off**	- see page 6-6
	set *W1* **compression on**|**off**|**stack**|**vj**	- see page 6-7
•	**set** *W1* **crossbar-ip** *Ipaddress*	- see page 7-5
•	**set** *W1* **destination** *Ipaddress* [*Ipmask*]	- see page 6-8
	set *S0*|*W1* **extended on**|**off**	- see page 6-8
	set *S0*|*W1* **group** *Group*	- see page 6-9
	set *W1* **hangup on**|**off**	- see page 6-9
	set *W1* **idletime** *Number* [**minutes**|**seconds**]	- see page 6-10
•	**set** *W1* **ifilter** [*Filtername*]	- see page 6-10
•	**set** *W1* **ipxnet** *Ipxnetwork*	- see page 6-11
•	**set** *W1* **lmi** [*Seconds*]	- see page 6-12
•	**set** *W1* **mtu** *MTU*	- see page 6-13
•	**set** *W1* **netmask** *Ipmask*	- see page 6-13
	set *S0*|*W1* **network dialin**|**dialout**|**twoway**|**hardwired**	- see page 6-14
•	**set** *W1* **ofilter** [*Filtername*]	- see page 6-15
	set *W1* **ospf on**|**off**	- see page 8-7
•	**set** *S0*|*W1* **protocol slip**|**ppp**|**frame**|**x75-sync**	- see page 6-15
•	**set** *W1* **rip on**|**off**|**broadcast**|**listen**|**v2** {**broadcast**|**multicast**|**on**|**v1-compatibility**}	- see page 7-17
	set *W1* **route-filter incoming**|**outgoing** [*Filtername*]	- see page 7-8

Table 6-1 Synchronous Port Configuration *(Continued)*

Command Syntax	
set *W1* **speed 9600|14400|19200|38400|57600|76800|115200|** **56000|64000|1344k|1536k|2048k|t1|t1e|e1**	- see page 6-16
show all	- see page 2-19
show *W1*	- see page 6-17

Synchronous Commands

These commands affect the synchronous interface of the PortMaster. You must use *W1* to configure a synchronous WAN port and *S0* to configure an ISDN PRI port.

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

add *W1* dlci

This command adds data link connection identifiers (DLCIs) for Frame Relay service on a network hardwired synchronous port.

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

dlci	Use for IP connections.
Dlci	DLCI number, from 1 to 1023. You can add or delete only one DLCI number at a time.
ipxdlci	Use for IPX connections.
:*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 Local Management Interface (LMI) or Annex-D polling, 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 DCLI 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 – The PortMaster 4 supports IPX protocols on ComOS releases 4.1 and later.

Note – This command is used only for network hardwired synchronous ports.

Example

```
Command 1> add dlci w1 16 192.168.2.3
New dlci successfully added
```

See Also

add dlci - page 11-23
set *W1* **annex-d** - page 6-5
set *W1* **lmi** - page 6-12

delete *W1* dlci

This command deletes data link connection identifiers (DLCIs) for Frame Relay service on a network hardwired synchronous port.

   delete dlci|ipxdlci *W1 Dlci*

dlci	Use for IP connections.
ipxdlci	Use for IPX connections.
Dlci	DLCI number, from 1 to 1023. You can add or delete only one DLCI number at a time.

Usage

Note – The PortMaster 4 supports IPX protocols on ComOS releases 4.1 and later.

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 **add dlci** *W1* command.

Example

```
Command 1> delete dlci w1 16
DLCI successfully deleted
```

See Also

add dlci - page 11-23
set *W1* **annex-d** - page 6-5
set *W1* **lmi** - page 6-12

set *W1* address

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

> **set** *W1* **address** *Ipaddress*

Ipaddress   IP address in dotted decimal notation or hostname—a string of up to 39 characters.

Usage

If the local IP address of the port is set to 0.0.0.0 for PPP, the PortMaster uses the Ether0 IP address for this end of the serial link. If the address is set to 0.0.0.0 for Frame Relay, the port is disabled.

Note – This command is used only for network hardwired synchronous ports.

Example

```
Command> set w1 address 192.168.7.2
Port W1 local address changed from 0.0.0.0 to 192.168.7.2
```

See Also

set *C0* **address** - page 5-6

set *W1* annex-d

This command sets the Annex-D polling interval for a network hardwired synchronous port to allow the Frame Relay switch to monitor link status.

> **set** *W1* **annex-d** *Seconds*

Seconds   Keepalive interval in seconds, from 0 to 240. The default value is 10.

Usage

The Annex-D default value is 10 seconds. However, if your telephone company chooses another value, change this value as they instruct you. Enabling Annex-D (or LMI) causes the DLCI list to be completed automatically. Setting the interval to 0 (zero) seconds, or enabling LMI, disables Annex-D. You can display Annex-D activity using the **set debug 0x51** command.

Note – Check with your Frame Relay service provider to determine whether they use LMI or Annex-D; both can be referred to as LMI.

Note – This command is used only for network hardwired synchronous ports.

Example

```
Command> set w1 annex-d 10
ANNEX-D keepalive timer for S1 changed from 0 to 10
```

See Also

set debug - page 14-6
set *W1* **lmi** - page 6-12

set *W1* cd

This command enables the PortMaster to monitor the presence of the data carrier detect (DCD) signal on a modem attached to a 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 1> set w1 cd on
CD required for port W1 changed from off to on
```

See Also

set *C0* **cd** - page 5-7

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. This is the default.

off   Disables compression.

stac   Enables Stac LZS data compression only.

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 1> set w1 compression on
Compression for port w1 changed from off to on
```

See Also

set location compression - page 11-6
set *C0* **compression** - page 5-9
set user compression - page 10-6

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 hostname—a string of up to 39 characters. Enter the IP address of the remote router in dotted decimal notation.
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 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 1> set w1 destination 255.255.255.255
Port W1 destination changed from 0.0.0.0 to 255.255.255.255
```

See Also

set *C0* **destination** - page 5-10

set *S0|W1* extended

This command sets the extended mode on or off for the synchronous port.

> **set** *S0|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 *S0|W1* **group**

This command assigns synchronous ports to pools for use by V.25bis dial-out locations.

set *S0|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 11-7 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 11-7
set *C0* **group** - page 5-14

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 2-13

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 6-6

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 12-3
set *W1* **ofilter** - page 6-15
show table filter - page 12-18

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

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 OXC009C801**
Port W1 ipxnet changed from 00000000 to OXC009C801

See Also

set *Ether0* **ipxnet** - page 4-8
set ipx on - page 3-13
set *C0* **ipxnet** - page 5-18

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 14-6
set *W1* **annex-d** - page 6-5

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 6-15

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 7-7
set *C0* **netmask** - page 5-23

set *S0|W1* **network**

This command sets the network type for the synchronous port.

set *S0|W1* **network dialin|dialout|twoway|hardwired**

dialin	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.
	A remote host can connect to the port. This setting is used for ISDN or switched 56Kbps connections.
dialout	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.
	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.
twoway	The port accepts dial-in network connections, as well as being available for dial-out to remote destinations.
hardwired	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 an RJ-45 cable. Refer to the *PortMaster 4 Installation Guide* for more information. You must also set the remote destination address with **set** *W1* **destination**.

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 *C0* **network** - page 6-14

set *S0|W1* ofilter

This command sets a packet filter for packets exiting the PortMaster on a network hardwired synchronous port.

> **set** *S0|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 12-3
set *W1* **ifilter** - page 6-10
show table filter - page 12-18

set *S0|W1* protocol

This command sets the transport protocol for a network hardwired synchronous port.

> **set** *S0|W1* **protocol slip|ppp|frame|x75-sync**

slip	SLIP protocol.
ppp	PPP. Used for leased lines, ISDN, and switched 56Kbps connections.
frame	Frame Relay.
x75-sync	X.75 Protocol.

Usage

Select PPP for direct leased line connections between routers, for ISDN, or for switched 56Kbps. Select Frame Relay when attaching the port to a Frame Relay network via a Frame Relay switch.

Note – This command is used only for network hardwired synchronous ports.

Example

```
Command> set w1 protocol ppp
Protocol for port W1 changed from frame relay to ppp
```

See Also

set debug - page 14-6
set *W1* **annex-d** - page 6-5
set *W1* **lmi** - page 6-12

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 so on	Indicates DTE rate in bits per second.
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 *C0* **speed** - page 6-16

show *W1*

Shows the current status and configuration for synchronous WAN ports on the PortMaster 4.

show *W1*

Example

```
Command> show w70
---------------------- Current Status - Port W70 ----------------------
        Status:  ESTABLISHED
         Input:  507781                   Abort Errors:  0
        Output:  882686                     CRC Errors:  0
       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
   Modem Control:  off
      Interface:  Unassigned (FRM,Listen) (FRM,Routing)
            Mtu:  1500                    0
     Dial Group:  0
      IP DLCI's:  DLCI                    Address
                  ------                  -----------
                  16                      192.168.1.2
```

Explanation

Status	State of the port. Refer to the information on port status in Table 2-3 on page 2-20.
Input/Output/ Pending	Number of bytes input, output, or pending since last reboot.
TX Errors	Number of transmission errors since last reboot.

Abort Errors	Number of abnormal termination errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—**framing errors/device errors**:
	Framing errors—This count increments when the receiver chip reports either a framing error or an abnormal termination.
	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.
CRC Errors	Number of cyclic redundancy check (CRC) errors occurring since last reboot.
Overrun Errors	Number of overrun errors occurring since last reboot.
Frame Errors	Number of frame errors occurring since last reboot. A slash (/) in this field indicates two separate error counts—**short frame errors/large frame errors**:
	Short frame errors—This count increments when a short frame is received.
	Large frame errors—This count increments when a packet is too large and must be dropped.
Modem Status	The plus signs (+) on DCD and CTS indicate that the DCD and CTS signals on the port are asserted (high).
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 5-29.
Line Speed	Ext. indicates external line speed in kilobits per second.
Modem Control	Modem carrier detect signal setting.
Remote Host	IP address of remote host. If the destination address is set to 255.255.255.255 for PPP connections, the PortMaster attempts to learn the remote IP address.
Netmask	The netmask of the local network.
Interface	The interface specification used by the port.
Mtu	The maximum transmission unit (MTU) set for the port.
Dial Group	The dial group number allocated to the port.

See Also

show *S0* **-** page 2-34

Basic Routing 7

This chapter describes the commands you use to configure the PortMaster 4 for static and default routing, the Routing Information Protocol, versions RIP-1 and RIP-2, 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 8, "OSPF Routing," and Chapter 9, "BGP Routing."

Displaying Routing Information

To display routing information on the console, use the following commands:

- **show ipxroutes**

- **show routes**

- **show route to-dest**

- **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)

- RIP-1 and RIP-2

- Route filters

- Route propagation from one routing protocol into another

- Netmask tables

Table 7-1   Routing Commands

Command Syntax	
add route *Ipaddress*[*/NM*] *Ipaddress(gw) Metric*	- see page 7-13
add ipxroute *Ipxnetwork Ipxgateway:Ipxhost Metric Ticks*	- see page 7-12
add netmask *Ipaddress Ipmask*	- see page 7-21

Table 7-1   Routing Commands *(Continued)*

Command Syntax	
add propagation *Protocol(src) Protocol(dest) Metric Filtername*	- see page 7-3
add route *Ipaddress*[*/NM*] *Ipxgateway:Ipxhost Metric*	- see page 7-13
delete ipxroute *Ipxnetwork*	- see page 7-14
delete netmask *Ipaddress*	- see page 7-22
delete propagation *Protocol(src) Protocol(dest)*	- see page 7-3
delete route *Ipaddress*[*/NM*]	- see page 7-15
reset propagation	- see page 7-5
save netmask	- see page 7-22
save route	- see page 7-15
set debug rip|**rip-detail on**|**off**	- see page 14-12
set default on|**off**|**broadcast**|**listen**	- see page 7-16
set *Ether0*|*W1*|**user** *Username*|**location** *Locname* **crossbar-ip** *Ipaddress*	- see page 7-5
set *Ether0*|*C0*|*W1* **netmask** *Ipmask*	- see page 7-7
set *Ether0*|*C0*|*W1*|**user** *Username*|**location** *Locname* **rip on**|**off**|**broadcast**|**listen**|**v2** {**broadcast**|**multicast**|**on**| **v1-compatibility**}	- see page 7-17
set *Ether0*|*C0*|*W1*|**user** *Username*|**location** *Locname* **rip cost**	- see page 7-19
set *Ether0*|*C0*|*W1*|**user** *Username*|**location** *Locname* **route-filter incoming**|**outgoing** *Filtername*	- see page 7-8
set gateway *Ipaddress* [*Metric*]	- see page 7-11
set rip-password *Password*|**none**	- see page 7-20
set user-netmask on|**off**	- see page 7-11
show ipxroutes	- see page 7-23
show propagation	- see page 7-24
show routes [*String*|*Prefix/NM*]	- see page 7-24
show route to-dest *Ipaddress*	- see page 7-26
show table netmask	- see page 7-27

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.

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

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

Protocol(src)	Designates the source protocol of the route. Use one of the following keywords:
	• **rip**
	• **static**
	• **ospf**
	• **bgp**
Protocol(dest)	Designates the destination routing protocol for the route propagation. Use one of the following keywords:
	• **rip**
	• **static**
	• **ospf**
	• **bgp**
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.
Filtername	IP access filter added to the filter table with the **add filter** command and configured with the **set filter** command for use in the propagation rule.

Caution – If you plan to use a constant metric instead of the automatically generated metric provided by the ComOS, then you run the risk of creating routing loops if you do not provide for filters or policies to screen the route information that the PortMaster accepts from each routing protocol.

Usage

Use the **add propagation** command to create or modify an entry. See "Modifying a Propagation Rule" later in this section for modification instructions. Use the **delete propagation** command to delete an entry.

The **add propagation** command allows routes coming from one protocol to be advertised into another, based on the filter specified in the rule. The filter is a familiar IP access filter that uses the source address(es) specified in the filter to indicate the routes.

BGP-to-OSPF or BGP-to-RIP Propagation. You must explicitly configure the **add propagation** command to enable BGP routes to be propagated into OSPF or RIP.

Static-to-BGP Propagation. When static routes are the source protocol and BGP is the destination protocol, you need no other routing protocol. This combination allows the automatic, immediate advertisement into BGP of any configured static routes or static routes learned via RADIUS. This type of configuration is useful 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 12-3
set *Ether0* **ospf accept-rip on** - page 8-6
set filter - page 12-5

reset propagation

This command resets the propagation rules system.

> **reset propagation**

Usage

This command must be used each time the propagation filters are changed. If the propagation affects OSPF or BGP, use the commands **reset ospf** or **reset bgp**, respectively.

Example

```
Command> reset propagation
Propagation rules reset
```

See Also

reset bgp - page 9-8
reset ospf - page 8-5

set *Ether0|W1* crossbar-ip

This command enables the crossbar IP feature on the specified interface or for a specified location (destination) or user.

> **set** *Ether0|W1|***user** *Username|***location** *Locname* **crossbar-ip** *Ipaddress*

Ether0	Ethernet interface. For a list of configurable Ethernet interfaces see page 4-3. To activate crossbar IP configuration, you must also use the **reset slot***Slotnumber* command.
W1	Network hardwired synchronous port. You must first select the slot associated with the port using the **set view** command. To activate the new crossbar IP setting, you must reset the port.
Username	Network user in the user table. Configures the crossbar IP feature on the user profiles of a network user on the PortMaster user table.
	You can also configure a crossbar IP address for a user via RADIUS. If both are configured, the PortMaster uses the local user table by default.
	The new crossbar IP setting is activated the next time the user connects.

Location	Dial-out location or Frame Relay subinterfaces in the location table.
	The crossbar IP setting takes effect the next time the location is used.
Ipaddress	IP address of the next hop for all packets leaving the interface. Enter the IP address in dotted decimal notation or the hostname—a string of up to 39 characters.

Usage

The PortMaster 4 supports IP crossbar on ComOS 4.1 and later releases.

Use the crossbar IP address to specify the next hop destination of packets leaving the specified interface. The PortMaster 4 selects the next hop address chosen in the following order of priority:

1. Crossbar IP address, if specified

2. IP pool range gateway address, if specified

3. IP pool gateway address, if specified

4. PortMaster routing table

To disable the crossbar IP address on an interface, use the address 0.0.0.0.

When crossbar IP is enabled on an interface, the output from the **ifconfig** command displays **CROSSBAR** next to interface. You do not have to configure named IP pools to use the IP crossbar feature.

Note – To use the crossbar IP feature, you must also add corresponding RADIUS attribute **194** to the RADIUS dictionary file. The attribute for crossbar IP is expressed as an IP address in dotted decimal notation.

Examples

```
Command> set ether1 crossbar-ip 149.198.96.78
Changing crossbar ip address from 0.0.0.0 to 149.198.96.78

Command 2> set w70 crossbar-ip 192.168.123.4
Changing crossbar ip address from 0.0.0.0 to 192.168.123.4

Command 2> set location krabappel crossbar-ip 192.168.96.69
Changing crossbar ip address from 0.0.0.0 to 192.168.96.69

Command> set user skinner crossbar-ip 192.168.1.2
Changing crossbar ip address from 0.0.0.0 to 192.168.1.2
```

See Also

reset slot*Slotnumber* - page 3-5
set ippool - page 3-10
set ippool default - page 3-12

set *Ether0|C0|W1* **netmask**

This command sets the IP netmask for a specified interface.

> **set** *Ether0|C0|W1|***user** *Username|***location** *Location* **netmask** *Ipmask*

Ether0	Ethernet interface. See page 4-3 for more information.
C0	Network hardwired asynchronous port.
W1	Network hardwired synchronous port.
Username	User from the user table.
Locname	Location from the location table.
Ipmask	IP netmask in dotted decimal notation.

Example

```
Command> set c0 netmask 255.255.255.0
C0 netmask changed from 0.0.0.0 to 255.255.255.0
```

See Also

set *Ether0* **address** - page 4-3
set location netmask - page 11-15
set user netmask - page 10-14

set *Ether0|C0|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 "BGP Routing" on page 9-1 for details on the **add bgp policy** and **set bgp policy** commands.

> **set** *Ether0|C0|W1|***user** *Username|***location** *Locname* **route-filter**
> **incoming|outgoing** [*Filtername*]

Ether0	Ethernet interface that the route filter is applied to. See page 4-3 for more information.
C0	Asynchronous port that the route filter is applied to.
W1	Synchronous port that the route filter is applied to.
Username	User from the user table.
Locname	Location from the location table.
incoming	Inbound filter.
outgoing	Outbound filter.
Filtername	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 *Filtername* 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. See Table 7-2 for more information.

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 7-2   The Effect of Protocol on Route Filters

Protocol	Inbound Route Filter—Route Injection	Outbound Route Filter—Route Advertisement
RIP	The filter permit/deny rule applies and determines which routes are placed into the PortMaster routing table when • 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. For RIP, the advertiser is the next-hop (direct) advertiser of the information.	The destination addresses in the filter determine which routes are advertised out of this interface.
OSPF	The filter permit/deny rule applies and determines which routes are placed into the routing table when • 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. 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. 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.	The filter is ignored. OSPF area flooding rules make the definition of outbound route filters impractical on a per-interface basis. 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 7-3 for details.

Examples

1. The following example disables an outbound route filter on the *W1* interface:

```
Command> set w1 route-filter outgoing
Outgoing route filter on W1 disabled
```

2. The following example changes the inbound route filter on the *W1* interface:

```
Command> set w1 route-filter incoming inb
Incoming route filter for port W1 changed from ina to inb
```

3. 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 12-3
reset ospf - page 8-5
set bgp policy (advertisement) - page 9-24
set bgp policy (injection) - page 9-21

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 7-24

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

Because ComOS supports variable-length subnet masks (VLSMs), you do not have to use the same netmask for all subnets of a network.

If the user netmask is set to **off,** the PortMaster 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 must 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 7-13
set user netmask - page 10-14

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.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

> **add ipxroute** *Ipxnetwork Ipxgateway***:***Ipxhost Metric Ticks*

Ipxnetwork	Destination IPX network number. A 32-bit hexadecimal number.
*Ipxgateway***:** *Ipxhost*	Gateway IPX address in the following format: IPX gateway and IPX host address separated by a colon (:).
Metric	Hop count to the remote destination. An integer from 1 to 15.
Ticks	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 7-14
show ipxroutes - page 7-23

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 RIP-2 or the OSPF routing protocol instead of a netmask table for most routing configurations. The PortMaster supports RIP-2 on ComOS 4.1 and later releases.

> **add route** *Ipaddress*[*/NM*] *Ipaddress*(*gw*) *Metric*

Ipaddress	Destination address or network.
/NM	Netmask—a number from 1 to 32 preceded by a slash (/)—for example, /24.
Ipaddress(gw)	Gateway IP address.
Metric	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 7-21
add user-netmask - page 7-11
delete route - page 7-15
show ipxroutes - page 7-23

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.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Example

Command> **delete ipxroute 192.168.1.32/27**
Route successfully deleted

See Also

add ipxroute - page 7-12
show ipxroutes - page 7-23

delete route

This command deletes a static route from the PortMaster IP static route table.

>   **delete route** *Ipaddress*[*/NM*]

Ipaddress	Destination IP address.
/NM	Netmask—a number from 1 to 32 preceded by a slash (/)—for example, /24.

Usage

Only static routes can be deleted. Use this command only when the routing entry is unique.

Examples

```
Command> delete route 192.168.7.0/24 192.168.7.1
Route successfully deleted
```

See Also

add route - page 7-13

save route

This command writes the current PortMaster static IP and IPX route tables to the nonvolatile memory of the PortMaster.

>   **save route**

Usage

save all can also be used.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Example

```
Command> save route
Static route table successfully saved
New configurations successfully saved.
```

RIP Commands

[4.1] ComOS 4.1 and later releases support both RIP-1 and RIP-2 on the PortMaster 4. Earlier releases of ComOS support only RIP-1.

Unlike RIP-2 and OSPF, RIP-1 does not support variable length subnet masks (VLSMs). RIP-1 fails to propagate netmask information and next-hop addresses in its route information.

set default

When RIP is enabled, this command sets all PortMaster interfaces to send and listen for default route information.

> **set default on|off|broadcast|listen**

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

Usage

With this command set **on**, the PortMaster listens for default route information in RIP and OSPF messages, and if the PortMaster has a default route it is advertised to RIP and OSPF.

Example

```
Command> set default on
Default routing changed from off (no_broadcast,no_listen) to on (broadcast,listen)
```

See Also

set gateway *Ipaddress* - page 7-11
set rip - page 7-17
show global - page 2-26

set *Ether0|C0|W1|user|location* rip

This command enables RIP-1 or RIP2 parameters on a specified interface.

> **set** *Ether0|C0|W1|***user** *Username|***location** *Locname*
> **rip on|off|broadcast|listen|v2**
> {**broadcast|multicast|on|v1-compatibility**}

Ether0	Ethernet interface. For a list of configurable Ethernet interfaces see page 4-3.
C0	Console port—*C0* or *C1*—asynchronous ports.
W1	Network hardwired synchronous port.
user	Sets RIP-1 or RIP-2—options for a network user. If set to **on**, the PortMaster sends and listens for RIP packets to the interface established when this user logs in.
Username	Name of a network user.
location	Sets RIP-1 or RIP-2—options for a location.
	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** for 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.
Locname	Location name that is in the location table.
rip	Enables RIP-1 or RIP-2 on the interface. Use **rip** with one of the following options:

	on	The PortMaster sends RIP broadcasts and listens for RIP-1 packets on this interface.
	off	The PortMaster neither sends nor listens for RIP packets on this interface. This is the default for all interfaces.
	broadcast	The PortMaster sends RIP-1 updates on the interface's broadcast address every 30 seconds, and ignores RIP packets received on the interface.
	listen	RIP packets received on the interface are interpreted as RIP-1 updates. Any subnet mask or next-hop information is ignored.
4.1 ▷	**v2**	Enables RIP-2 on the interface. **v2** is used with one of the following options:
		broadcast—The PortMaster 4 sends RIP-2 updates using the interface's broadcast address every 30 seconds and ignores received RIP-1 and RIP-2—packets on the interface.

on—The PortMaster 4 sends RIP-2 updates every 30 seconds using multicast, and listens for RIP-1 updates on the multicast address, or on the interface's broadcast address.

multicast—The PortMaster 4 sends RIP-2 updates every 30 seconds using the multicast broadcast address 244.0.0.9. The PortMaster 4 does not use the Internet group management protocol (IGMP) when it sends RIP-2 packets because the updates are sent from router to router. Received RIP packets are ignored.

v1-compatibility—The PortMaster 4 sends RIP-2 updates on the broadcast address of the interface every 30 seconds. RIP-1 updates are listened for coming from the broadcast address.

Usage

4.1 >
Lucent Technologies supports RIP-2 on the PortMaster 4 running ComOS 4.1 and later releases.

This command enables the PortMaster to send and listen for RIP packets—and IPX RIP packets if IPX is enabled—on the specified interface. By default, if IPX is enabled, IPX RIP is enabled on the Ethernet interface.

Using this command without specifying any interface or port sets **ether0** by default. Normally, the PortMaster 4 sends RIP packets at least every 30 seconds. However, it may broadcast RIP packets sooner if it detects changes in routing information in nonvolatile RAM.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Examples

```
Command> set c0 rip on
Routing for port C0 changed from listen to on (broadcast,listen)

Command> set location hq rip on
hq routing changed from off to on (broadcast,listen)


  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

set debug rip|rip-detail - page 14-12
set default - page 7-16
set rip cost - page 7-19
set rip password - page 7-20

set rip cost

This command sets the RIP cost per interface.

> `4.1`

set *Ether0|C0|W1|***user** *Username|***location** *Locname* **rip cost** *Number*

Ether0	Ethernet interface. For a list of configurable Ethernet interfaces see page 4-3.
C0	Console port—*C0* or *C1*—asynchronous ports.
W1	Network hardwired synchronous port.
Username	Name of a network user.
Locname	Location name that is in the location table.
Number	Cost—integer between 0 and 16 that is added to the metric of RIP routes learned over the interface.

Usage

Lucnet Technologies implementation of RIP supports this command on the PortMaster 4 running ComOS 4.1 and later releases.

Example

```
Command> set ether1 rip cost 10
Routing for ether1 changed to RIP On (Broadcast, Listen) Cost 10
```

See Also

set debug rip|rip-detail - page 14-12
set default - page 7-16
set rip|v2 broadcast|listen|on|off - page 7-17
set rip password - page 7-20

set rip-password

This command sets the password for RIP-2 packets.

> **4.1**

set rip-password *Password*|**none**

Password	16-character password. The first character cannot be a question mark (?). If quotation marks (" ")are used to encapsulate the password, the quotation marks are dropped.
none	Removes the password. This is the default.
	Using **set rip-password** without any arguments also disables the password.

Usage

Lucent Technologies implementation of RIP-2 supports this command on ComOS 4.1 releases and later. This command prevents RIP packets from being accepted unless they are authenticated. Because the password is sent in the packet as clear text, no security is implied. If a password is set and the PortMaster 4 receives a RIP-1 or RIP-2 packet without the matching password, the packet is dropped.

Because authentication occupies the first route entry of every RIP packet sent, setting the RIP password adds 20 bytes of overhead for every 24 routes sent via RIP-2.

The RIP password is enabled as soon as it is configured.

Example

Command> **set rip-password test**
RIP Password Updated

See Also

set debug rip|**rip-detail** - page 14-12
set default - page 7-16
set rip|**v2 broadcast**|**listen**|**on**|**off -** page 7-17
set rip cost - page 7-19

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 4 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 and RIP-2 instead of using the netmask table and RIP-1. Lucent strongly recommends that 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 4 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-1. 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 7-22
save netmask - page 7-22
show table netmask - page 7-27

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 7-21
save netmask - page 7-22
show table netmask - page 7-27

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 7-21
delete netmask - page 7-22
show table netmask - page 7-27

Routing Information

The following commands display routing information on the console.

show ipxroutes

This command shows the IPX routing table.

show ipxroutes

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 and node.
Flag	• **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**

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 the 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:

	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	• **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 7-24

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 7-21
delete netmask - page 7-22
save netmask - page 7-22
set user-netmask - page 7-11
show routes - page 7-24

OSPF Routing 8

This chapter describes the commands you use to configure the PortMaster when using the Open Shortest Path First (OSPF) routing protocol. ComOS release 4.0 does not support dial-in and dial-out OSPF.

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 the *PortMaster 4 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 2-26

- **show memory**—see page 2-30

- **show propagation**—see page 7-24

- **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

The OSPF commands summarized in Table 8-1 allow you to configure the PortMaster to use the OSPF IP routing protocol.

Table 8-1   OSPF Commands

Command Syntax	
add ospf area *Area*	- see page 8-3
add propagation *Protocol(src) Protocol(dest) Metric Filtername*	- see page 7-3

Table 8-1　OSPF Commands *(Continued)*

Command Syntax	
add route *Ipaddress*[*/NM*] *IPaddress(gw) Metric*	- see page 7-13
delete ospf area *Area*	- see page 8-4
delete propagation *Protocol(src) Protocol(dest)*	- see page 7-3
ifconfig	- see page 2-9 and page 8-4
reset ospf	- see page 8-5
reset propagation	- see page 7-5
save ospf	- see page 8-5
set default on|**off**|**broadcast**|**listen**	- see page 7-16
set debug ospf on|**off**	- see page 14-11
set *Ether0* **ospf accept-rip on**|**off**	- see page 8-6
set *Ether0* **ospf on**|**off** [**cost** *Number*][**hello-interval** *Seconds*][**dead-time** *Seconds*]	- see page 8-6
set *Ether0*|*C0*|*S0*|*W1*|**user** *Username*|**location** *Locname* **route-filter in**|**out** [*Filtername*]	- see page 7-8
set *S0*|*S10*|*W1* **ospf on**|**off** [**cost** *Number*] [**hello-interval** *Seconds*][**dead-time** *Seconds*][**nbma**|**point-to-multipoint**|**wan-as-stub-ptmp**]	- see page 8-7
set ospf area *Area* **external on**|**off**	- see page 8-9
set ospf area *Area* **md5** *Number String*	- see page 8-10
set ospf area *Area* **nssa on**|**off**	- see page 8-10
set ospf area *Area* **password** *String*	- see page 8-11
set ospf area *Area* **range** *Prefix*/*NM* [**advertise**|**quiet**|**off**]	- see page 8-12
set ospf area *Area* **stub-default-cost** *Number*	- see page 8-13
set ospf enable|**disable**	- see page 8-13
set ospf priority *Number*	- see page 8-14
set ospf router-id *Ipaddress*|*Number*	- see page 8-15
show ospf areas	- see page 8-15
show ospf links [**router**|**network**|**summary**|**external**|**nssa**]	- see page 8-18

Table 8-1 OSPF Commands *(Continued)*

Command Syntax	
show ospf neighbor	- see page 8-20
show propagation	- see page 7-24
show routes [*String*|*Prefix*/*NM*]	- see page 8-22
show table ospf	- see page 8-15

OSPF Commands

These commands are used for configuring OSPF routing protocol on the PortMaster. ComOS release 4.0 does not support dial-in and dial-out OSPF.

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*

Area   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 range - page 8-12

delete ospf area

This command deletes an area from the area table of the router.

> **delete ospf area** *Area*

Area   Area specified in decimal or dotted decimal notation.
                         A 32-bit number.

Example

```
Command> delete ospf area 0.0.0.0
Area successfully deleted
```

ifconfig

This command displays configuration values for all interfaces, and is described more fully on page 2-9. Examples of output are given here to illustrate how **ifconfig** shows OSPF state parameters for the interface, with the identity of the designated router (DR), backup designated router (BACKUP), and other (DROTHER) routers on the network.

> **ifconfig**

Examples

1. 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 ffffff00 broadcast 192.168.200.0
area 192.168.200.0 ospf-state DR mtu 1500
```

2. 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 ffffff00 broadcast 192.168.200.0
area 192.168.200.0 ospf-state BACKUP mtu 1500
```

3. 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 ffffff00 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. MD5 is the Message-Digest Algorithm from RSA Data Security, Inc., as defined in RFC 1321. 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**

Ether0   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**

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*]

Ether0   Ethernet interface. See page 4-3 for more information.

on   Enables OSPF on the Ethernet interface.

off   Disables OSPF on the Ethernet interface.

cost   Cost of sending a packet on the interface. This value is also known as the link state metric. The range is 0 to 15. Lower-cost routes are preferred.

Number	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 *S0|W1* **ospf**

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

> set *S0|W1* **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.

S0	Asynchronous port or ISDN PRI port—configured as a network hardwired port.
W1	Synchronous port—configured as a network hardwired port.
on	Enables OSPF on the selected interface.
off	Disables OSPF on the selected interface.
cost	Cost of sending a packet on the interface—also known as the link state metric.
Number	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.
nbma	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.
	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.
	This is the default behavior.
point-to-multipoint	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.
	If you set the port to this value, the partially meshed Frame Relay network is modeled as a series of **point-to-point** interfaces.
wan-as-stub-ptmp	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**.
	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.

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 8-18
show routes - page 8-22

set ospf area external

This command allows the propagation of external routes into the OSPF area.

> **set ospf area** *Area* **external on|off**

Area	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 8-10
set ospf area stub-default-cost - page 8-13

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*

Area	OSPF area address, specified in decimal or dotted decimal notation.
Number	Key ID number associated with the MD5 secret. An integer from 1 to 255.
String	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**

Area	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 8-13

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**]

Area	OSPF area address, specified in decimal or dotted decimal notation.
Prefix	IP prefix shared by all IP addresses within the range.
/NM	Netmask that indicates the number of high-order bits in an IP address that must match those in *Prefix* 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.

The maximum number of ranges for a single area supported by the PortMaster 4 is 8 if you are running ComOS 4.0 and 16 if you are running ComOS 4.1.

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*

Area	Address of the OSPF area being configured—specified in decimal or dotted decimal notation.
Number	Cost given to the default stub or NSSA route. This value is an integer from 0 to 15. Lower-cost routes are preferred. Setting *Number* 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 8-9
set ospf area nssa - page 8-10

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, 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.

Example

Command> **set ospf priority 1**
OSPF priority changed from 5 to 1

set ospf router-id

This command sets the OSPF router address or ID number.

set ospf router-id *Ipaddress|Number*

Ipaddress	The OSPF router address, specified in decimal or dotted decimal notation. If the router address is set to 0.0.0.0, it defaults to the router's Ethernet address.
Number	A 32-bit number in decimal format. If the router address is set to 0, it defaults to the router's Ethernet address.

Usage
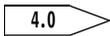
4.0 The PortMaster 4 propagates OSPF neighbor information as all zeroes when Ether0 has no IP address configured. Use the **set ospf router-id** command to ensure that correct information is propagated.

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 8-14

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.**

    ```
    Command> show ospf areas
                                      Authentication                      Stub
                                                           External       Default
    Area           Network Range     Type      ID   Key    Routes         Cost
    -----------    ---------------   --------- ---  ------  --------       -------
    192.168.96.0   192.168.96.0/24   Password       abcd   Yes            N/A
                   172.16.1.0/24
                   192.168.1.0/24
    ```

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
                                      Authentication                      Stub
                                                           External       Default
    Area           Network Range     Type      ID   Key    Routes         Cost
    -----------    ---------------   --------  ---  ------  --------       -------
    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
                                      Authentication                      Stub
                                                           External       Default
    Area           Network Range     Type      ID   Key       Routes      Cost
    -----------    ---------------   -------   ---  --------   --------    -------
    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
                                    Authentication                        Stub
                                                            Area          Default
Area           Network Range       Type    ID   Key        Type          Cost
-----------    ---------------     ------  ---  --------    --------      -------
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 8-12). 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 8-11, and the **set ospf area md5** command on page 8-10.

External Routes	Indicates if external routes are flooded into this area. A **No** value indicates that the area is a stub area. A **Yes** value indicates that the area is a transit area. See the **set ospf area external** command on page 8-9.
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       Sequence      TOS    Ext    Age
                 Router
  ------------   -----------------  ------------  ----   ----   ----
  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
```

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
Network Links for Area 0.0.0.0						
------------	-----------------	------------	----	----	----	-----
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

Link ID	Advertising Router	Sequence	TOS	Ext	Age	Mask
Summary Links from others for Area 0.0.0.0						
-------------	-----------------	------------	----	----	----	-----
192.168.64.19	192.168.1.64	0x80000f2a	No	No	305	N/A
192.168.64.100	192.168.1.64	0x80000f19	No	No	305	N/A
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       Sequence      TOS    Ext    Age    Mask
               Router

-------------  ----------------  ------------  ----   ----   ----   -----


External Links for All Areas
Link ID        Advertising       Sequence      TOS    Ext    Age    Mask
               Router

-------------  ----------------  ------------  ----   ----   ----   -----
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 2328.
Ext	External—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 neighbors

This command shows information about routers directly accessible through your network interfaces.

show ospf neighbors

4.0   >   The PortMaster 4 propagates OSPF neighbor information as all zeroes when Ether0 has no IP address configured. Use the **set ospf router-id** command to ensure that correct information is propagated.

Example

```
Command> show ospf neighbors

                                                       Last   MD5
Interface   Area         Neighbor      State    Pri  IP Address    Hello  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   OSPF state of the neighbor. The possible states follow:

     Down   Either the link to the neighbor is down, or this router is currently not receiving hello packets from the neighbor.

     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.

     2Way   This router received a hello packet from the neighbor that indicates the neighbor has received a hello packet from this router.

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 8-4 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 8-10 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:

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

- **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 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.

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 2-26
- **show memory**—see page 2-30
- **show propagation**—see page 7-24
- **show bgp memory**
- **show bgp next-hop**
- **show bgp paths**
- **show bgp peers**
- **show bgp policy**
- **show bgp summarization**

Summary of BGP Commands

BGP commands, shown in Table 9-1, allow you to configure the PortMaster for BGP routing.

Table 9-1   BGP Commands

Command Syntax	
add bgp peer *Ipaddress(sr) Ipaddress(dest) ASN*	- see page 9-4
add bgp policy *Policyname*	- see page 9-5

Table 9-1   BGP Commands *(Continued)*

Command Syntax	
add bgp summarization *Prefix/NM*	- see page 9-5
add propagation *Protocol(src) Protocol(dest) Metric Filtername*	- see page 7-3
delete bgp peer *Ipaddress(dest)*	- see page 9-6
delete bgp policy *Policyname*|**all**	- see page 9-6
delete bgp summarization *Prefix/NM*	- see page 9-7
delete propagation *Protocol(src) Protocol(dest)*	- see page 7-3
reset bgp [**peer** *Ipaddress*]	- see page 9-8
reset propagation	- see page 7-5
save bgp	- see page 9-8
set bgp as *ASN*	- see page 9-9
set bgp cluster-id *Ipaddress*	- see page 9-9
set bgp cma *ASN*	- see page 9-10
set bgp connect-retry-interval *Seconds*	- see page 9-10
set bgp enable|**disable**	- see page 9-11
set bgp hold-time *Seconds*	- see page 9-11
set bgp id *Ipaddress*	- see page 9-12
set bgp igp-lockstep on|**off**	- see page 9-12
set bgp keepalive-timer *Seconds*	- see page 9-13
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**]}	- see page 9-13

Table 9-1   BGP Commands *(Continued)*

Command Syntax	
set bgp policy *Policyname* [**before**] *RuleNumber* **permit**|**deny**|**include** *Policyname* [**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*] [**local-pref** *Number*] [**output-multi-exit-disc** *Number*|**strip**] [**next-hop** *Ipaddress*] [**community add**|**replace**|**strip** *Tag*] [**ignore-community-restrictions**]]	- see page 9-17, page 9-21, page 9-24
set bgp policy *Policyname* **blank**	- see page 9-28
set bgp summarization *Prefix/NM* [**as** *ASN*] [**cms** *ASN*] [**multi-exit-disc** *Number*] [**local-pref** *Number*] [**community** *Tag*] [**all**]	- see page 9-29
set debug bgp on|**off**	- see page 14-2
show bgp memory	- see page 9-31
show bgp next-hop	- see page 9-32
show bgp paths [*Prefix/NM* [**verbose**]]	- see page 9-33
show bgp peers [**verbose**|**packets**]	- see page 9-36
show bgp policy [*Policyname*]	- see page 9-40
show bgp summarization	- see page 9-41
show routes [*String*|*Prefix/NM*]	- see page 9-42

BGP Commands

These commands are used for configuring the BGP routing protocol on the PortMaster 4.

Note – BGP is a complex protocol to configure. Consult the instructions and examples in the *PortMaster Routing Guide* before configuring BGP on a PortMaster 4.

`add bgp peer`

This command creates entries on the PortMaster for BGP peers.

> **add bgp peer** *Ipaddress(src) Ipaddress(dest) ASN*

Ipaddress(src)	Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.
Ipaddress(dest)	Destination address of the peer, specified in dotted decimal notation.

Usage

Adding or Changing Peer Parameters. The **set bgp peer** command permits you to specify the parameters for an existing BGP peer without deleting that peer. However, the command assumes a "clean slate" for all parameters, and requires that you reenter them completely. For example, supposing you want to change your configuration of a peer 192.168.1.5 configured with the following command:

add bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client always-next-hop accept all inject all

If you now want to add **advertise all** as a policy statement to the command, you must specify all the original parameters together with the new parameter in the **set bgp peer** command, as follows:

set bgp peer 192.168.1.1 192.168.1.5 105 route-reflector-client always-next-hop accept all inject all advertise all

See Also

set bgp peer - page 9-13
set bgp policy (acceptance) - page 9-17
set bgp policy (injection) - page 9-21
set bgp policy (advertisement) - page 9-24

add bgp policy

This command creates a BGP policy for route acceptance, injection, or advertisement.

> **add bgp policy** *Policyname*

Policyname Name of the policy to be created or deleted—a string of up to 16 nonspace characters.

Usage

Use the **delete bgp policy** command to delete a BGP policy. Define BGP policies with the **set bgp policy** commands.

Example

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

See Also

delete bgp policy - page 9-6
set bgp policy (acceptance) - page 9-17
set bgp policy (injection) - page 9-21
set bgp policy (advertisement) - page 9-24

add bgp summarization

This command creates a BGP summarization entry.

> **add bgp summarization** *Prefix/NM*

Prefix Address prefix that you want to advertise to the BGP peers in dotted decimal notation.

/NM Netmask that indicates the number of high-order bits in the address prefix. This is a number from 1 to 32, preceded by a slash (/)—for example, /24.

See Also

set bgp policy - page 9-17

delete bgp peer

This command deletes existing BGP peer entries on the PortMaster.

> **delete bgp peer** *Ipaddress(dest)*

Ipaddress(src)	Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.
Ipaddress(dest)	Destination address of the peer, specified in dotted decimal notation.

Usage

When a peer deletion is in process, the message and countdown timer "Deletion in Progress. Countdown 216" are displayed in the Accept, Inject, and Advertise columns of the **show bgp peers** command. Deletion is complete when the countdown drops to zero.

Example

Command> **delete bgp peer 172.16.0.0**
BGP peer to 172.16.0.0 successfully deleted

See Also

add bgp peer - page 9-4
set bgp peer - page 9-13

delete bgp policy

This command deletes a BGP policy.

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

> **delete bgp policy** *Policyname*|**all**

Policyname	Name of the policy to be created or deleted—a string of up to 16 nonspace characters.
all	Predefined policy that you can use to permit all routes to be accepted, injected, or advertised.

Usage

Use the **add bgp policy** command to create a BGP policy. Define BGP policies with the **set bgp policy** commands.

Example

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

See Also

add bgp policy - page 9-5
set bgp policy (acceptance) - page 9-21
set bgp policy (injection) - page 9-21
set bgp policy (advertisement) - page 9-24

delete bgp summarization

This command deletes a BGP summarization entry.

> **delete bgp summarization** *Prefix/NM*

delete	Deletes an existing BGP summarization entry.
Prefix	Address prefix that you want to advertise to the BGP peers. Specified in dotted decimal notation.
/NM	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.

Example

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

See Also

add bgp summarization - page 9-5
set bgp policy – page 9-17
set bgp summarization - page 9-29

reset bgp

This command recreates startup conditions for BGP.

> **reset bgp** [**peer** *Ipaddress*]

peer	Resets only the session with the specified peer.
Ipaddress	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 re-establishes 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 save all configuration information, 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*

ASN   Unique number that identifies the autonomous system—a 16-bit number ranging from 1 to 65535.

Usage

Autonomous system identifiers are supplied by the Internet Network Information Center (InterNIC). If autonomous system confederations are in use, this number identifies your BGP confederation's autonomous system to BGP peers outside the confederation.

Example

```
Command> set bgp as 106
BGP AS number changed from 0 to 106
```

set bgp cluster-id

This command identifies the PortMaster as a BGP route reflector in a cluster.

> **set bgp cluster-id** *Ipaddress*

Ipaddress   IP address in dotted decimal notation. It can be any IP address, but is typically the BGP ID of one of the route reflectors. Setting the cluster ID to 0.0.0.0 removes it, and disables the ability of this PortMaster to be a route reflector.

Route reflection is disabled by default.

Usage

An autonomous system can be divided into many clusters. Each cluster contains one or more internal peers configured as route reflectors, with the remaining peers in the cluster called route reflector clients. Peers configured as route reflectors in an autonomous system are fully meshed with each other, but the clients are configured as peers only with route reflectors in their cluster.

The same cluster ID must be set on each route reflector in a cluster, but cluster IDs are not set on the reflector clients.

Advantages of Clustering. The use of clusters reduces the traffic and CPU overhead compared with a fully meshed system. When compared to confederations, route reflector clusters are simpler to configure, but do not allow the degree of policy control

that is possible across confederation boundaries. The primary advantage of route reflector clusters is that they allow the PortMaster to interoperate with BGP peers that are third-party routers without the ability to be configured into confederations.

For information about the effects of route reflection on BGP policies, see page 9-16.

Example

```
Command> set bgp cluster-id 1.2.3.4
BGP Cluster ID changed from 0.0.0.0 to 1.2.3.4
```

set bgp cma

This command sets the number of the BGP confederation member autonomous system (CMAS) that the PortMaster is in.

> **set bgp cma** *ASN*

ASN	The CMAS identifier—a 16-bit number ranging from 0 to 65535. A value of 0 disables the CMAS configuration. Confederations are disabled by default.

Usage

You can divide an autonomous system into multiple autonomous systems and group them into a single confederation. To external autonomous systems, the confederation appears as a single autonomous system. When confederations are in use, the PortMaster advertises this autonomous system identifier to BGP peers that are marked as confederation members in its configuration.

Choosing a value of zero disables use of confederations on this PortMaster. Confederations are disabled by default.

Example

```
Command> set bgp cma 120
BGP Confederation member AS number changed from 0 to 120
```

set bgp connect-retry-interval

This command sets the BGP connection retry interval for the PortMaster.

> **set bgp connect-retry-interval** *Seconds*

Seconds	Connection retry interval in seconds. The valid range is from 30 to 1000 seconds. The default is 120 seconds.

Usage

This command sets the interval at which the PortMaster attempts to open sessions to peers that are not fully established.

Example

```
Command> set bgp connect-retry-interval 180
BGP connect retry interval changed from 120 to 180
```

set bgp enable|disable

This command enables or disables the use of BGP on the PortMaster.

Note – You must issue the **save all** and **reboot** commands immediately after issuing the **set bgp enable** command, before you can continue with any other BGP configuration.

set bgp enable|disable

enable	Loads the BGP software upon the next PortMaster reboot.
disable	Disables the use of BGP upon the next reboot of the PortMaster, and frees the system memory used by BGP. This is the default.

Usage

You must enable BGP and reboot the PortMaster before configuring or using BGP. The **save all** and **reboot** commands must be issued after you use this command with either the **enable** or **disable** options.

set bgp hold-time

This command sets the BGP hold time interval for the PortMaster.

set bgp hold-time *Seconds*

Seconds	Hold time interval in seconds. The valid range is from 30 to 1000 seconds. The default is 90 seconds.

Usage

This command sets the interval that the PortMaster waits between keepalive, update, or notification messages from a peer, before identifying the peer as no longer operational and dropping all information learned from that peer.

Example

Command> **set bgp hold-time 120**
BGP hold time changed from 90 to 120

set bgp id

This command identifies the PortMaster as a BGP router.

> **set bgp id** *Ipaddress*

Ipaddress   PortMaster IP address, specified in dotted decimal notation.

Usage

The BGP identifier must be an IP address on the PortMaster. A setting of 0.0.0.0 removes the BGP ID.

Example

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 Interior Gateway Protocol (IGP) route—an OSPF, RIP, or static route, or a static route via RADIUS—that supports the route before advertising it. An IGP route supports a BGP route if it has the same IP address and prefix as the BGP route.

Note – Exact matches only are allowed because simple default routes to support BGP routes can lead to network instability or lost packets.

Example

Command> **set bgp igp-lockstep on**
bgp igp-lockstep changed from off to on

set bgp keepalive-timer

This command sets the BGP keepalive timer interval.

> **set bgp keepalive-timer** *Seconds*

Seconds	Keepalive timer interval in seconds. The valid range is from 30 to 1000 seconds. The default is 30 seconds.

Usage

This command sets the interval at which the PortMaster sends keepalive messages to its peers, to let them know it is still reachable.

Example

Command> **set bgp keepalive-timer 45**
BGP keepalive timer changed from 30 to 45

set bgp peer

This command modifies entries on the PortMaster for BGP peers, and provide options that control how policies are implemented for route selection.

> **set bgp peer** *Ipaddress(src) Ipaddress(dest) ASN*
> [**assume-default** [*Number*]] [**confederation-member**]
> [**route-reflector-client**] [**normal**] [**always-next-hop**]
> {**easy-multihome**|[**accept-policy** *Policyname*|**all**]
> [**inject-policy** *Policyname*|**all**] [**advertise-policy** *Policyname*|**all**]}

Ipaddress(src)	Local address of the PortMaster put in outgoing packets, specified in dotted decimal notation.
Ipaddress(dest)	Destination address of the peer, specified in dotted decimal notation.
ASN	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.
Number	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. *Number* 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	Enables a BGP policy *Policyname* 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 9-17), 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.

If not specified, and **easy-multihome** is not enabled for this peer, then nothing is accepted from this peer. |
| **all** | Predefined policy that you can use to permit all routes to be accepted, injected, or advertised. |
| *Policyname* | Name of a BGP policy statement defined by the **set bgp policy** command. |
| **inject-policy** | Enables a BGP policy *Policyname* 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.

If not specified, and **easy-multihome** is not enabled for this peer, then nothing is injected from this peer into the routing table. |
| **advertise-policy** | Enables a BGP policy *Policyname* 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.

If not specified, and **easy-multihome** is not enabled for this peer, then nothing is advertised to this peer. |

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.

Example

```
Command> set bgp peer 192.168.0.0 172.16.0.0 21 easy-multihome
New BGP peer successfully added
```

See Also

set bgp policy (acceptance) - page 9-17
set bgp policy (injection) - page 9-21
set bgp policy (advertisement) - page 9-24

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** *Policyname* [**before**] *RuleNumber*
> **permit|deny|include** *Policyname*
> [**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*]]

Policyname	Name of an acceptance policy already created.
before	Optionally inserts this BGP rule before an existing rule in the policy.
RuleNumber	Number of a rule in the policy.
	• Use the *RuleNumber* of an existing rule to replace that rule.
	• Add this rule to the end of the list of rules by using a *RuleNumber* value that is 1 greater than the current largest rule number.
	• A maximum of 160 rules is permitted in a policy. If more rules are needed, they can be added with the **include** *Policyname* 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 *Policyname*	Inserts an existing policy *Policyname* into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.
if	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.
	• 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 *Prefix*/*NM*	IP prefix *Prefix* and netmask *NM* to compare the prospective IP prefix against. 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.
	By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.
exactly	Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.
prefix-longer-than *NM*	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 *NM*.
as-path *String*	Autonomous system path *String* to compare the prospective IP prefix against.
	String is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.
	When *String* is compared to an autonomous system path **sequence**, the order of the sequence must match the order of *String*. When *String* is compared to an autonomous system path **set**, the **set** is put in ascending numerical order, and then matched against *String*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *String*.
	The following special characters have the following meaning in the expression:
	• An asterisk (*) matches one or more entries in the autonomous system sequence.
	• A question mark (?) matches any single item in the autonomous system sequence.
empty	Value for *String* that matches only paths containing no autonomous system path information.
	Use **as-path empty** only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.
community	Identifier *Tag* that categorizes a group of destinations to compare the prospective IP prefix against.
	See RFC 1997 for more information on a BGP community.

Tag	32-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, injection and advertisement policies.

Performing Three Functions in One Policy. You can create separate policies for each function, or create one policy to perform all three functions.

Permitting or Denying All Prefixes. If you define a rule that contains no **if** or **then** clauses, the rule universally permits or denies all prefixes, with no modification.

Applying and Saving a Rule. After adding or changing a rule in a BGP policy, use one of the following commands to apply and save the modified policy:

- Use **reset bgp peer** *Ipaddress(dest)* to reset only those peers that use a policy.

- Use **reset bgp** to reset all peers.

Removing a Rule. Specifying only the rule number *RuleNumber* in the command, as in **set bgp policy policyname 1**, removes that rule from the BGP policy.

Creating a Common Policy. You can create a common BGP policy for inclusion in other BGP policies. For example:

1. Create and define a common BGP policy as follows:

   add bgp policy permit1011

   set bgp policy permit1011 1 permit if prefix 10.0.0.0/8

   set bgp policy permit1011 2 permit if prefix 11.0.0.0/8

2. Include this policy by reference in another policy as follows:

   set bgp policy otherone 5 include permit1011

   This command inserts the statements of the **permit1011** policy at line 5 of the **otherone** policy.

Policy inclusions can be nested to a maximum depth of 10 levels. Any inclusions beyond the 10th level are ignored.

Reducing the Number of Advertised Routes. Some BGP routes received by your PortMaster might not be summarized. Unsummarized routes can include IP prefixes containing as many as 32 high-order bits—many specific addresses rather than fewer route summaries. If your BGP policy rules accept such routes into your BGP database, you can propagate extremely large numbers of routes to your BGP peers and possibly overwhelm them. To avoid this problem, use the **prefix-longer-than** keyword in a

BGP acceptance policy to deny IP prefixes with a netmask longer than a particular *NM* value. Specifying **prefix-longer-than** 16, for example, would be highly effective for this purpose.

For more information about the effects of route reflection on BGP policies, see page 9-16.

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*]]

Policyname	Name of an injection policy already created.
before	Optionally inserts this BGP rule before an existing rule in the policy.
RuleNumber	Number of a rule in the policy.
	Use the *RuleNumber* of an existing rule to replace that rule.
	Add this rule to the end of the list of rules by using a *RuleNumber* value that is 1 greater than the current largest rule number.
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 *Policyname*	Inserts an existing policy *Policyname* into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.

if	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.
	• 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 *Prefix/NM*	IP prefix *Prefix* and netmask *NM* to compare the prospective IP prefix against. 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.
	By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.
exactly	Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.
as-path *String*	Autonomous system path *String* to compare the prospective IP prefix against.
	String is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.
	When *String* is compared to an autonomous system path **sequence**, the order of the sequence must match the order of *String*.
	When *String* is compared to an autonomous system path **set**, the **set** is put in ascending numerical order, and then matched against *String*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *String*.
	The following special characters have the following meaning in the expression:
	• An asterisk (*) matches one or more entries in the autonomous system sequence.
	• A question mark (?) matches any single item in the autonomous system sequence.

empty	Value for *String* that matches only paths containing no autonomous system path information.
	Use **as-path empty** only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.
community	Identifier *Tag* that categorizes a group of destinations to compare the prospective IP prefix against.
	See RFC 1997 for more information on a BGP community.
Tag	32-bit number that indicates a destination category in one of the following forms:

• One 32-bit value identifying the autonomous system of the destination

• Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *Tag*, replace the second 16-bit value with the keyword **any**.

• One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:

no-export	**Destinations only within a confederation.** Advertise the route only to BGP peers within your confederation or autonomous system.
no-advertise	**No destinations.** Do not advertise this route.
no-export-subconfed	**Internal destinations only.** Advertise this route only to internal BGP peers.

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

Usage

A BGP **policy** is a list of rules that restrict the BGP routes your PortMaster accepts from its peers, uses, and advertises to its peers. You can use the **easy-multihome** alternative to policies—or **inject-policy all** to use all routes—when you add each BGP peer to your peer group, or you can define your own policies.

A PortMaster uses an **injection policy** to determine whether to add an IP prefix to its routing table, as shown in the output of the **show route** command. The PortMaster has already accepted this IP prefix for consideration as a BGP route via an **acceptance policy**. If the PortMaster injects the route, it will use the route to forward packets. The PortMaster also subjects the IP prefix to an **advertisement policy** to determine whether to share the route with its BGP peers.

An injection policy allows the PortMaster to receive and forward BGP routing information, but to forward packets based on simpler criteria. For example, you might want to forward packets only on routes received from OSPF or on a configured default route.

For more information about creating injection policies, see page 9-20.

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**]]

Policyname	Name of an advertisement policy already created.
before	Optionally inserts this BGP rule before an existing rule in the policy.
RuleNumber	Number of a rule in the policy.
	• Use the *RuleNumber* of an existing rule to replace that rule.
	• Add this rule to the end of the list of rules by using a *RuleNumber* value that is 1 greater than the current largest rule number.
permit	Allows the IP prefix to be advertised if the criteria in the rule are met.
deny	Prohibits the IP prefix from being advertised if the criteria in the rule are met.

include *Policyname* Inserts an existing policy *Policyname* into the current policy. Included policies can themselves include other policies, up to a maximum level of 10 nested included policies.

if 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.

- If all elements of the IP prefix match these **if** criteria, this rule is applied to the prefix and the prefix is either advertised or not advertised.

- If the elements do not match, the list of policy rules is further scanned for a matching rule.

- If no matches are found, the IP prefix is not advertised.

prefix *Prefix*/*NM* IP prefix *Prefix* and netmask *NM* to compare the prospective IP prefix against. 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.

By default, any prefix that matches the netmask in the rule prefix in the leftmost—most significant—bits, matches the rule prefix.

exactly Requires the entire prospective IP prefix and netmask to exactly match the IP prefix and netmask specified in the rule.

as-path *String* Autonomous system path *String* to compare the prospective IP prefix against.

String is a list of autonomous system numbers, separated by periods (.)—for example, AS1.AS2.AS3. or AS2.AS1.

When *String* is compared to an autonomous system path **sequence**, the order of the sequence must match the order of *String*. When *String* is compared to an autonomous system path **set**, the **set** is put in ascending numerical order, and then matched against *String*. Multiple sequences or sets in a single autonomous system path are concatenated before being compared to *String*.

The following special characters have the following meaning in the expression:

- An asterisk (*) matches one or more entries in the autonomous system sequence.

- A question mark (?) matches any single item in the autonomous system sequence.

empty	Value for *String* that matches only paths containing no autonomous system path information.
	Use **as-path empty** only to permit or deny routes originating from an internal or confederation member peer within the autonomous system of the PortMaster.
community	Identifier *Tag* that categorizes a group of destinations to compare the prospective IP prefix against.
	See RFC 1997 for more information on a BGP community.
Tag	32-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. For more information about creating injection policies, see page 9-20.

Examples

Command> **set 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 to be created or deleted—a string of up to 16 nonspace ASCII characters.

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 9-6
set bgp policy (acceptance) - page 9-17
set bgp policy (injection) - page 9-21
set bgp policy (advertisement) - page 9-24

set bgp summarization

This command modifies a BGP summarization entry that indicates how Interior Gateway Protocol (IGP) routing information from OSPF, RIP, or static routing is forwarded into BGP for advertisement to other BGP peers.

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

set	Modifies an existing BGP summarization entry. All settings need to be respecified.
delete	Deletes an existing BGP summarization entry.
Prefix	Address prefix that you want to advertise to the BGP peers in dotted decimal notation.
/NM	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.
ASN	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.

community	Advertises the 32-bit community attribute, defined by *Tag*, along with this summarization.
Tag	Thirty-two-bit number that indicates a destination category in one of the following forms:

- One 32-bit value identifying the autonomous system of the destination

- Two 16-bit values: one containing the autonomous system number of the destination, and the other containing additional information about the autonomous system. If only the first 16-bit word is considered significant in matching the community *Tag*, replace the second 16-bit value with the keyword **any**.

One of the following reserved community keywords that restrict route advertisement for peers receiving the route information:

no-export	**Destinations only within a confederation.** Advertise the route only to BGP peers within your confederation or autonomous system.
no-advertise	**No destinations.** Do not advertise this route.
no-export-subconfed	**Internal destinations only.** Advertise this route only to internal BGP peers.

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

Usage

BGP originates to peers only the routing information that is explicitly indicated by—and supported by—the interior routing protocols in use (OSPF, RIP, static routes, or directly attached routes). These special advertisements are called **summarizations**, and must be explicitly configured in most cases.

The settings you configure for community, local preference, and multiexit discriminator in this summarization command interact with advertisement policy definitions as follows:

- The advertisement policy definition overrides any values for local preference and multiexit discriminator.

- If the advertisement policy definition adds new community categories (**community add**), that information is added to the community information specified in the summarization.

- If the advertisement policy definition replaces community categories (**community replace**), it replaces any community information specified in the summarization.

To help provide stability in the Internet, summarizations are advertised only when supported by one or more specific routes that exist for at least 30 seconds before the advertisement.

Example

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

See Also

set bgp policy - page 9-17

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 the gateways to them.

> **show bgp next-hop**

Usage

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.

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

Next Hop	Next hop address, learned from the next hop attribute in a BGP route.
Gateway	Address of the directly adjacent router that forwards packets so that they reach the next hop. If the next hop and gateway addresses are the same, the next hop router is directly adjacent to the PortMaster.
Src Addr to it	Local network address of the interface on the PortMaster that is used to reach the next hop.
Source	Origin of the route information:

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

Metric	Hop count to the next hop.
Interface	Interface used for forwarding packets to the gateway for the next hop.

show bgp paths

This command displays BGP path information learned by the PortMaster.

> **show bgp paths** [*Prefix*/*NM* [**verbose**]]

Prefix	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.
/*NM*	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 Learned/Used:	Multiexit discriminator for this path that indicates a preference for a specific path when more than one exists. Both the learned multiexit discriminator 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.
	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 *A/B/C/D/E* 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 *A/B/C*:

> *A*   Autonomous system number—the first 16-bit portion of the communities attribute.
>
> *B*   Additional information about the autonomous system—the second 16-bit portion of the communities attribute.
>
> *C*   *A+B*—a single 32-bit number for the communities attribute.

| NLRI: | Network layer reachability information (NLRI), shown in the format +*Prefix/NM/BMAd/BMP*: |

> +   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.
>
> BMAd   Combined bit mask, in hexadecimal, of all peers that have advertised this NLRI and path to this PortMaster. The bit mask for each peer can be found in the output of **show bgp peers verbose**.
>
> BMP   Combined bit mask, in hexadecimal, of all peers to whom the PortMaster has advertised this NLRI for this path.

show bgp peers

This command displays a list of BGP peers and, optionally, a summary of packets sent to and received from the peers.

> **show bgp peers** [**verbose**|**packets**]

> **show table bgp**

verbose	Provides detailed information about BGP peers.
packets	Provides a summary of packets sent to and received from the peers.

Usage

Using the command without either optional keyword provides summary information. This is the default.

The command **show table bgp** displays the same output as **show bgp peers**.

Example 1—Summary Information

```
Command> show bgp peers
Remote IP       AS    Fl    DH    Up    Accept        Inject         Advertise
-------------   ---   ---   ---   ---   ------------  -------------  ----------
192.168.1.2     2     RN    2     Up    only207       only207        only207
192.168.1.3     3     C     --    Dn    all           all            all
```

Explanation

Remote IP	IP address of the BGP peer.
AS	Autonomous system number of the BGP peer.
Fl	Flags:

	C	Identifies this peer as a confederation member peer of the PortMaster.
	R	Identifies this peer as a route-reflector client of the PortMaster.
	N	This peer is configured to always consider the PortMaster as the next hop for any update packet sent from this peer.

DH	Hop count for the default route to this peer, if one is configured with the **assume-default** keyword.
Up	State of the peer:

	Up	Peer is in a fully established state.
	Dn	Peer is not in a fully established state.
Accept		Acceptance policy name, if configured.
Inject		Injection policy name, if configured.
Advertise		Advertisement policy name, if configured.

Note – When a peer deletion is in process, a message and countdown timer is displayed in the Accept, Inject, and Advertise columns, as follows:
    -- Deletion in Progress. Countdown 216 --
Deletion is complete when the countdown drops to zero. A similar "idling" message is shown when the peer is idling **down** from a previously established **up** state.

Example 2—Verbose Information

```
Command> show bgp peers verbose
Incoming Peer Source: 192.168.96.135    Destination: 192.168.96.130
Remote Autonomous System: 60149         Remote Id:    192.168.96.130
Current state: Established              Last Event: Received Update
Timer expiration in 64 seconds          Bitmask: 8
NLRI from/to this peer: 43839/ 43211    Peer up 10:40.80
Last sent error: 0/0. Last received error: 2/3.
Accept 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:

- 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 *hours:minutes.seconds*.

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
                        Open        Keepalive    Notification   Update      NLRI
Remote IP        Up     In/Out      In/Out       In/Out         In/Out      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 an existing policy for which you want details displayed—a string of up to 16 nonspace ASCII characters. 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 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	IP prefix and netmask of the route summary.
	/C—A configured summarization.
	/A—A summary automatically generated from static route information with the **add propagation static bgp** command.
Count of Supporting Routes	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.
LP:	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.

MED:	Configured multiexit discriminator to use when advertising this summary to external and confederation member peers.
CAS:	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.
Export to AS:	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.
Export to CMA:	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.

show routes

This command shows the IP routing table. For more information, see the explanation of routing tables in the *PortMaster Routing Guide*.

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

String	Displays only routes that contain the matching *String* in their **show routes** command output. For example, **show routes bgp** shows only routes that contain the string **bgp**.
Prefix/*NM*	Displays routes only to the destination indicated by this IP address prefix *Prefix* and netmask *NM*. The netmask indicates the number of high-order bits in the IP prefix.

- Specify *Prefix* in dotted decimal notation.

- Specify *NM* as number from 1 to 32, preceded by a slash (/)—for example, /24.

Example

```
Command> show routes bgp
Destination    Mask    Gateway         Source    Flag    Met    Interface
------------   -----   --------------  -------   -----   ----   ----------
0.0.0.0        0       172.31.96.129   bgp/D     ND      3      ether0
192.168.1.0    24      172.31.96.129   bgp/E     ND      1      ether0
172.16.0.0     16      172.31.96.130   bgp/I     ND      2      ether0
```

Explanation

Destination	IP address of the host or network to which packets are sent.
Mask	Netmask in use for the destination.
Gateway	IP address of the directly connected host through which packets are forwarded to the destination.
Source	Source of the route information:

	local	Route learned from an interface on the PortMaster.
	rip	RIP route learned from a connected network.
	ospf	OSPF route learned from an internal neighbor.
	ospf/E1 **ospf/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	• **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.

Users   10

This chapter describes how to use the command line interface to configure the PortMaster to authenticate dial-in users. The configuration settings are stored in 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 Settings," and the *RADIUS for UNIX Administrator's Guide* and *RADIUS for Windows NT 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 11, "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 user configuration, use the following commands:

- `show table user`

- `show user username`

Summary of User Commands

The commands in Table 10-1 configure the PortMaster to authenticate dial-in users. The **User Type** column in the table denotes commands for login users (L) and network users or **netusers** (N). RADIUS can also be used to authenticate dial-in users; however, the PortMaster consults its own user table first.

Table 10-1   User Configuration Commands

User Type	Command Syntax	
N	**add netuser** *Username* [**password** *Password*]	- see page 10-3
L	**add user** *Username* [**password** *Password*]	- see page 10-4
L/N	**delete user** *Username*	- see page 10-4
L/N	**save user**	- see page 10-5
N	**set user** *Username* **address|destination assigned|negotiated|***Ipaddress*	- see page 10-5
N	**set user** *Username* **compression on|off**	- see page 10-6
N	**set user** *Username* **crossbar-ip** *Ipaddress*	- see page 7-5
L/N	**set user** *Username* **dialback|callback** *Locname|String|***none**	- see page 10-7
L	**set user** *Username* **host default|prompt|***Ipaddress*	- see page 10-8
L/N	**set user** *Username* **idle** *Number* [**minutes|seconds**]	- see page 10-8
L/N	**set user** *Username* **ifilter** [*Filtername*]	- see page 10-9
N	**set user** *Username* **ipxnet** *Ipxnetwork*	- see page 10-10
N	**set user** *Username* **local-ip-address** *Ipaddress*	- see page 10-11
N	**set user** *Username* **map** *Hex*	- see page 10-12
L/N	**set user** *Username* **maxports** *Number*	- see page 10-13
N	**set user** *Username* **mtu** *MTU*	- see page 10-13
N	**set user** *Username* **netmask** *Ipmask*	- see page 10-14
N	**set user** *Username* **ofilter** [*Filtername*]	- see page 10-15
L/N	**set user** *Username* **password** *Password*	- see page 10-16
N	**set user** *Username* **protocol slip|ppp|x75-sync**	- see page 10-16
N	**set user** *Username* **rip on|off|broadcast|listen|v2** {**broadcast|multicast|on|v1-compatibility**}	- see page 7-17
L/N	**set user** *Username* **route-filter incoming|outgoing** [*Filtername*]	- see page 7-8

Table 10-1   User Configuration Commands *(Continued)*

User Type	Command Syntax	
L	**set user** *Username* **service** netdata|**portmaster**|**rlogin**|**telnet** [*Tport*]	- see page 10-17
L/N	**set user** *Username* **session-limit** *Minutes*	- see page 10-18
L/N	**show table user**	- see page 10-18
L/N	**show user** *Username*	- see page 10-19

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   Network username of 1 through 8 characters.

Password   Network user password of 0 through 16 characters.

Usage

A network user must be added to the user table before other netuser parameters can be configured. You cannot add network users with blank network usernames.

Example

Command> **add netuser jaime password 1mno+vwab**
New User successfully added

See Also

delete user - page 10-4

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	Login username of 1 through 8 characters. Usernames cannot begin with a quotation mark (") or a question mark (?).
Password	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 10-18

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.
Ipaddress	Uses the specified IP address, or hostname with a maximum of 39 characters. If *Ipaddress* 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 3-5

set user compression

This command sets Van Jacobson TCP/IP header compression and Stac LZS data compression for a network user.

> **set user** *Username* **compression on|off**

Username	Name of a network user.
on	Enables compression. The PortMaster tries to negotiate both Van Jacobson and Stac LZS compression. 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**

Username	Username of a login user or network user.
dialback|callback	Keywords **dialback** and **callback** are synonyms and generate the same result.
Locname	Network user location name that is in the location table. *Locname* must be between 1 and 12 characters in length.
String	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 *C0* **dialback_delay** - page 5-12

set user host

This command indicates the login host for the login user.

> **set user** *Username* **host default|prompt|***Ipaddress*

Username	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.
Ipaddress	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 host - page 5-15

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**]

Username	Name of a user.

idle *Number*	Timeout value from 0 to 240. The default value is 0.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.

Usage

If the idle time value is set to 0, the idle timer is disabled. If the value is set to 2 seconds or a longer interval, the user is disconnected after there is no traffic for the designated time.

You can set user idle timeout in the user table using this command, or you can use the RADIUS Idle-Timeout attribute. The RADIUS attribute is specified in seconds, but when greater than 240 seconds it is rounded up to minutes by the PortMaster.

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.

Example

```
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 10-18

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.

When a valid access control filter from the filter table is set for a login user, it restricts the hosts that the user can log in to 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 12-3
set user host prompt - page 10-8
set user ofilter - page 10-15

set user ipxnet

This command sets the IPX network number for the user's network connection.

   set user *Username* **ipxnet** *Ipxnetwork*

Username	Name of a network user.
Ipxnetwork	Number of IPX network to be used for a serial link—a 32-bit hexadecimal value.

Usage

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 3-5
set ipx on - page 3-13

set user local-ip-address

This command allows a network user to assert a local IP address on a PortMaster asynchronous or ISDN dialout port for a numbered IP network.

> **set user** *Username* **local-ip-address** *Ipaddress*

Username   Name of a network user.

Ipaddress   IP address. A hostname is not accepted.

Usage

Use this command only when a unique IP subnet is required for a point-to-point network connection—when both ends of the connection require an IP address.

This function is not available in RADIUS.

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 local-ip-address - page 3-14
set reported_ip - page 3-21
set user destination - page 10-5

set user map

This command sets the PPP asynchronous map to replace nonprinting ASCII characters found in the data stream.

> **set user** *Username* **map** *Hex*

Username	Name of a network user.
Hex	A 32-bit hexadecimal number. The default is 0x00000000.

Usage

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

The command **set user** *Username* **map 0** disables the asynchronous mapping.

Example

```
Command> set user joe map 0x00009000
          Username:  joe                     Type:  Dial-in Network User
           Address:  Negotiated           Netmask:  0.0.0.0
          Protocol:  PPP                  Options:  Quiet, Compression
               MTU:  1500               Async Map:  0x00009000
    Packet Filters:  student.in/student.out
```

set user maxports

This command, if set, limits the number of network dial-in ports the user can use on the PortMaster for Multilink V.120, Multilink PPP, and asynchronous multiline load-balancing.

> **set user** *Username* **maxports** *Number*

Username	Name of a user.
Number	Number between 0 and 95.

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 11-12

set user mtu

This command sets the size of 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 value 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 10-16

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 4 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 7-11

set user ofilter

This command sets the output packet filter for packets leaving the PortMaster on the interface established by this dial-in network user.

> **set user** *Username* **ofilter** [*Filtername*]

Username   Name of a network user.

Filtername   Output filter name. The maximum is 15 characters.

Usage

When an output packet filter is specified, packets being sent to the serial interface are evaluated against the rule set for this filter, which has been defined and is in the filter table. Only packets that are permitted by this filter are allowed to leave the PortMaster.

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

Note – This command does not apply to login users.

Example

```
Command> set user joe ofilter student.out
       Username:  joe                 Type:  Dial-in Network User
        Address:  Negotiated       Netmask:  0.0.0.0
       Protocol:  SLIP             Options:  Quiet, Compression
            MTU:  1006
 Packet Filters:  /student.out
```

See Also

add filter - page 12-3
set user ifilter - page 10-9

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 *CO* **network dialin** - page 5-23

set user service

This command selects the login service for the login user.

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

Username	Name of a login user.
netdata	Uses a **netdata** connection (TCP clear channel).
portmaster	Uses the PortMaster login service to connect to **in.pmd** on login host. This is the default.
rlogin	Uses the **rlogin** protocol to connect to the login host.
telnet	Uses Telnet to connect to the login host.
Tport	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 *CO* **service_login** - page 5-31

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.

Example

```
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 10-8

show table user

This command shows the current users in the user table.

> **show table user**

Example

```
Command> show table user

                                           Netmask/
Name    Type               Address/Host    Service          RIP
------  -----------------  ----------------  ---------------  ----
bill    Netuser            Assigned          ffffff00         No
hideo   Dialback User      default           Telnet
```

```
marie    Netuser         192.168.1.74        ffffffff        No
kwasi    Login User      default             PortMaster
jill     Netuser         Negotiated          ffffffff        Yes
```

See Also

show user - page 10-19

show user

This command shows the configuration of the specified user.

> **show user** *Username*

Username   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 10-18

This chapter describes how to use the command line interface to configure the PortMaster to recognize dial-out network connections (locations). The configuration settings are stored in the location table. Detailed command definitions follow a command summary table. A summary table and details for the data link connection identifier (DLCI) commands 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 dial-out locations:

- **show table location**
- **show location** *Locname*
- **dial** *Locname* **-x**—see page 2-6
- **ifconfig**—see page 2-9

Summary of Location Commands

The commands in Table 11-1 are used to configure the PortMaster for network dial-out.

DLCI commands begin on page 11-22.

Table 11-1   Location Configuration Commands

Command Syntax	
add location *Locname*	- see page 11-3
delete location *Locname*	- see page 11-3
save location	- see page 11-4
set location *Locname* **analog on|off**	- see page 11-4
set location *Locname* **automatic|manual|on_demand**	- see page 11-5
set location *Locname* **chap on|off**	- see page 11-6
set location *Locname* **compression on|off|stac|vj**	- see page 11-6
set location *Locname* **crossbar-ip** *Ipaddress*	- see page 7-5

Table 11-1 Location Configuration Commands *(Continued)*

Command Syntax	
set location *Locname* **destination** *Ipaddress*	- see page 11-7
set location *Locname* **group** *Group*	- see page 11-7
set location *Locname* **high_water** *Number*	- see page 11-8
set location *Locname* **idletime** *Number* [**minutes**|**seconds**]	- see page 11-9
set location *Locname* **ifilter** [*Filtername*]	- see page 11-9
set location *Locname* **ipxnet** *Ipxnetwork*	- see page 11-10
set location *Locname* **local-ip-address** *Ipaddress*	- see page 11-11
set location *Locname* **map** *Hex*	- see page 11-12
set location *Locname* **maxports** *Number*	- see page 11-12
set location *Locname* **mtu** *MTU*	- see page 11-13
set location *Locname* **multilink on|off**	- see page 11-14
set location *Locname* **netmask** *Ipmask*	- see page 11-15
set location *Locname* **ofilter** [*Filtername*]	- see page 11-15
set location *Locname* **password** *Password*	- see page 11-16
set location *Locname* **protocol** **slip|ppp|frame_relay|x75-sync**	- see page 11-17
set location *Locname* **rip on|off|broadcast|listen|v2** {**broadcast|multicast|on| v1-compatibility**}	- see page 7-17
set location *Locname* **route-filter incoming|outgoing** [*Filtername*]	- see page 7-8
set location *Locname* **script|v25bis** *RuleNumber* "*String1*" "*String2*"	- see page 11-18
set location *Locname* **telephone** *String*	- see page 11-19
set location *Locname* **username** *Username*	- see page 11-20
set location *Locname* **voice on|off**	- see page 11-21
show location *Locname*	- see page 11-21
show table location	- see page 11-22

Location Commands

These commands configure the location table of the PortMaster.

add location

This command adds a dial-out 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 11-3
save location - page 11-4
show table location - page 11-22

delete location

This command deletes a dial-out location from the location table.

> **delete location** *Locname*

Locname	Location name that is in the location table.

Example

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

See Also

add location - page 11-3
save location - page 11-4
show table location - page 11-22

save location

This command writes any changes in 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**

Locname	Location name that is in the location table.
on	Enables analog modem service on dial-out.
off	Disables analog modem service on dial-out, 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 11-21

set location automatic|manual|on_demand

This command modifies configuration parameters for the specified dial-out location.

set location *Locname* **automatic|manual|on_demand**

Locname	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 2-13
set location idletime - page 11-9

set location chap

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

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

Locname	Location name that is in the location table. The username and password entered in the location table are used as the system identifier and MD5 secret in the CHAP authentication.
on	CHAP authentication is negotiated for the specified location.
off	CHAP authentication is not supported for an outbound dial. This is the default.

Usage

The username and password entered in the location table are used as the system identifier and MD5 secret in the CHAP authentication. Use of this feature eliminates the need to use the system name and user table configurations for CHAP, unless the device being dialed also dials into the PortMaster.

See Also

set chap - page 3-7
set location password - page 11-16
set pap - page 3-19

set location compression

This command sets the use of Van Jacobson TCP/IP header compression and Stac LZS data compression for the dial-out location, improving interactive session performance.

> **set location** *Locname* **compression on|off|stac|vj**

Locname	Location name that is in the location table.
on	Enables both Van Jacobson and Stac LZS compression. This is the default.
off	Disables compression.
stac	Enables Stac LZS data compression only.
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. 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 *CO* **group** - page 5-14
set *SO|W1* **group** - page 6-9

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 11-7
set location maxports - page 11-12

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 dial-out location.

set location *Locname* **idletime** *Number* [**minutes**|**seconds**]

Locname	Location name that is in the location table.
Number	Timeout value from 0 to 255. The default value is 0.
minutes	Sets the idle time in minutes. This is the default.
seconds	Sets the idle time in seconds.

Usage

The idle timeout value is specified in minutes or seconds and can be any value from 0 to 255. It is for manual and on-demand locations.

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

If the value is set to 2 seconds or a longer interval, the connection is disconnected after having no traffic for the designated time. RIP packets are not counted as traffic.

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.

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 dial-out 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 for the changes take effect.

To remove the filter, enter 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 12-3
set location ofilter - page 11-15

set location ipxnet

This command sets the IPX network number for the point-to-point connection.

set location *Locname* **ipxnet** *Ipxnetwork*

Locname	Location name that is in the location table.
IPXnetwork	IPX network to be used for a serial link. A 32-bit hexadecimal value.

Usage

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 3-13

set location local-ip-address

This command allows a dial-out location to assert a local IP address on a PortMaster asynchronous or ISDN dialout port for numbered IP networks.

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

Locname	Location name that is in the location table.
Ipaddress	IP address or 39-character hostname.

Usage

Use this command only when a unique IP subnet is required for a point-to-point network connection—when both ends of the connection require an IP address. This command is not needed for typical PortMaster operation. If this value is not set, the PortMaster uses the IP address of the Ether1 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 11-7
set reported_ip - page 3-21

set location map

This command sets the PPP asynchronous map for a specified dial-out location.

> **set location** *Locname* **map** *Hex*

Locname	Location name that is in the location table.
Hex	A 32-bit hexadecimal number. The default is 0x00000000.

Usage

The PPP protocol supports the replacement of nonprinting ASCII data in the PPP stream. These characters are not sent through the line, but instead are replaced by a special set of characters that the remote site interprets as the original characters. The PPP asynchronous map is a bit map of characters that must be replaced. The lowest-order bit corresponds to the first ASCII character NUL, and so on. Most environments 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 95. 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 11-8
set location multilink - page 11-14

set location mtu

This command sets the size of the maximum transmission unit (MTU) for the dial-out 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 11-17

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**

Locname	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 11-8
set location maxports - page 11-12

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 4 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 dial-out 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 12-3
set location ifilter - page 11-9

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 11-6. 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 11-6
set location script - page 11-18
set location telephone - page 11-19
set location username - page 11-20

set location protocol

This command sets the protocol for encapsulating packets for the specified dial-out location.

set location *Locname* **protocol slip|ppp|frame_relay|x75-sync**

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

Usage

PPP can be used with either IP or IPX packet routing, or both.

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

Example

```
Command> set location hq protocol ppp
hq protocol changed to ppp
```

See Also

add dlci - page 11-23
set location mtu - page 11-13

set location script

This command sets up a dial script for dialing to a remote location.

set location *Locname* **script**|**v25bis** *RuleNumber* **"***String1***"** **"***String2***"**

Locname	Location name that is in the location table.
script	Enables a dial script for dial-out on an asynchronous port. The total length of all strings in the script must not exceed 256 characters.
v25bis	Enables a dial script for synchronous V.25bis protocol dial-out, for switched 56Kbps or ISDN.
RuleNumber	Rule number, from 1 up. Use rule number 99 to delete the script.
"*String1***"**	Send string of up to 30 characters, in quotation marks.
"*String2***"**	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** for information.

Usage

Each send string is sent from the PortMaster to the modem or remote host. When the expect string is matched against the input from the remote end, the next line in the send string is sent, and so on. When the last line in the script is finished, the PortMaster activates the data link protocol specified for this location. Therefore, the last entry in the dial command script must be an expect string indicating that the remote location is ready to begin receiving network packets.

Any printable ASCII character can be placed in the send or expect strings. In addition, the following special characters are available:

\r	ASCII carriage return. Send strings usually end with the **\r** character. Do not use **\r** in the send string for the V.25bis protocol.
\0XX	Replaced by the octal digit in the XX.
****	Replaced by a single backslash.

When you are connecting to a remote PortMaster, the final expect string to verify must be **SL/IP** for SLIP connections and **PPP** or a tilde (**~**) for PPP connections. A tilde is always the first character of a PPP frame. For other manufacturer's products, consult their manuals.

The dial script can also be used to implement outbound PAP authentication. If you specify a PAP username and password in the last line of the dial script, the PortMaster can be authenticated by the remote end using PAP. This capability is shown in the final example below.

Examples

Command> **set location hq script 1 "atdt18005551212\r" "CONNECT"**
New script entry successfully added.

Command> **set location hq script 2 "\r" "ogin:"**
New script entry successfully added.

Command> **set location hq script 3 "my_login\r" "ssword:"**
New script entry successfully added.

Command> **set location hq script 4 "my_password\r" "PPP"**
New script entry successfully added.

Command> **set location denver v25bis 1 "CRN7005552227" "=DCD="**
New script entry successfully added.

Command> **set location denver v25bis 2 "=PAP=my-login/my-password"**
New script entry successfully added.

See Also

set location password - page 11-16
set location telephone - page 11-19
set location username - page 11-20

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*

Locname	Location name that is in the location table.
String	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.

Example

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

See Also

set location password - page 11-16
set location script - page 11-18
set location username - page 11-20

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 11-6
set location password - page 11-16
set location script - page 11-18
set location telephone - page 11-19

set location voice

This command forces a data-over-voice call on an outbound ISDN connection to a specified dial-out location.

set location *Locname* **voice on|off**

Locname	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 11-3
set location analog - page 11-4
show location - page 11-21

show location

This command displays configuration information for a specified dial-out 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 2-19
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 commands in Table 11-2 configure the PortMaster to recognize data link connection
identifiers (DLCIs). You can split a Frame Relay interface into primary and secondary
subinterfaces according to the data link connection identifier (DLCI). The configuration
settings are stored in the DLCI table.

Table 11-2   DLCI Configuration Commands

Command Syntax	
add dlci|**ipdlci**|**ipxdlci** *Locname Dlci* [*Ipaddress*|*Ipxnode*]	- see page 11-23
add *W1* **dlci**	- see page page 6-3
delete dlci|**ipdlci**|**ipxdlci** *Locname Dlci*	- see page 11-24
delete *W1* **dlci**	- see page 6-4
show location *Locname*	- see page 11-21

add dlci

This command sets the Frame Relay subinterfaces for a specified location that has been configured to use Frame Relay service.

> **add dlci**|**ipxdlci** *Locname Dlci* **:**[*Ipaddress*|*Ipxnode*]

dlci	Use for IP connections.
ipxdlci	Use for IPX connections.
Locname	Location name that is in the location table.
Dlci	DLCI number, from 1 to 1023.
:*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

Note – The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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.

You can configure the PortMaster for no more than 864 (T1) or 810 (E1) interfaces. Refer to the *PortMaster 4 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 *W1* **dlci** - page 6-3
delete dlci - page 11-24

delete dlci

This command deletes entries from the DLCI table.

> **delete dlci|ipxdlci** *Locname Dlci*

dlci	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

The PortMaster 4 supports IPX protocols on ComOS 4.1 and later releases.

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 11-23
delete *W1* **dlci** - page 6-4
show location - page 11-21

Filters 12

This chapter describes how to use the command line interface to create, edit, and delete filters. The configuration settings are stored in the filter table. 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 4 Configuration Guide*.

Displaying Filter Information

To display information about your filters, use the following filter-specific commands:

- **ifconfig**—see page 2-9

- **show filter**

- **show table filter**

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 12-1 configure filters. 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 – Enter the commands on one line, without any breaks. Line breaks shown here are due to the limited space available.

Table 12-1   Filter Configuration Commands

Command Syntax	
add filter *Filtername*	- see page 12-3
delete filter *Filtername*	- see page 12-4

Table 12-1   Filter Configuration Commands *(Continued)*

Command Syntax	
save filter	- see page 12-4
set filter *Filtername* **blank**	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** [*Ipaddress*/NM *Ipaddress(dest)*/NM] [**esp|ah|ipip|ospf**] [**log**] [**notify**]	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** [*Ipaddress*/NM *Ipaddress(dest)*/NM] [**protocol** *Number*] [**log**] [**notify**]	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** =*ListName Ipaddress(dest)*/NM [**esp|ah|ipip|ospf**] [**log**] [**notify**]	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** =*ListName Ipaddress(dest)*/NM [**protocol** *Number*] [**log**] [**notify**]	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** *Ipaddress*/NM =*ListName* [**esp|ah|ipip|ospf**] [**log**] [**notify**]	- see page 12-5
set filter *Filtername RuleNumber* **permit|deny** *Ipaddress*/NM =*ListName* [**protocol** *Number*] [**log**] [**notify**]	- see page 12-6
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**]	- see page 12-7
set filter *Filtername RuleNumber* **permit|deny** =*ListName Ipaddress(dest)*/NM **tcp** [**src eq|lt|gt** *Tport*] [**dst eq|lt|gt** *Tport*] [**established**] [**log**] [**notify**]	- see page 12-7
set filter *Filtername RuleNumber* **permit|deny** *Ipaddress*/NM =*ListName* **tcp** [**src eq|lt|gt** *Tport*] [**dst eq|lt|gt** *Tport*] [**established**] [**log**] [**notify**]	- see page 12-8
set filter *Filtername RuleNumber* **permit|deny** [*Ipaddress*/NM *Ipaddress(dest)*/NM] **udp** [**src eq|lt|gt** *Uport*] [**dst eq|lt|gt** *Uport*] [**log**] [**notify**]	- see page 12-10
set filter *Filtername RuleNumber* **permit|deny** =*ListName Ipaddress(dest)*/NM **udp** [**src eq|lt|gt** *Uport*] [**dst eq|lt|gt** *Uport*] [**log**] [**notify**]	- see page 12-10
set filter *Filtername RuleNumber* **permit|deny** *Ipaddress*/NM =*ListName* **udp** [**src eq|lt|gt** *Uport*] [**dst eq|lt|gt** *Uport*] [**log**] [**notify**]	- see page 12-10

Table 12-1   Filter Configuration Commands *(Continued)*

Command Syntax
set filter *Filtername RuleNumber* **permit**|**deny** [*Ipaddress/NM Ipaddress(dest)/NM*] **icmp** [**type** *Itype*] [**log**] [**notify**]   - see page 12-12
set filter *Filtername RuleNumber* **permit**|**deny** =*ListName Ipaddress(dest)/NM* **icmp** [**type** *Itype*] [**log**] [**notify**]   - see page 12-12
set filter *Filtername RuleNumber* **permit**|**deny** *Ipaddress/NM* =*ListName* **icmp** [**type** *Itype*] [**log**] [**notify**]   - see page 12-12
set ipxfilter *Filtername RuleNumber* **permit**|**deny** [**srcnet** *Ipxnetwork*] [**srchost** *Ipxnode*] [**srcsocket eq**|**gt**|**lt** *Ipxsock*] [**dstnet** *Ipxnetwork*] [**dsthost** *Ipxnode*] [**dstsocket eq**|**gt**|**lt** *Ipxsock*]   - see page 12-14
set sapfilter *Filtername RuleNumber* **permit**|**deny** [**server** *String*] [**network** *Ipxnetwork*][**host** *Ipxnode*] [**socket eq**|**gt**|**lt** *Ipxsock*]   - see page 12-16
show filter|**ipxfilter**|**sapfilter** *Filtername*   - see page 12-18
show table filter   - see page 12-18

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 12-3
show table filter- page 12-18

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 12-4

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**]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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.
Ipaddress	IP address expressed in dotted decimal notation to compare with the source IP address of the packet. Hostnames are not recognized.
/NM	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are /0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
Ipaddress(dest)	IP address expressed in dotted decimal notation, 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 *Number*	Matches packets using the specified Internet Protocol. *Number* is a specified protocol number, as listed in RFC 1700, *Assigned Numbers*.
=ListName	Specifies a list of sites in the **/etc/choicenet/lists** directory on the ChoiceNet server. The equal sign (**=**) must immediately precede the value.

Usage

You construct filters by first creating the filter using the command **add filter**, and then adding rules 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, but you can do so with the FilterEditor application. These and other Java-based configuration tools are available via FTP at **ftp://ftp.livingston./pub/livingston/software/java/**.

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 12-3
set choicenet - page 3-30
set loghost - page 3-16

set filter (TCP)

These commands set filtering rules for Transmission Control Protocol (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**
*Ipaddress***/NM** *=ListName* **tcp** [**src eq|lt|gt** *Tport*]
[**dst eq|lt|gt** *Tport*] [**established**] [**log**] [**notify**]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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.
Ipaddress	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.
/NM	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are

/0—To match all packets with any address.
/16—Looks at high-order 16 bits of the address.
/24—Looks at high-order 24 bits of the address.
/32—Looks at the entire IP address. |
Ipaddress(dest)	IP address expressed in dotted decimal notation, 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**).
Tport	Number of the designated TCP port. See Table B-1 on page B-1 for a list of the port numbers 20 through 1701 commonly assigned to TCP and UDP services.
dst	Specifies that the packet destination port number be tested; see "Usage" for test criteria.
established	Accepts only packets being sent to an established TCP network connection, and denies packets sent to establish new TCP connections.

log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. If you have the ChoiceNet notifier installed, this keyword is used to cause a notification pop-up to appear on your computer.
=*ListName*	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory on the ChoiceNet server. The equal sign (**=**) must immediately precede the value.

Usage

The filtering rules are 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 4 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 12-3
set loghost - page 3-16

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**]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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.
Ipaddress	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.

/NM	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are
	/0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
Ipaddress(dest)	IP address expressed in dotted decimal notation, 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**).
Uport	Designated UDP port. See Table B-1 on page B-1 for a list of the port numbers 20 through 1701 commonly assigned to TCP and UDP services.
dst	Specifies that the packet destination UDP port number be tested; see "Usage" for test criteria.
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. If you have the ChoiceNet notifier installed, this keyword is used to cause a notification pop-up to appear on your computer.
=ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory on the ChoiceNet server. The equal sign (**=**) must immediately precede the value.

Usage

The filtering rules are very similar to those used for TCP packets, except that there is no **established** keyword for UDP. The order of rules in a filter is important because the PortMaster evaluates the rules in the order that they are numbered. Refer to the *PortMaster 4 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 12-3
set loghost - page 3-16

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**]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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.
Ipaddress	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.

/NM	Netmask that indicates the number of high-order bits of the source or destination IP address of the packet that must match an address in the filter. Any value between 0 and 32 can be used; common mask values are
	/0—To match all packets with any address. /16—Looks at high-order 16 bits of the address. /24—Looks at high-order 24 bits of the address. /32—Looks at the entire IP address.
Ipaddress(dest)	IP address expressed in dotted decimal notation, to compare with the destination IP address of the packet. Hostnames are not recognized.
Itype	ICMP message type to compare against the ICMP message type contained in the packet. ICMP message types are defined in RFC 1700, *Assigned Numbers*. Common ICMP types are the following: **0**—Echo reply **3**—Destination Unreachable **4**—Source Quench **5**—Redirect **8**—Echo **11**—Time Exceeded **12**—Parameter Problem **13**—Timestamp **14**—Timestamp Reply **15**—Information Request **16**—Information Reply
log	Packets matching the rule are logged by **syslog** to the loghost.
notify	Packets matching the rule are logged by **syslog** to the source of the packet. If you have the ChoiceNet notifier installed, this keyword is used to cause a notification pop-up to appear on your computer.
=ListName	Specifies a list of source or destination sites in the **/etc/choicenet/lists** directory on the ChoiceNet server. The equal sign (**=**) must immediately precede the value.

Example

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

See Also

add filter - page 12-3
set loghost - page 3-16

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*]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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
Ipxnetwork	IPX network number, a 32-bit hexadecimal value.
srchost	Specifies the comparison with the source IPX node address contained in the packet, a 48-bit hexadecimal value—usually the MAC address of the host.
Ipxnode	IPX node address, a 48-bit hexadecimal value—usually the MAC address of the host.
srcsocket	Specifies that the source IPX socket number contained in the packet must be compared with the IPX socket number specified in the filter. A second keyword—**eq**, **lt**, or **gt**—must be used to indicate the mode of comparison, an integer from 0 to 65535.
eq, lt, or **gt**	Mode of comparison of socket numbers; equal (**eq**), less than (**lt**), or greater than (**gt**).
Ipxsock	A socket number specified for the comparison, an integer from 1 to 65535.

dstnet   Specifies the comparison with the destination IPX network number contained in the packet. A 32-bit hexadecimal number.

dsthost   Specifies the comparison with the destination IPX node address contained in the packet. A 32-bit hexadecimal number.

dstsocket   Specifies that the destination IPX socket number contained in the packet must be compared with the IPX socket number specified in the filter. A second keyword—**eq**, **lt**, or **gt**—must be used to indicate the mode of comparison, an integer from 0 to 65535.

Usage

The filtering rules are based on the 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 12-3

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*]

Filtername	Name of an existing filter that is in the filter table.
RuleNumber	Filter rule number—between 1 and 256.
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.
String	SAP server name.
network	Specifies the comparison with the server's IPX network number.
Ipxnetwork	IPX network number, a 32-bit hexadecimal value.
host	Specifies the comparison with the server's IPX node address.
Ipxnode	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**).
Ipxsock	Socket number specified for the comparison, an integer from 1 to 65535.

Usage

The filtering rules are based on the 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 12-3

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.
Filtername	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 12-18

Hosts 13

This chapter describes how to configure the PortMaster to recognize hostnames. The configuration settings are stored in the host table in the nonvolatile RAM of the PortMaster 4.

Each host attached to an IP network has a unique IP address. The PortMaster 4 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.

For information on setting the NIS or DNS server and domain, refer to Chapter 3, "Global Settings."

Displaying Host Information

To display information about hostnames, use the following command:

• **show table host**

Summary of Host Commands

The commands in Table 13-1 are used to configure the host table.

Table 13-1 Host Configuration Commands

Command Syntax	
add host *Ipaddress String*	- see page 13-2
delete host *Ipaddress|String*	- see page 13-2
save host	- see page 13-2
show table host	- see page 13-3

Note – The PortMaster always checks its 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.

Example

```
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 4 configuration and operation.

Summary of Debug Commands

The debug commands in Table 14-1 are used for PortMaster debugging sessions.

Table 14-1   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 14-2
set debug ccp-stac on│off	- see page 14-3
set debug choicenet on│off	- see page 14-4
set debug clock on│off	- see page 14-6
set debug comport on│off *S0*	- see page 14-4
set debug flash on│off	- see page 14-5
set debug *Hex*	- see page 14-6
set debug imt	- see page 14-7
set debug isdn│isdn-dframes│termination│isdn-v120 on│off	- see page 14-8
set debug l2tp max│packets *Bytes*│**rpc│setup│stats**	- see page 14-9
set debug off	- see page 14-6
set debug mdp-status│mdp-events│mdp-internal│mdp-max on│off	- see page 14-9
set debug nfas	- see page 14-10
set debug ospf-hello│ospf-event│ospf-spfcalc│ospf-lsu │ospf-lsa│ospf-dbdesc│ospf-error│ospf-routing│ospf-max on│off	- see page 14-11
set debug rip│rip-detail on│off	- see page 14-12

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—except ISDN debug settings for a specific D channel—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 *Hex* 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**

See Also

set console - page 2-16
reset console - page 2-13

set debug ccp-stac

This command sets debug flags used for troubleshooting Stac LZS compression implementation. Debug information is displayed to the console.

>   **set debug ccp-stac on|off**

ccp-stac	Set **on** to display debugging messages for Stac LZS compression.
off	Clears all debug settings—including *Hex* debug settings—currently active on the PortMaster.

Usage

The **set debug ccp-stac** 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-stac on**

To stop the debugging output, enter the following:

Command> **set debug off**
Command> **reset console**

See Also

set console - page 2-16
reset console - page 2-13

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
```

See Also

set console - page 2-16
reset console - page 2-13

set debug comport

This command debugs information from a specific port. Debug information is displayed to the console.

> **set debug comport on|off** *S0*

on	Enables debugging on the specified communications port.
off	Disables debugging on the specified communications port.
S0	One of the ISDN line ports on a T1 or E1 board.

Example

```
Command> set console
Setting CONSOLE to admin session

Command> set debug comport on s3
Command> ==sleep_queue S3 newproc=listen modem_status=20
flow_control_state=4(None) port_options=2 port_type=2 hw_type=10
carrier_detect=1
```

See Also

set console - page 2-16
reset console - page 2-13

set debug flash

This command debugs information that is written to and read from the nonvolatile RAM of the PortMaster.

> **set debug flash on|off**

Usage

To display debug information to the console, use the **set console** command. To stop the output use **set debug off** or **reset console**.

Note – Using the **reset console** command only suspends the output—debugging is still active. To resume the output to console, type **set console**.

Example

```
Command> set console
Setting CONSOLE to admin session

Command> set debug flash on
Enabling Flash debugging
```

See Also

set console - page 2-16
reset console - page 2-13

set debug (Hex and Clock)

These commands set debug flags for general PortMaster troubleshooting. Debug information is displayed to the console.

> **set debug clock on|off**

> **set debug** *Hex*

> **set debug off**

clock	Set **on** to time-stamp the console debug messages. The time is measured since the last reboot and is specified in hours, minutes, seconds, and hundredths of a second. To turn the time stamp off, use the **set debug clock off** command.
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 4 Troubleshooting Guide* for information on interpreting the output.

See Also

ptrace - page 2-11
reset console - page 2-13
set console - page 2-16
traceroute - page 2-44

set debug imt

This command sets debug flags for Q.931 packet transmission. Debug information is displayed to the console.

   set debug imt on|off

   on   Set **on** to debug packets on a T1 line connected to an IMT.

   off   Clears debug settings.

Usage

Before using this command, you must first select a Quad T1 board using the **set view** command and issue the **set console** command to display packet transmission events to the console.

set debug isdn

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

set debug isdn|isdn-dframes|termination|isdn-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-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 *Hex* 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—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
```

See Also

set console - page 2-16
reset console - page 2-13

set debug l2tp

This command displays L2TP activities to the console.

> **4.1**   **set debug l2tp max|packets** [*Bytes*]**|rpc|setup|stats on|off**

max	Set **on** to display all the information generated when you use all the other debug options listed below.
packets [*Bytes*]	Set **on** to display L2TP packets. *Bytes* is an optional integer between 0 and 1500 that specifies the number of bytes to display.
rpc	Set **on** to display remote procedure call communication between the system manager module and the Quad T1, Tri E1, or LNS boards.
setup	Set **on** to display control messages and errors.
stats	Set **on** to display L2TP session statistics.
off	Clears all L2TP debug settings currently active on the PortMaster 4.

Usage

To display L2TP debug information for the entire PortMaster 4, use the **set view** command to select the manager module. To display debug information about a specific Quad T1, Tri E1, or LNS board, set the view to the slot containing the desired board.

set debug mdp

This command sets debug flags used for troubleshooting PortMaster 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 *Hex* debug settings—currently active on the PortMaster.

Usage

The **debug** command is useful for troubleshooting PortMaster digital modems as they are initialized and while their operating code is being loaded.

Examples

1. To track digital modem operation, enter the following commands:

```
Command> set console
Command> set debug mdp-max on
Enabling Maximum Modem debugging
Command> slot2: S2: Called-Station-ID <4160150> Caller-Station-ID <9254600115>
slot2: M2: mdp_allocate service 90
slot2: S2: Modem M2 bound
slot2: S2: Modem M2 connecting
slot2: M2: mdp_bind: (S2) dsl_id 0 ch_n 3 slot 12
```

2. To track digital modem status only, enter the following commands:

```
Command> set console
Command> set debug mdp-status on
```

3. To stop the debugging output, enter the following:

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

See Also

set console - page 2-16
reset console - page 2-13

set debug nfas

This command enables or disables the PortMaster 4 to log NFAS events to the console.

> `4.1`   **set debug nfas on|off**

  on   Logs NFAS events.
  off   Disables the logging of NFAS events.

Usage

The PortMaster 4 supports NFAS on ComOS 4.1 and later releases. Before using this command, you must first select a Quad T1 board using the **set view** command and issue the **set console** command to display NFAS events to the console.

See Also

reset console - page 2-13
set console - page 2-16
set *Line0* **nfas** - page 15-12

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 *Hex* 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
```

See Also

reset console - page 2-13
set console - page 2-16

set debug rip|rip-detail

This command enables the PortMaster 4 to view incoming and outgoing routes and problems with RIP authentication.

> 4.1

set debug rip|rip-detail on|off

rip	Set **on** to show incoming and outgoing routes.
rip-detail	Set **on** to show routes transferring RIP packets.
on	Enables debugging.
off	Disables debugging.

Usage

The PortMaster 4 supports this command on ComOS 4.1 and later releases.

Example

```
Command> set console
Setting CONSOLE to admin session

Command> set debug rip on
set debug rip on

Enabling RIP debugging
RIP: Recv ether1 (0.10) from 149.198.96.2 Version-1 length 500
RIP: Recv ether1 (0.10) from 149.198.96.2 Version-1 length 500
RIP: Recv ether1 (0.10) from 149.198.96.2 Version-1 length 500
RIP: Recv ether1 (0.10) from 149.198.96.2 Version-1 length 280
RIP: Send ether1 (0.10) Version-2
RIP: Send ptp0 (0.0) Version-1
RIP: Send ptp0 (0.0) Version-1
```

See Also

reset console - page 2-13
set console - page 2-16

This chapter describes how to use the command line interface to configure T1 and E1 lines on the PortMaster 4 for the following kinds of services:

T1 Line0 through Line3	E1 Line0 through Line2
Full T1	Full E1
Fractional T1	Fractional E1
Channelized T1	Multifrequency R2 (MFR2) signaling for channelized E1
ISDN Primary Rate Interface (PRI)	ISDN PRI
	Fractional PRI

This chapter also describes commands for monitoring the digital modems on the PortMaster 4.

For additional configuration information, see the *PortMaster 4 Installation Guide*.

Note – After making any configuration changes to a line, you must use the **save all** and **reset slot** commands for the changes to take effect.

Displaying ISDN PRI, T1, and E1 Diagnostic Information

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

- **set console**—see page 2-16
- **set debug imt**—see page 14-7
- **set debug isdn on**—see page 14-8
- **set debug isdn-dframes on**—see page 14-8
- **set debug mdp-status on**—see page 14-9
- **set debug nfas**—see page 14-10

When finished, use the following commands:

- **set debug off**—see page 14-6
- **reset console**—see page 2-13

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

- **show all**—see page 2-19
- **show global**—see page 2-26
- **show imt**

- **show** *Line0*
- **show modems**
- **show** *M0*
- **show nfas**
- **show sessions**—see page 2-37

Summary of ISDN PRI, T1, and E1 Commands

The ISDN PRI, T1, and E1 configuration commands are shown in Table 15-1.

Table 15-1   ISDN PRI, T1, and E1 Commands

Command Syntax	
attach *C0*	- see page 5-4
save all	- see page 2-15
set call-check on|off	- see page 3-6
set debug imt on|off	- see page 14-7
set debug isdn|isdn-dframes|termination|isdn-v120 on|off	- see page 14-8
set debug mdp-status on|off	- see page 14-9
set debug nfas on|off	- see page 14-10
set imt-parms *Ipaddress Tport1 Tport2* [**1a**|**default**]	- see page 15-3
set isdn-switch net5|euroisdn|vn2|vn3|1tr6|ntt|kdd|ts014	- see page 15-5
set isdn-switch ni-2|dms-100|att-4ess|att-5ess	- see page 15-5
set *Line0* **clock backplane|external|internal**	- see page 15-7
set *Line0* **encoding b8zs|ami|hdb3**	- see page 15-8
set *Line0* **framing esf|d4|crc4|fas**	- see page 15-8
set *Line0* **group** *Cgroup* **56k|64k**	- see page 15-9
set *Line0* **group** *Cgroup*|**none channels** *Channel-list*	- see page 15-10
set *Line0* **imt**	- see page 15-11
set *Line0* **isdn|t1|e1|fractional|isdn-fractional|inband**	- see page 15-6
set *Line0* **loopback on|off**	- see page 15-12
set *Line0* **nfas primary|secondary|slave|disabled** *Identifier Group*	- see page 15-12
set *Line0* **pcm u-law|a-law**	- see page 15-14
set *Line0* **signaling fxs|immediate|wink**	- see page 15-14
set *Line0* **signaling r2generic|mfr2** *Profile*	- see page 15-15

Table 15-1   ISDN PRI, T1, and E1 Commands (Continued)

Command Syntax	
set *Line0* **signaling rbs**|**norbs**	- see page 15-16
set *Line0* **source local**|*Slotnumber:Channel*	- see page 16-2
set location *Locname* **analog on**|**off**	- see page 11-4
set *M0* **on**|**off**	- see page 15-17
set *S0* **directory** *Number*	- see page 15-18
show all	- see page 2-19
show imt	- see page 15-18
show isdn	- see page 15-19
show *Line0*	- see page 15-20
show *M0*	- see page 15-23
show modems	- see page 15-23
show nfas	- see page 15-24

ISDN PRI, T1, and E1 Commands

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

set imt-parms

This command sets the Signaling System 7 (SS7) gateway address, the listening port on the SS7 gateway, the PortMaster 4 base socket, and the switch type for an intermachine trunk (IMT).

> 4.1

set imt-parms *Ipaddress Tport1 Tport2* [**1a**\|**default**]

Ipaddress	SS7 gateway address—IP address in dotted decimal notation—provided by the SS7 gateway administrator.
Tport1	SS7 gateway port—the TCP socket in the SS7 gateway that is used to listen for SS7 clients. The gateway port is provided by the SS7 gateway administrator.
Tport2	Local port—the base value assigned to slot 0 from which the PortMaster 4 derives the originating TCP port number for each Quad T1 and Tri E1 board. Each board derives its local port number by adding its slot number to the base local port value.

Note – The *Tport2* value is same for all slots on any single PortMaster 4.

1a   Sets the switch type to 1A. This switch type enables the
                          PortMaster 4 to interpret the loopback command from the
                          SS7 gateway as 1A continuity check requests.

Note – If you set the switch type to **1a**, you must also set signaling to robbed bit
signaling using the **set** *Line0* **signaling rbs** command.

default   Supports all other switch types. This is the default. If no
                          argument is specified, the PortMaster assumes the **default**
                          setting.

Usage

The PortMaster 4 supports SS7 signaling on ComOS 4.1 and later releases.

To use this command, you must first select a slot for configuration using the **set view**
command.

A single PortMaster 4 supports only one SS7 gateway, and any single PortMaster 4
supports only 96 modems for SS7 signaling. Because modem pools are managed on a
slot-by-slot basis, each slot on the PortMaster 4 connected to an intermachine trunk
(IMT) is an independent SS7 client and establishes an independent session with the SS7
gateway.

You must also configure the lines of a Quad T1 or Tri E1 board using the **set** *Line0* **imt**
command.

To save the SS7 settings and activate them, you must enter **save all** and reset slot.

For more information about SS7 configuration, see the *PortMaster 4 Configuration Guide*.

Example

The following example sets an SS7 gateway with IP address 192.168.0.0 and TCP port
number 1000 to communicate with a line board in slot 0 of the PortMaster 4 on TCP
port 7000. Any additional slots configured for SS7 on this PortMaster 4 must also use
7000 as a local base port.

```
Command> set view 0
View changed from 4 to 0

Command 0> set imt-parms 192.168.0.0 10000 7000 1a
Changed gateway IP address from 0.0.0.0 to 192.168.0.0
Changed gateway port from 0 to 100000
Changed local port from 7000 to 7000
```

See Also

set *Line0* **imt** - page 15-11
set *Line0* **signaling rbs** - page 15-16
show imt - page 15-18

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|att-4ess|att-5ess**

> **set isdn-switch net5|euroisdn|vn2|vn3|1tr6|ntt|kdd|ts014**

ni-2	National ISDN-2 (NI-2) compliant. This is the default.
dms-100	Northern Telecom DMS-100.
att-4ess	AT&T 4ESS.
att-5ess	AT&T 5ESS.
net5, euroisdn	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

To use this command, you must first select a slot for configuration using the **set view** command.

The switch type information is available from your ISDN PRI telephone service provider. Any change you make in the switch provisioning setting does not take effect until you reset the active slot using the **reset slot** command.

Example

```
Command 1> set isdn-switch att-5ess
ISDN switch type set to ATT-5ESS
```

set *Line0*

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 in-band 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**

Line0	**line0**, **line1**, **line2**, or **line3**.
isdn	Uses the line as PRI B channels. This is the default.
t1	Uses the entire line as a T1 line.
e1	Uses the entire line as an E1 line.
isdn-fractional	Divides an ISDN line into groups specified by the **set** *Line0* **group** command (see page 15-10).
fractional	Divides a channelized T1 or E1 line into groups specified by the **set** *Line0* **group** command (see page 15-10).
inband	Sets the line for in-band signaling for channelized T1 and E1. The signaling protocol for channelized T1 is specified by the **set** *Line0* **signaling** command (see page 15-14). For channelized E1, use the **set** *Line0* **signaling mfr2** command (see page 15-15).

Usage

You must first select a slot for configuration with the **set view** command before using this command.

T1 and E1 lines might require an external clock signal provided either by the device that the PortMaster is connected to or by the telephone company network. Each Quad T1 and Tri E1 board uses the clock of the first active line port, starting with Line0, as its transmit clock that is shared among all the line ports. See the *PortMaster 4 Installation Guide* for more information about connecting T1 and E1 lines.

set *Line0* clock

This command specifies the clocking source for a synchronous line on a Quad T1 board.

> 4.1

        set *Line0* **clock backplane|internal|external**

Warning – Do not set *Line0* to **internal** if another line on the same Quad T1 board is configured with an active synchronous line set to **external** or **backplane** as a clocking source**.**

Line0	**line0**, **line1**, **line2**, or **line3** on a Quad T1 line board.
backplane	Sets *Line0* to obtain its clock signal from the PortMaster 4 backplane. The backplane can receive its clocking from a T3 Mux board. You must also enable clocking on the backplane.
internal	Sets *Line0* to obtain its clock signal from the Quad T1 board.
external	Sets the Quad T1 board to obtain its clock signal from the DS-1 line itself.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

If you choose the backplane as a clock source, you must also use the **set mux backplane-clock** command to enable the T3 Mux board to provide clocking to the backplane.

Example

```
Command 7> set line0 clock backplane
line0 clocking changed to backplane
```

See Also

set mux backplane-clock – page 16-3

set *Line0* encoding

This command sets the encoding method used with T1 or E1 lines.

> **set** *Line0* **encoding b8zs|ami|hdb3**

Line0	**line0**, **line1**, **line2**, or **line3**.
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.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

Example

```
Command 1> set line0 encoding b8zs
line0 encoding successfully changed
```

set *Line0* framing

This command sets the framing format used for the E1 or T1 line.

> **set** *Line0* **framing esf|d4|crc4|fas**

Line0	**line0**, **line1**, **line2**, or **line3**.
esf	Extended superframe. This is the default format for T1 lines.
d4	D4 framing, an alternative format for T1 lines.
crc4	Cyclic redundancy check 4. This is the default format for E1 lines.
fas	Frame Alignment Signal, an alternative format for E1 lines.

Usage

You must first select a slot for configuration using the **set view** command before using this command.

Example

```
Command 1> set line0 framing esf
line0 framing successfully changed
```

set *Line0* **group**

This command allows you to set the channel rate for a group on a fractional T1 or E1 line to 56Kbps or 64Kbps.

>   **set** *Line0* **group** *Cgroup* **56k|64k**

Line0	**line0**, **line1**, **line2**, or **line3**.
Cgroup	Defined channel group from 1 to 32.
56k	56Kbps, typically used for D4 framing.
64k	64Kbps, used for framing types other than D4. This is the default.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

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.

Example

```
Command 1> set line0 group 0 56k
line0 group 0 channels set to 56000 bps
```

See Also

set *Line0* **fractional** - page 15-6
set *Line0* **group channels** - page 15-10

set *Line0* group channels

This command allows you to divide an ISD PRI line, T1 line, or E1 line into groups that function as synchronous ports.

> **set** *Line0* **group** *Cgroup* **channels** *Channel-list*

Line0	**line0**, **line1**, **line2**, or **line3**.
Cgroup	Group number from 1 to 32 that designates a port number on each ISDN line, T1, or E1 line, or **none** to unassign channels.
Channel-list	Space-separated list of one or more channel numbers, from 1 through 24 for T1, or 1 through 30 for E1. The channel numbers do not have to be contiguous.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

To use channel groups, you must first set the line type to **fractional** or **isdn-fractional** with the **set** *Line0* command.

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 channels to a channel rate of 64Kbps, use the following commands:

```
Command 1> set line0 fractional
Command 1> set line0 group 2 channels 1 2 3 4
Command 1> set line0 group 2 64k
Command 1> save all
Command 1> reset slot1
```

Now configure the channel group 2 as you would any PortMaster synchronous port.

See Also

set *Line0* **fractional** - page 15-6
set *Line0* **group 64k** - page 15-9

set *Line0* imt

This command sets the line connected to an intermachine trunk (IMT) for SS7 signaling.

4.1 >   **set** *Line0* **imt**

Line0	**line0**, **line1**, **line2**, or **line3**.
imt	Sets the line connected to an intermachine trunk (IMT) for SS7 signaling.

Usage

The PortMaster 4 supports SS7 signaling on ComOS 4.1 and later releases.

You must first select a slot for configuration with the **set view** command before using this command.

To configure SS7 signaling, you must also use the **set imt** command to specify the SS7 gateway address and gateway port, the PortMaster 4 local port, and the switch type. For more information about configuring SS7 signaling, see the *PortMaster 4 Configuration Guide*.

If the switch type is **1a**, you must configure the line for robbed bit signaling using the **set** *Line0* **signaling rbs** command.

To save and activate the new settings, you must **save all, set slot off** and **set slot on** for every slot.

Example

```
Command> set view 0
View changed from 4 to 0

Command 0> set line1 imt
line1 changed to imt
```

See Also

set imt-parms - page 15-3
set *Line0* **signaling rbs** - page 15-16
show imt - page 15-18

set *Line0* **loopback**

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

> **set** *Line0* **loopback on|off**

Line0	**line0**, **line1**, **line2**, or **line3**.
on	Turns on local network loopback.
off	Turns off local network loopback.

Usage

This command is used for telephone line testing purposes.

Example

```
Command 1> set line0 loopback on
Loopback set ON for Line0
```

set *Line0* **nfas**

This command sets non-facility associated signaling (NFAS) parameters for a T1 line.

 4.1 >   **set** *Line0* **nfas primary|secondary|slave|disabled** *Identifier Group*

Line0	**line0**, **line1**, **line2**, or **line3**.
primary	Sets the line as the primary D channel for the specified group.
secondary	Sets the line as the backup D channel for the specified group
slave	Sets the line as a slave interface—all channels on the line are B channels.
disabled	Disables NFAS on the interface.
Identifier	Integer between 0 and 19 that uniquely identifies a T1 interface in an NFAS group.
Group	Group number—a common number assigned to all the T1 lines belonging to the same NFAS group. *Group* is an integer between 1 and 99.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

NFAS is a service provided by the telephone company allowing a single D channel to provide signaling for a group of ISDN PRI lines or interfaces, so that the channels normally used for signaling on the remaining PRIs can be used as B channels.

The PortMaster 4 supports NFAS on ComOS 4.1 and later releases. Up to 20 PRIs can be grouped together to share a primary D channel with or without D channel backup (DCBU).

The T1 interfaces of any single Quad T1 board must belong to the same NFAS group. Once NFAS is enabled on a Quad T1 board, all T1 lines can no longer run in the standard PRI configuration of 23 B channels and 1 D channel. If only one T1 interface is available on a Quad T1 board, it can belong to an NFAS group by itself.

Note – Setting multiple pairs of primary and backup D channels in the same group causes NFAS to break.

When the primary D channel fails, the backup D channel is enabled but the active calls on the lines serviced by the failed D channel are terminated. No calls are saved during the switch to the backup D channel. When the primary D channel is restored, it acts as a backup to the currently active D channel.

NFAS is serviced by UDP port 1650.

To debug NFAS events, use the **set debug nfas** command. For more information about configuring your PortMaster 4 for NFAS, refer to the *PortMaster 4 Configuration Guide.*

Note – You must use the **save all** and **reset slot** commands for the new settings to take effect.

Examples

In the following example, Line0 of the Quad T1 board occupying slot 0 is configured as the primary D channel, Line1 is configured as the backup D channel, and Line2 and Line3 are set as slaves with only B channels.

```
Command> set view 0
View changed from 4 to 0

Command 0> set line0 nfas pri 0 4
New NFAS parameters will be effective after next reboot

Command 0> set line1 nfas sec 1 4
New NFAS parameters will be effective after next reboot

Command 0> set line2 nfas sla 2 4
New NFAS parameters will be effective after next reboot

Command 0> set line3 nfas sla 3 4
```

See Also

show *Line0* - page 15-20
show nfas - page 15-24
set debug nfas - page 14-10

set *Line0* pcm

This command sets the companding method used for digitized audio signals.

> **set** *Line0* **pcm u-law|a-law**

Line0	**line0**, **line1**, **line2**, or **line3**.
u-law	Default method of "companding"—compressing and expanding—the amplitude of audio signals over T1 PRI lines.
a-law	Default method companding the amplitude of audio signals transmitted over E1 PRI lines.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

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.

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 companding. V.90 is not supported for dial-out modems. The maximum analog dial-out speed is 33600bps for K56flex and V.90 protocols.

Example

```
Command 1> set line0 pcm u-law
line0 PCM encoding changed to u-law
```

set *Line0* signaling

This command sets the in-band signaling protocol and the in-band call options used with channelized T1.

> **set** *Line0* **signaling fxs|immediate|wink**

Line0	**line0**, **line1**, **line2**, or **line3**.
fxs	Foreign exchange station (FXS) loop start protocol.
immediate	E & M immediate start protocol.
wink	E & M wink start protocol, an option for use with channelized T1 lines. This is the default.

Usage

You must first select a slot for configuration with the **set view** command before using this command.

Note – You must first set *Line0* to in-band signaling using the command **set line0 inband** before using the command **set** *Line0* **signaling**.

Example

```
Command 1> set line0 signaling wink
line0 changed to inband signaling wink
```

See Also

set *Line0* **inband** - page 15-6

set *Line0* signaling r2generic|mfr2

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

> **set** *Line0* **signaling r2generic|mfr2** *Profile*

Line0	**line0**, **line1**, **line2**, or **line3**.
r2generic	Generic R2, the default when Line0 is set for in-band signaling. Sets in-band signaling to MFR2 but without tone signaling.
mfr2 *Profile*	One of the following channelized E1 in-band signaling profiles:

	0	ITU-T standard: Argentina, Saudi Arabia, 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

You must first select a slot for configuration with the **set view** command before using this command.

A number profile can apply to different countries, and a country can have more than one MFR2 profile available.

Use the **show line0** command to display the type of in-band signaling used and the MFR2 profile selected.

For more information on configuring for MFR2 signaling, refer to the *PortMaster 4 Configuration Guide.*

Note – You must first set the line to in-band signaling using the command **set** *Line0* **inband** before setting the line to MFR2 signaling.

Examples

```
Command 1> set line0 signaling mfr2 0
line0 changed to inband signaling, MFR2

Command 1> set line1 signaling r2gen
line1 changed to inband signaling, R2MF generic
```

See Also

set *Line0* **inband** - page 15-6
show *Line0* - page 15-20

set *Line0* signaling rbs|norbs

This command sets the PortMaster 4 to recognize the IMT as a line with twenty-four 56k bit channels using robbed bit signaling.

> 4.1   **set** *Line0* **signaling rbs|norbs**

Line0	**line0**, **line1**, **line2**, or **line3**.
rbs	Sets the PortMaster to recognize robbed bit signaling on the IMT line. Use this command only if the IMT is connected to a **1a** switch.
norbs	Supports all other switch types. This is the default.

Usage

The PortMaster 4 supports this command on ComOS 4.1 and later releases.

You must first select a slot for configuration with the **set view** command before using this command.

To save and activate the new settings, you must **save all**, **set slot off**, and **set slot on** for every slot.

Example

```
Command> set view 0
View changed from 4 to 0
```

```
Command 0> set line0 signaling rbs
line0 signaling changed to rbs
```

See Also

set imt-parms - page 15-3
set *Line0* **imt** - page 15-11
show imt - page 15-18

set *M0*

This command makes the digital modems on the PortMaster 4 available or unavailable.
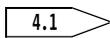
4.1 ▷   **set** *M0* **on**|**off**

M0	Any modem number from **m0** to **m95**. 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 PortMaster 4 supports this command on ComOS 4.1 and later releases.

You must first select a slot for configuration with the **set view** command before using this command. The digital modems on Quad T1 board are numbered from M0 to M95, for a maximum of 96 modems. Any user on a modem that is busied is disconnected.

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

Example

```
Command 0> set m0 off
Modem M0 changed from on to off
```

See Also

set location analog - page 11-4

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*

S0	One of the virtual ISDN PRI ports.
Number	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.

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 RADIUS 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 imt

This command displays settings for a slot configured for SS7 signaling.
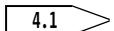
> **4.1** >   **show imt**

Usage

You must first select a slot using the **set view** command before using the **show imt** command.

Example

Command 0> **show imt**

Gateway IP address: 198.36.134.27, gateway port: 10000, local port: 7000
Switch type: 1a

See Also

set imt-parms - page 15-3
set *Line0* **imt** - page 15-11
set *Line0* **signaling rbs** - page 15-16

show isdn

This command displays the status of the ISDN PRI ports.

> 4.1

show isdn [**d***Number*|*S0*]

Number   D channel number.

S0   Serial port number associated with the PRI port.

Usage

You must first select a slot using the **set view** command before using this command.

The PortMaster 4 supports the **show isdn** command on ComOS 4.1 and later releases.

To display comprehensive information about an ISDN port, enter the command with the active D channel number or the serial port number associated with the PRI port.

Example

Command 0> **show isdn**

D	Ports	State	L1 L2	Change	init	Up	Down
0	S0–S22	UP	Active	1days	3	1	2
1	S24–S46	UP	Active	1days	3	1	2
2	S48–S70	UP	Active	1days	3	1	2
3	S72–S94	UP	Active	1days	3	1	2

Explanation

D	D channel.
Ports	ISDN port numbers supported by the D channel PortMaster.
State	D channel status.
L1 L2	Line status.
Change	Time since last change in status.
Init	Number of times a network termination 1 device (NT1) has attempted to bring up a link.
Up	Number of times a link has gone to **Up** status.
Down	Number of times a link has gone to **Down** status.

show *Line0*

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

> **show** *Line0*

Line0	**line0**, **line1**, **line2**, or **line3**.

E1 Example

Line1 is configured as an ISDN PRI line.

```
Command 1> 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

1. Line0 is configured as an ISDN PRI line.

```
Command 1> 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
```

2.   Line0 is configured for in-band signaling—channelized T1.

```
Command 1> show line0
-------------------- line0 - T1 Inband DS0 --------------------------
Status: UP              Framing: ESF    Encoding: B8ZS     PCM: u-law
Signaling: Trunk E&M wink start         Options: inbound calls only
Receive Level:          +2dB to -7.5dB
Alarms                                  Violations
---------------------------------       --------------------------------
Blue                            0  Bipolar                     5
Yellow                          0  CRC Errors                  0
Receive Carrier Loss            0  Multiframe Sync             2
Loss of Sync                    0
```

ISDN Example

Line0 is configured as a fractional ISDN line with one group of seven channels.

```
Command 1> 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 15-8.
Encoding	Encoding method in use.	See page 15-8.
PCM	Pulse code modulation method in use.	See page 15-14.
Channel Group	Channel group number.	See page 15-10
Speed	Connect speed.	
Channels	Channel numbers.	See page 15-10.
Signaling	Type of in-band signaling in use	See page 15-14 and page 15-14.
Options	In-band signaling options in use.	See page 15-14.
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 the same polarity.	
	CRC Errors—Errors in CRC6 code words (ESF framing), or in the Ft framing bit position (D4 framing).	
	Multiframe Sync—Multiframes received out of synchronization.	

show *M0*

This command shows the status of a digital modem on a PortMaster.

> **show** *M0*

> *M0*   The digital modem number.

show modems

This command displays the status of all digital modems on a PortMaster.

> **show modems**

Usage

To display modem information about a specific line board of a PortMaster 4, you must first use the **set view** command.

Example

The following example is from a PortMaster 4 T1 line board in slot 1.

```
Command 1> 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              READY     UNKNWN     NONE           NONE        0        0          NORMAL
M4              READY     UNKNWN     NONE           NONE        0        0          NORMAL
M5              READY     UNKNWN     NONE           NONE        0        0          NORMAL
.
.
.
M95             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	Connect speed in bits per second.
Compression	Compression standard used.
Protocol	Data link layer protocol used.
Calls	Number of calls since the last PortMaster reboot.
Retrain	Number of times the modem changes speed (retrains) due to a change in line quality since the last PortMaster reboot.
Disconnect	Type of modem disconnection: normal or lost carrier.

show nfas

This command displays NFAS information for the selected Quad T1 board and the neighboring Quad T1 boards in the same NFAS group.

> **4.1**   **show nfas**

Usage

The PortMaster 4 supports NFAS on ComOS 4.1 and later releases.

To view information for NFAS, you must first select a board using the **set view** command.

Example

```
Command 1> show nfas
N   group  line0   line1   line2   line3  state0   state1  state2   state3
-   ----   ------  ------- -----   ----   -------  -----   ------   ---
1   5      2(SEC)  1(SLA)  X       X      STANDBY  UP
9   5      0(PRI)  X       X       X      IN-SERV
6   56     0(PRI)  1(SLA)  2(SEC)  X      NO-SERV  DOWN    NO-SERV
```

Explanation

N	Slot number of a Quad T1 board belonging to an NFAS group.
group	Group number—integer between 1 and 99.
line0, line1, line2, or line3	Interface number of the T1 line and the type of NFAS service it provides:

PRI	Line is set as the primary D channel servicing all interfaces in the NFAS group.
SEC	Line set as the backup D channel interface.
SLA	Slave interface.

	X	Line is not active or is not set for NFAS.
state0, **state1**, **state2**,or **state3**	Displays the status of the lines in the NFAS group:	
	STANDBY	Line is set as a D channel and is in standby mode.
	IN-SERV	Line is the active D channel.
	NO-SERV	Line is configured but not functional.
	UP	Slave line is functional.
	DOWN	Slave line is configured but is not functional.

See Also

set *Line0* **nfas** - page 15-12
set debug nfas - page 14-10

The T3 Mux board on the PortMaster 4 divides (demultiplexes) a DS-3 signal from a T3 line into 28 individual DS-1 signals and terminates it on Quad T1 board. ComOS 4.1 and later releases support the T3 Mux board. The T3 Mux board can be inserted into any slot except slot 4, which is reserved for the manager module.

For information about installing and configuring the T3 Mux board, refer to the *PortMaster 4 Installation Guide* and *PortMaster 4 Configuration Guide*.

Note – To activate the T3 Mux board, you must first configure Ether0 or Ether1 with an IP address.

Displaying T3 Mux Diagnostic Information

To display T3 Mux debug information on the console, use the following commands:

- **show mux**

- **show** *Line0*

Summary of T3 Mux Commands

Table 16-1 shows the T3 Mux board configuration commands.

Table 16-1   T3 Mux Configuration Commands

Command Syntax	
set *Line0* **source local**|*Slotnumber***:***Channel*	- see page 16-2
set *Line0* **clock backplane**|**external**|**internal**	- see page 15-7
set mux backplane-clock disable|**enable**	- see page 16-3
set mux channel-loop *Channel* **auto**|**on**|**off**	- see page 16-4
set mux line-clock external|**internal**	- see page 16-5
set mux line-loop auto|**on**|**off**	- see page 16-5
show mux	- see page 16-6
show mux status	- see page 16-8

T3 Mux Commands

These commands are used for configuring and displaying the status of T3 Mux boards.

set *Line0* source

This command sets the line termination for a DS-1 line on a Quad T1 board to its own physical port on the Quad T1 board or to a channel from a T3 Mux board.

> 4.1

        set *Line0* **source local**|*Slotnumber***:***Channel*

Line0	**line0**, **line1**, **line2**, or **line3** on a Quad T1 line board.
local	Terminates *Line0* at its own external RJ-45 synchronous port. This is the default.
*Slotnumber***:***Channel*	Maps *Line0* to a DS-1 channel on a T3 Mux board and disables the RJ-45 port on the Quad T1 board.

	Slotnumber	Physical slot containing the T3 Mux board—an integer between 0 and 9, except slot 4.
	Channel	Integer between 1 and 28 that specifies the DS-1 channel number on the T3 line.

Usage

Before using this command, you must first set the view to the slot containing the Quad T1 board.

The T3 Mux board maps a line port on a Quad T1 board to one of the 28 channels of a T3 line. Only one line port can be mapped to any one T3 channel. You need not demultiplex an entire T3 line when using a T3 Mux board.

The provisioning for the DS-1 lines must match the provisioning of the individual T3 channels the DS-1 lines are mapped to.

The line ports on the Quad T1 board can then be configured as ISDN PRI or full, fractional, or channelized T1. The T3 Mux board supports the M13 framing format and converts bipolar 3-zero substitution (B3ZS) line encoding to nonreturn to zero (NRZ) digital DS-3 signaling.

⚠ **Caution –** Each synchronous line must be mapped to a unique DS-1 channel—two synchronous lines cannot share the same DS-1 channel.

Example

```
Command> set view 7
View changed from 4 to 7
Command 7> set line0 source 8:25
line0 source set to T3 stream 25 in slot 8
```

See Also

set view - page 2-18
show mux - page 16-6

set mux backplane-clock

This command enables and disables the PortMaster 4 backplane to receive a clock signal from the T3 Mux board.

> 4.1   **set mux backplane-clock disable|enable**

disable   Disables the T3 Mux board from providing clocking to the PortMaster 4 backplane. This is the default.

enable   Enables the T3 Mux board to provide a clock signal to the PortMaster 4 backplane, allowing the backplane to provide clocking to the other line boards on the PortMaster 4. In this configuration, the physical Quad T1 line ports are unused.

You must also use the **set mux line-clock external** command to set a clock source for the T3 Mux board.

Usage

Before using this command, you must first set the view to the slot containing the T3 Mux board.

Example

```
Command> set view 8
View changed from to 8

Command 8> set mux backplane-clock enable
T3 Mux (slot 8) Backplane Clock set to Enabled
```

See Also

set mux line-clock - page 16-5
set *Line0* **clock** - page 15-7
set view - page 2-18

set mux channel-loop

This command enables the PortMaster 4 to perform diagnostic loopback tests on a single DS-1 channel within a T3 line.

4.1 ▷   **set mux channel-loop** *Channel* **auto|on|off**

Channel	Integer between 1 and 28 that specifies the channel within the T3 line to be looped.
auto	Sets the specified DS-1 line to enter or exit loopback mode if it detects a loop-up or loop-down sequence from an external source, such as the telephone company. This is the default.
on	Manually enables DS-1 loopback for the specified channel.
off	Disables DS-1 loopback for the specified T3 channel and ignores external loop-up and loop-down commands.

Usage

You must first set the view to the slot containing the T3 Mux board before using this command.

Example

```
Command> set view 0
View changed from 4 to 0

Command 0> set mux channel-loop 1 auto
Mux (slot 0) chan 1 loopback set to Auto
```

See Also

set mux line-loop - page 16-5

set mux line-clock

This command sets the clocking source for a T3 Mux board and its T3 line.

> 4.1   **`set mux line-clock external|internal`**

external	Sets the T3 Mux board to receive its 44.74Mbps clock signal from the T3 line.
internal	Sets the T3 Mux board to generate a 44.74Mbps clock signal for the T3 line.

Usage

The line port on the Quad T1 can be configured to receive its clock signal from the backplane if the T3 Mux board is configured to provide clocking to the backplane.

You must first set the view to the slot containing the T3 Mux board before using this command.

Example

```
Command> set view 8
View changed from 4 to 8

Command 8> set mux0 line-clock external
T3 Mux (slot 8) Line Clock set to External
```

See Also

`set mux backplane-clock` - page 16-3

set mux line-loop

This command enables the PortMaster 4 to perform diagnostic loopback tests on an entire T3 line.

> 4.1   **`set mux line-loop auto|on|off`**

auto	Sets the entire T3 line to enter or exit loopback mode if it detects a loop-up or loop-down sequence from an external source such as the telephone company.
on	Enables loopback for the entire T3 line.
off	Disables T3 line loopback and ignores external loop-up and loop-down commands.

Usage

Before using this command, you must first set the view to the slot containing the T3 Mux board.

Example

```
Command> set view 0
View changed from 4 to 0

Command 0> set mux line-loop on
Mux (slot 0) Line Loop set to On
```

See Also

set mux channel-loop - page 16-4

show mux

This command displays the status of a T3 Mux board.

```
 4.1      show mux
```

Example

```
Command 8> show mux
MUX Line Status: Up     Line Clock: External    Backplane clock: Enabled
```

Mux Channel	Slot	Line	Line Status	Line Type	Line Sync Loss	X-Connect
1	7	0	Up	Inband	0	OK
2	7	1	Up	Inband	0	OK
3	7	2	Up	Inband	0	OK
4	7	3	Up	Inband	0	OK
5	1	0	Up	Inband	0	OK
6	1	1	Up	Inband	0	OK
7	1	2	Up	Inband	0	OK
8	1	3	Up	Inband	0	OK
9	2	0	Up	Inband	0	OK
10	2	1	Up	Inband	0	OK
11	2	2	Up	Inband	0	OK
12	2	3	Up	Inband	0	OK
13	3	0	Up	Inband	0	OK
14	3	1	Up	Inband	0	OK

15	3	2	Up	Inband	0	OK
16	3	3	Up	Inband	0	OK
17	5	0	Up	Inband	0	OK
18	5	1	Up	Inband	0	OK
19	5	2	Up	Inband	0	OK
20	5	3	Up	Inband	0	OK
21	6	0	Up	Inband	0	OK
22	6	1	Up	Inband	0	OK
23	6	2	Up	Inband	0	OK
24	6	3	Up	Inband	0	OK
25	0	0	Up	ISDN	0	OK
26	0	1	Up	ISDN	0	OK
27	0	2	Up	ISDN	0	OK
28	0	3	Up	ISDN	0	OK

Explanation

MUX Line Status Displays the status of the T3 Mux board.

Line Clock Source of clocking.

Backplane clock Displays the source of backplane clocking:

Enabled T3 Mux board is providing the clocking to the backplane.

Disabled T3 Mux board does not provide clocking to the backplane.

Mux Channel Integer between 1 and 28 that corresponds to a digital signaling channel on the T3 line.

Slot Integer between 0 and 9 that identifies a physical slot occupied by a Quad T1 board on the PortMaster 4. Seven Quad T1 boards are required to fully terminate a T3 Mux card.

Line Line 0, line 1, line 2, or line 3 on a Quad T1 board that terminates a T3 channel.

Line Status Status of a T1 line:

Up T1 line is active.

Down T1 line is inactive.

Carrier T3 Mux board detects a signal for the channel, but the Quad T1 board might be inactive or removed from its slot.

No Signal T3 Mux board detects no signal from the DS-1 channel.

Alarm T3 Mux board detects an alarm condition for the channel.

Line Type	Type of service that the T1 line is set to:

Inband	Line is configured as channelized T1—robbed bit signaling.
ISDN	Line is configured as ISDN PRI.

Line Sync Loss	Number of times synchronous timing was lost for the channel specified.
X-Connect	Displays the connection status between the T3 Mux board and the T1 line.

Ok	Backplane connection is made between the T3 Mux board and the T1 line, and a channel is assigned to the line.
Connected	Backplane connection is made between the T3 Mux board and the T1 line, but no channel has been assigned to the line.
Connecting	Backplane connection between the T3 Mux board and the T1 line is in progress.
T3 Not Ready	T3 Mux board is inactive.
T1 Not Ready	Quad T1 board is inactive.
n/a	Quad T1 is not in its slot.

show mux status

This command displays information about DS-3 line on a T3 Mux board.

    show mux status

Example

```
Command 8> show mux status
-------------------- Statistics for Mux0 in slot0 --------------------
      Rx Loss of Signal:  0          Rx Out of Frame:  0
          Rx AIS alarm:  0          Rx IDLE Pattern:  0
       Rx Clock Failure:  0          Tx Clock Failure:  0
         F&M Bit Errors:  0             M Bit Errors:  0
          Parity Errors:  0
```

Explanation

Rx Loss of Signal	Occurs when incoming DS-3 data is stuck low for more than 1022 clock cycles. Recovery occurs when two or more ones are detected in the incoming data bit stream.
Rx AIS alarm	Ensures that the T3 Mux board is detecting DS-3 framing.

Rx Clock Failure	Receive DS-3 clock failure alarm—occurs when the receive clock is stuck high or low for from 30 to 100 DS-3 clock periods. Recovery occurs on the first clock transition.
F&M Bit Errors	8-bit saturation counter—number of DS-3 F-bits and DS-3 M-bits that are in error since the last read cycle. This counter is inhibited when a DS-3 loss-of-signal or out-of-frame error occurs.
Parity Errors	Number of P-bit parity errors received since the last cycle. This counter is inhibited when a DS-3 loss-of-signal or out-of-frame error occurs.
Rx Out of Frame	Occurs when 3 out of 16 F-bits are in error—in a sliding window of 16 bits—or when one or more M-bits are in error in two consecutive frames. Recovery occurs when the F-framing pattern of **1001** is detected and the M-framing pattern of **010** is detected for two consecutive frames. Recovery takes approximately 0.95 milliseconds.
Rx IDLE Pattern	Occurs when six or more 4-bit groups of the pattern **1-1-0-0** per DS-3 frame contain errors.
Tx Clock Failure	Occurs when the transmit input clock is stuck high or low for from 30 to 100 DS-3 clock periods. Recovery occurs when the first clock transition is detected.
M Bit Errors	Number of M-bits that are in error since the last read cycle. The counter is inhibited when a DS-3 loss-of-signal or out-of-frame error occurs.

This chapter describes the commands you use to configure the Layer 2 Tunneling Protocol (L2TP) on the PortMaster 4. L2TP allows the PortMaster to tunnel PPP frames from an incoming call across an IP network from one PortMaster that answers the call—an L2TP access concentrator (LAC)—to another PortMaster that processes the PPP frames—an L2TP network server (LNS).

ComOS releases 4.1 and later support LAC and LNS features on the PortMaster 4. ComOS 4.0 and ComOS 4.0.3 support only LAC on the PortMaster 4.

L2TP can be implemented on the PortMaster 4 with or without the call-check feature. If call-check is not enabled, the LAC uses the username and password to retrieve information from the RADIUS server, such as L2TP tunnel information. The LNS uses the username and password to retrieve the user profile. The LAC and the LNS can use the same RADIUS server. If call-check is enabled, the LAC uses the called station ID and/or the calling-station ID to determine if it should accept the call. If the LAC accepts the call, it replies with the tunnel information.

To use L2TP, you must add the corresponding L2TP and call-check attributes to the RADIUS dictionary.

The PortMaster 4 supports the LNS board on ComOS 4.1 and later releases. The LNS board terminates up to 500 concurrent L2TP sessions over multiple L2TP tunnels. Up to nine LNS boards can be installed in a PortMaster 4. For information about installing the LNS board, see the *PortMaster 4 Installation Guide*.

For additional information about configuring L2TP on the PortMaster 4, see the ComOS 4.1 release notes.

Displaying L2TP Diagnostic Information

To display L2TP debug information on the console, use the following commands:

- **set console**—see page 2-16

- **set debug l2tp**—see page 14-9

When finished, use the following commands:

- **set debug off**—see page 14-6

- **reset console**—see page 2-13

To display L2TP session information or line status, use the following commands:

- **show l2tp**

- **show global**—see page 2-26

- **show** *S0*—see page 2-34

Summary of L2TP Commands

Table 17-1 shows the L2TP configuration commands.

Table 17-1   L2TP Commands

Command Syntax	
`create l2tp tunnel udp` *Endpoint* [*Password*|**none**]	- see page 17-2
`reset l2tp` [**stats**|**tunnel** *Number*]	- see page 17-3
`set call-check on`|**off**	- see page 3-6
`set debug l2tp max`|**packets** [*Bytes*]|**rpc**|**setup**|**stats** **on**|**off**	- see page 14-9
`set l2tp authenticate-remote on`|**off**	- see page 17-5
`set l2tp choose-random-tunnel-endpoint on`|**off**	- see page 17-6
`set l2tp-lac enable`|**disable**	- see page 17-7
`set l2tp noconfig`|**disable**|**enable** {**lac**|**lns**}	- see page 17-4
`set l2tp secret` [*Password*|**none**]	- see page 17-8
`show l2tp global`|**sessions**|**stats**|**tunnels**	- see page 17-8

L2TP Commands

`create l2tp tunnel`

This command manually establishes an L2TP tunnel for the entire PortMaster 4 for testing and troubleshooting.

> 4.1

   `create l2tp tunnel udp` *Ipaddress* [*Password*\|**none**]

Ipaddress	IP address of the L2TP tunnel endpoint expressed in dotted decimal notation.
Password	Optional password that the PortMaster 4 uses to authenticate itself when responding to a tunnel request from the L2TP endpoint.
none	Sets the PortMaster 4 to use the L2TP secret configured for it with the **set l2tp secret** command. This is the default.

Usage

Use this command for testing and troubleshooting L2TP. It is global for the entire PortMaster 4.

Example

```
Command> create l2tp tunnel udp 149.198.110.19
OK
```

See Also

set l2tp - page 17-4
set l2tp secret - page 17-8

reset l2tp

This command resets active L2TP tunnels and sessions or resets the L2TP statistics counter for the entire PortMaster 4.

> 4.1

reset l2tp [**stats**|**tunnel** *Number*]

stats	Resets L2TP counters displayed by the **show l2tp stats** command to zero. Using this command does not reset active L2TP sessions.
tunnel *Number*	Resets the specified tunnel. To view L2TP tunnel numbers, use the **show l2tp tunnels** command.
	Number is an integer between 1 and 100. If no tunnel number is specified, all L2TP tunnels are reset.

Usage

To reset all L2TP tunnels and terminate all PPP sessions, enter **reset l2tp** with no arguments.

Example

```
Command> reset l2tp stats
Command>
```

See Also

show l2tp - page 17-8

set l2tp

This command enables and disables L2TP features on the entire PortMaster 4 or on a particular line board.

`4.1` >   **set l2tp noconfig|disable|enable {lac|lns}**

noconfig   Sets the entire PortMaster 4 to have no L2TP configuration if set globally on the manager module. A line board set with **noconfig** has no L2TP configuration of its own, but inherits from the system manager module if the manager is configured for L2TP.

However, if the manager module is set with **noconfig** or is not configured for L2TP, the line board cannot inherit its configuration.

disable   Disables L2TP on the entire PortMaster 4 if set globally on the manager module. If set on a line board, **disable** turns off L2TP on that board and prevents the board from inheriting the L2TP configuration of the manager module.

enable lac   Enables the entire PortMaster 4 as a LAC if set globally on the manager module. If set on a Quad T1 or Tri E1 board, this option enables the board as a LAC. A LAC can answer calls and process them using L2TP.

enable lns   Enables the entire PortMaster 4 as an LNS if set globally on the manager module. If set on a Quad T1, Tri E1, or LNS board, this option enables the board as an LNS. On an LNS, any line ports are automatically set as T1 or E1 ports and can no longer be used for dial-in. The virtual *S0* ports become *W1* ports.

Usage

You must first select a slot for configuration using the **set view** command. Setting the view to the manager module sets the L2TP configuration globally for the entire PortMaster 4. If you do not configure a Quad T1, Tri E1, or LNS board for L2TP, the board inherits the L2TP configuration of the manager module.

Using this command on a Quad T1, Tri E1, or LNS board overrides the global setting.

To activate the new configuration, you must use the **save all** command and reboot the manager module or reset the slot if configuring a Quad T1, Tri E1, or LNS board.

A board on the PortMaster 4 can be enabled as either a LAC or LNS, but not as both.

L2TP and RADIUS Accounting. Both the LAC and LNS log any user sessions to RADIUS accounting. If you are using the RADIUS call-check feature to establish the L2TP tunnel, the LAC's accounting data contains only the calling line ID (CLID)

information, not the username, because that information has not yet been passed on the link. The LNS accounting data shows both the CLID and username in its accounting data along with the assigned IP address.

If partial authentication instead of call-check is taking place on the LAC, then the username might be available to it. In that case, the username appears in the RADIUS accounting logs for both the LNS and the LAC.

In both cases, the LNS displays NAS-Port-Type as **virtual**, while the LAC displays the NAS-Port-Type set to the actual physical interfaces connection type—the normal behavior of the network access server.

Examples

```
Command> set view 0
View changed from 4 to 0
Command 0> set l2tp disable
Command> save all
Command> reset slot

Command> set view 0
View changed from 4 to 0
Command 0> set l2tp enable lac
L2TP lac will be enabled after next reboot
Command> save all
Command> reset slot
```

See Also

set call-check - page 3-6
set l2tp-authenticate remote - page 17-5
show l2tp - page 17-8

set l2tp authenticate-remote

This command sets the PortMaster 4 to initiate L2TP tunnel authentication.

> 4.1

    set l2tp authenticate-remote on|off

on	Sets the PortMaster 4 to initiate authentication with the other side of the L2TP connection before it creates the tunnel.
off	Disables the PortMaster 4 from initiating authentication.

Usage

This command configures the PortMaster 4 to initiate authentication before establishing a tunnel, but does not determine how the PortMaster responds to an authentication request.

Example

Command> **set l2tp authenticate-remote on**
OK

See also

set l2tp - see page 17-4

set l2tp choose-random-tunnel-endpoint

This command determines the order in which the PortMaster 4 chooses a tunnel end point when multiple tunnel end points are set for a user.

> **set l2tp choose-random-tunnel-endpoint on|off**

4.1
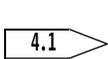
on	Sets the PortMaster 4 to choose the tunnel end point randomly from the list of tunnel end points returned by RADIUS.
off	Sets the PortMaster 4 to select a tunnel end point serially.

Usage

This command changes the way the PortMaster 4 selects a tunnel end point when multiple end points are set for a user. By default, the PortMaster 4 selects the tunnel end point serially.

You can configure a RADIUS user profile to support up to three L2TP redundant end points—the LAC discards any additional end points. See the ComOS release notes for additional information.

Note – The PortMaster 4 supports up to three L2TP end points.

Example

Command> **set l2tp choose-random-tunnel-endpoint on**
OK

See Also

set l2tp - see page 17-4

set l2tp-lac

This command enables and disables L2TP access concentrator (LAC) features on a PortMaster 4.

> **4.0**
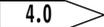
    set l2tp-lac enable|disable

enable	Enables LAC on a line board of the PortMaster 4 running ComOS 4.0.
disable	Disables LAC on a line board of the PortMaster 4. This is the default.

Usage

Note – The PortMaster 4 supports this command only on ComOS release 4.0. To enable LAC features on a PortMaster 4 running ComOS 4.1, use the **set l2tp enable lac** command.

L2TP can be implemented on the PortMaster 4 with or without the RADIUS call-check feature enabled. If call-check is disabled, the LAC uses the username and password to retrieve information from the RADIUS server, such as L2TP tunnel information. The LAC and the LNS can use the same RADIUS server.

You must enable the corresponding L2TP and RADIUS call-check attributes on the RADIUS server to activate L2TP. For more information about configuring L2TP, refer to the ComOS 4.1 release notes.

To establish an L2TP session on a PortMaster 4, you must first use the **save all** and **reset slot** commands after enabling the LAC feature.

Example

```
Command> set l2tp-lac enable
Command succeed
Command> save all
Command> reset slot
```

See Also

set call-check – page 3-6

set l2tp enable lac - page 17-4

set l2tp secret

This command sets the password used by the PortMaster 4 to respond to L2TP tunnel authentication requests.
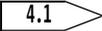
| 4.1 ⊳ | **set l2tp secret** [*Password*|**none**] |

| *Password* | Sets the global password that the PortMaster 4 uses to respond to L2TP tunnel authentication requests. *Password* is a string of up to 15 ASCII characters. |
| **none** | Disables the global L2TP password on the PortMaster 4. This is the default. |

Usage

This command sets a global L2TP password for the entire PortMaster 4.

Note – You cannot override this global command by configuring a secret on a Quad T1 or Tri E1 board.

However, if a PortMaster 4 configured as a LAC receives a tunnel authentication request, it uses the Tunnel-Password value from the RADIUS access-accept, if present, instead of the global L2TP secret. See the ComOS 4.1 release notes for additional information.

Example

```
Command> set l2tp secret isotopes
New secret: isotopes
```

See Also

set l2tp - page 17-4

show l2tp

This command displays information about active L2TP sessions for the entire PortMaster 4.
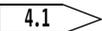
| 4.1 ⊳ | **show l2tp global|sessions|stats|tunnels** |

| **global** | Displays global L2TP settings. |

sessions	Displays information about active L2TP sessions.
stats	Displays L2TP statistics.
tunnels	Displays information about L2TP tunnels such as the tunnel identification number, assigned ID, tunnel ID, and port name.

Examples

```
Command> show l2tp global
debug packets debug stats debug setup Tunnel Authentication Enabled
Initiation of Authentication Remote Tunnel Disabled
Default Board configuration
```

```
Command> show l2tp sessions
 Id           Assign-Id      Tunnel-Id      Portname
 2305         1              1              S0
```

```
Command> show l2tp stats
```

NEW_SESSION	1
NEW_TUNNEL	4
TUNNEL_CLOSED	3
HANDLE_CLOSED	3
L2TP_STATS_MEDIUM_HANDLE	3
INTERNAL_ERROR	14
CTL_SEND	9
CTL_REXMIT	1
CTL_RCV	10
MSG_CHANGE_STATE	4
WRONG_AVP_VALUE	3
EVENT_CHANGE_STATE	3

```
Command> show l2tp tunnels
```

Id	Assign-Id	Hnd	State	Server-Endpoint	Client-Endpoint
1	1	24	L2T_ESTABLISHED	192.168.6.13	192.168.10.28

Basic Commands   A

Table A-1 lists the basic PortMaster commands. Some are complete commands; others require additional keywords or values as described in this reference.

Table A-1   Basic PortMaster Commands

Command	Description
add	Adds an entry to a PortMaster table.
attach	Allows you to communicate directly to a device attached to a specified asynchronous or ISDN PortMaster port.
clear	Deletes an entry.
copy	Copies the files in the nonvolatile file system across directories.
create	Creates an entry.
delete	Deletes an entry from a PortMaster table.
dial	Begins dialing to the specified network location.
erase	Removes all or part of nonvolatile RAM.
get	See **tftp get**.
help	Provides information on each of the commands, including usage and syntax.
ifconfig	Displays configuration values for all interfaces.
ping	Sends an Internet Control Message Protocol (ICMP) echo request packet to test connectivity.
pmlogin	Establishes a login using the PortMaster login service to a specified host on the network.
ptrace	Displays packet traffic passing through the PortMaster, using the specified filter.
quit, done, or **exit**	Exits the command line interface.
reboot	Reboots, using the currently saved configuration.
reset	Resets a specific physical or virtual port (or ports) to the current default configuration, and drops any active sessions on the port.
rlogin	Establishes a login using the **rlogin** service to a specified host on the network.
save	Writes the current configuration to PortMaster nonvolatile RAM.
set	Configures a value on a port, or configures a value globally, for a PortMaster table, or for a protocol.

Table A-1   Basic PortMaster Commands *(Continued)*

Command	Description
show	Shows the status of each specified port, file, filter, board, slot, PortMaster table, and so on, or the global configuration.
telnet	Connects via Telnet from the PortMaster to a specified host on the network.
tftp get	Retrieves a file of configuration commands or a ComOS image from a host using the Trivial File Transfer Protocol (TFTP).
traceroute	Traces network routes to show a connectivity path.
version	Displays the version number of the ComOS software that runs the PortMaster, and the uptime since the last boot.
!!	Repeats the last command.

TCP and UDP Ports and Services B

Table B-1 lists port numbers—**well-known ports**—assigned to TCP and UDP services—**well-known services**—by the Internet Assigned Numbers Authority (IANA). A more complete list is available in RFC 1700, *Assigned Numbers*.

Table B-1   TCP and UDP Ports and Services

Service	Port	Protocol	Description
ftp-data	20	TCP	File Transfer Protocol (FTP) (default data)
ftp	21	TCP	FTP (control)
telnet	23	TCP	Telnet
smtp	25	TCP	Simple Mail Transfer Protocol (SMTP) (email)
nicname	43	TCP	**whois** Internet directory service
nicname	43	UDP	**whois** Internet directory service
domain	53	TCP	Domain Name System (DNS)
domain	53	UDP	DNS
tftp	69	UDP	Trivial File Transfer Protocol (TFTP)
gopher	70	TCP	Gopher
gopher	70	UDP	Gopher
finger	79	TCP	Finger Protocol
finger	79	UDP	Finger Protocol
www-http	80	TCP	World Wide Web Hypertext Transfer Protocol (HTTP)
kerberos	88	TCP	Kerberos authentication
kerberos	88	UDP	Kerberos authentication
pop3	110	TCP	Post Office Protocol (POP) version 3
sunrpc	111	TCP	SUN Remote Procedure Call (RPC)
sunrpc	111	UDP	SUN RPC
auth	113	TCP	Authentication service
auth	113	UDP	Authentication service
nntp	119	TCP	Network News Transfer Protocol (NNTP)
ntp	123	TCP	Network Time Protocol (NTP)
ntp	123	UDP	NTP
snmp	161	TCP	Simple Network Management Protocol (SNMP)
snmp	161	UDP	SNMP
snmptrap	162	TCP	SNMP system management messages
snmptrap	162	UDP	SNMP system management messages
imap3	220	TCP	Interactive Mail Access Protocol (IMAP) version 3
imap3	220	UDP	IMAP version 3
exec	512	TCP	Remote process execution
login	513	TCP	Remote login

Table B-1   TCP and UDP Ports and Services *(Continued)*

Service	Port	Protocol	Description
who	513	UDP	Remote **who** daemon (**rwhod**)
cmd	514	TCP	Remote command (**rsh**)
syslog	514	UDP	System log facility
printer	515	TCP	Line printer daemon (LPD) spooler
talk	517	TCP	Terminal-to-terminal chat
talk	517	UDP	Terminal-to-terminal chat
ntalk	518	TCP	Newer version of Terminal-to-terminal chat
router	520	UDP	Routing Information Protocol (RIP)
uucp	540	TCP	UNIX-to-UNIX Copy Protocol (UUCP)
uucp	540	UDP	UUCP
uucp-rlogin	541	TCP	Variant of UUCP/TCP
uucp-rlogin	541	UDP	Variant of UUCP/IP
klogin	543	TCP	Kerberized login
klogin	543	UDP	Kerberized login
pmd	1642	TCP	PortMaster daemon **in.pmd**
pmconsole	1643	TCP	PortMaster Console Protocol
radius	1645	UDP	Remote Authentication Dial-In User Service (RADIUS)
radacct	1646	UDP	RADIUS accounting
choicenet	1647	UDP	ChoiceNet
l2tp	1701	UDP	Layer 2 Tunneling Protocol

Command Values   C

Table C-1 describes the values (arguments) that are used in PortMaster commands. These values must be replaced in the commands with appropriate values for your specific needs. For example, in the command **add filter** *Filtername*, replacing the value *Filtername* with the name **inet.in** adds a new filter named **inet.in** to the filter table.

Table C-1   Command Line Values

Value	Represents	Format and/or Value(s)
Alarm-id	Specific instance of an SNMP alarm.	Number.
Area	OSPF area.	Decimal or dotted decimal notation.
ASN	Autonomous system number.	A 16-bit number ranging from 1 to 65535.
Bytes	Number of bytes.	Integer 0 or higher.
Cgroup	Group of channels.	1 through 63.
Channel	T3 channel.	1 through 28.
Channel-list	Series of one or more channel numbers.	• For T1, any number(s) from 1 through 24, separated by spaces. • For E1, any number(s) from 1 through 30, separated by spaces.
C0	Asynchronous console port.	**c0** or **c1** on the PortMaster 4.
CommandName	Name of a ComOS command.	One of the general commands. See Chapter 2.
Device	Name of network device or pseudo-tty on a UNIX host.	**/dev/ttyp0**, or **/dev/network.**
Dlci	Data link connection identifier (DLCI) number.	1 through 1023.
Ether0	Ethernet interface.	• **ether0**, **ether1,** or **ether***Slotnumber***0**|**1** on the PortMaster 4 • Defaults to **ether0** if omitted.
Facility.Priority	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 3-23 for more information.

Table C-1   Command Line Values *(Continued)*

Value	Represents	Format and/or Value(s)
Filename	Name of a file in the PortMaster 4 subdirectory.	String of up to 16 characters.
Filtername	Name of an input or output packet filter.	String of up to 15 printable, nonspace, ASCII characters.
Group	Number of a group.	Integer from 0 to 100; 0 is default.
Handle	Network identifier.	**n** followed by a number, with no space in between.
Hex	Number in hexadecimal (hex) notation.	Hex number with leading **0x**.
Identifier	T1 interface in an NFAS group.	Integer between 0 and 19.
Interface	Interface specification.	For example, **ether0**, **frm1**, **ptp1**, **frmw1**, or **ptpw1**.
Ipaddress	IP address or hostname.	Dotted decimal notation or 39-character hostname.
Ipmask	IP subnet mask—also called a **netmask**.	Dotted decimal notation with ones in high-order bits, and zeros in low-order bits.
Ipxgateway	IPX gateway address.	32-bit hex number.
Ipxhost	IPX host address.	48-bit hex number. On PortMaster products, this is usually the media access control (MAC) address.
Ipxnetwork	IPX network number.	32-bit number.
Itype	ICMP packet type.	0 or higher.
Line0	T1 or E1 line.	**line0, line1**, **line2**, or **line3** on a PortMaster 4**.**
ListName	Name of a list of source or destination sites used for packet filters.	String of up to 15 printable, nonspace, ASCII characters.
Locname	Name of an internetwork dial-out destination.	String of up to 12 printable, nonspace, ASCII characters.
Logtype	One of five areas used for logging with the **set syslog** command.	The alternatives are **admin-logins**, **user-logins**, **packet-filters**, **commands**, and **termination**.
M0	Digital modem number.	**m0** through **m95**.
MTU	Maximum transmission unit. Maximum packet size, in bytes, that an interface can send.	Integer from 100 to 1520.
Metric	Hop count to a remote destination.	Integer from 1 to 15.

Table C-1   Command Line Values *(Continued)*

Value	Represents	Format and/or Value(s)
Minutes	Number of minutes.	Integer from 0 to 240.
ModemName	**User-defined** long or short name for a modem in the modem table.	Printable ASCII characters.
NM	Alternative netmask notation. Number of high-order bits set to 1.	**/n** where **n** is an integer from 0 to 32.
Number	Quantity.	Any number 0 or higher.
Password	PortMaster administrative password.	String of up to 15 printable, nonspace, ASCII characters.
Policyname	Name of a BGP policy statement.	String of up to 16 printable, nonspace, ASCII characters.
Prefix	IP prefix address.	Dotted decimal notation with ones in high-order bits, and zeros in low-order bits.
Profile	Type of Multifrequency R2 (MFR2) inband signaling for channelized E1.	Integer between 0 and 4.
Protocol	Type of routing protocol.	**bgp**, **ospf**, **rip**, or **static**.
RuleNumber	Number indicating the order of a filter rule or a BGP policy statement.	Integer between 1 and 256 for the PortMaster 4.
S0	Any virtual ISDN PRI synchronous port.	**s0** through **s95**, depending on the PortMaster 4 model.
Seconds	Number of seconds.	Any number 0 or higher; note that 1 has special meaning for idle timeout commands.
Slotnumber	Slot number in the PortMaster 4.	Integer between 0 and 16. Slots 0 through 9 are physical slots in the PortMaster 4 chassis. A slot number greater than 9 indicates a virtual slot.
String	Character string.	One or more characters in the ASCII printable character set.
Subdirectory	Path of a file in a PortMaster 4 subdirectory.	String of up to 16 characters.
Tag	Community attribute used to identify a BGP community.	A 32-bit number, two 16-bit numbers, or a reserved community keyword.

Table C-1   Command Line Values *(Continued)*

Value	Represents	Format and/or Value(s)
Ticks	Number of 50ms increments of time required to send a packet to the destination network.	Integer.
Tport	TCP/IP port.	Integer from 1 to 65535.
Uport	User Datagram Protocol (UDP)/IP port.	Integer from 0 to 65535.
Username	Name of user.	String of up to 8 printable ASCII characters.
W1	Any virtual synchronous WAN port.	**w0** through **w95** on the PortMaster 4

Command Index

Subject Index

L

V

X