PortMaster®

Troubleshooting Guide

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

June 1998

950-1192A

Copyright and Trademarks

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

Disclaimer

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

Contents

About This Guide

The *PortMaster® Troubleshooting Guide* can be used to identify and solve software and hardware problems in the Lucent Remote Access PortMaster family of products.

Audience

This guide is designed to be used by system administrators and network managers with knowledge of basic networking concepts.

PortMaster Documentation

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

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

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

- *ChoiceNet® Administrator's Guide*

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

- *PortMaster Command Line Reference*

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

- *PortMaster Configuration Guide*

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

- PortMaster hardware installation guides

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

- *PMconsole™ for Windows Administrator's Guide*

  This guide covers PMconsole Administration Software for Microsoft Windows, a graphical tool for configuring the PortMaster. The majority of the material in this guide also applies to the UNIX version of PMconsole.

  Lucent recommends that you use the Java graphical user interface (GUI) PMVision™ rather than PMConsole to configure and manage a PortMaster.

- *PortMaster Routing Guide*

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

- *RADIUS Administrator's Guide*

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

Additional References

RFCs

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

RFC 768, *User Datagram Protocol*
RFC 791, *Internet Protocol*
RFC 792, *Internet Control Message Protocol*
RFC 793, *Transmission Control Protocol*
RFC 854, *Telnet Protocol Specification*
RFC 950, *Internet Standard Subnetting Procedure*
RFC 1058, *Routing Information Protocol*
RFC 1112, *Host Extensions for IP Multicasting*
RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links*
RFC 1157, *A Simple Network Management Protocol (SNMP)*
RFC 1166, *Internet Numbers*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*
RFC 1256, *ICMP Router Discovery Messages*
RFC 1321, *The MD5 Message-Digest Algorithm*
RFC 1331, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*
RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
RFC 1334, *PPP Authentication Protocols*
RFC 1349, *Type of Service in the Internet Protocol Suite*
RFC 1413, *Identification Protocol*
RFC 1490, *Multiprotocol Interconnect Over Frame Relay*
RFC 1541, *Dynamic Host Configuration Protocol*
RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*
RFC 1552, *The PPP Internet Packet Exchange Control Protocol (IPXCP)*
RFC 1587, *OSPF NSSA Options*
RFC 1597, *Address Allocations for Private Internets*
RFC 1627, *Network 10 Considered Harmful (Some Practices Shouldn't be Codified)*
RFC 1634, *Novell IPX Over Various WAN Media (IPXWAN)*
RFC 1661, *The Point-to-Point Protocol (PPP)*
RFC 1700, *Assigned Numbers*
RFC 1771, *A Border Gateway Protocol 4 (BGP-4)*
RFC 1812, *Requirements for IP Version 4 Routers*
RFC 1814, *Unique Addresses are Good*
RFC 1818, *Best Current Practices*
RFC 1824, *Requirements for IP Version 4 Routers*
RFC 1825, *Security Architecture for the Internet Protocol*
RFC 1826, *IP Authentication Header*
RFC 1827, *IP Encapsulating Payload*
RFC 1828, *IP Authentication Using Keyed MD5*
RFC 1829, *The ESP DES-CBC Transform*
RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1878, *Variable Length Subnet Table for IPv4*
RFC 1918, *Address Allocation for Private Internets*
RFC 1965, *Autonomous System Confederations for BGP*
RFC 1966, *BGP Route Reflection, An Alternative to Full Mesh IBGP*
RFC 1974, *PPP Stac LZS Compression Protocol*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 1997, *BGP Communities Attribute*
RFC 2003, *IP Encapsulation within IP*
RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*

RFC 2125, *The PPP Bandwidth Allocation Protocol (BAP), The PPP Bandwidth Allocation Control Protocol (BACP)*
RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*
RFC 2139, *RADIUS Accounting*
RFC 2178, *OSPF Version 2*

Books

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

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

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

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

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

Document Conventions

The following conventions are used in this guide:

Convention	Use	Examples
Bold font	Indicates a user entry—a command, menu option, button, or key—or the name of a file, directory, or utility, except in code samples.	• Enter **version** to display the version number. • Press **Enter**. • Open the **permit_list** file.

Convention	Use	Examples
Italic font	Identifies a command-line placeholder. Replace with a real name or value.	• **set** *Ether0* **address** *Ipaddress* • Replace *Area* with the name of the OSPF area.
Square brackets ([ ])	Enclose optional keywords and values in command syntax.	• **set nameserver** [**2**] *Ipaddress* • **set** *S0* **destination** *Ipaddress* [*Ipmask*]
Curly braces ({ })	Enclose a required choice between keywords and/or values in command syntax.	**set syslog** *Logtype* {[**disabled**] [*Facility.Priority*]}
Vertical bar (|)	Separates two or more possible options in command syntax.	• **set** *S0*|*W1* **ospf on**|**off** • **set** *S0* **host default**|**prompt**|*Ipaddress*

Document Advisories

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

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

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

Contacting Lucent Remote Access Technical Support

The PortMaster comes with a 1-year hardware warranty.

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

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

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

For the EMEA Region

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

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

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

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

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

- By voice, dial 800-458-9966 within the United States (including Alaska and Hawaii), Canada, and the Caribbean, or +1-925-737-2100 from elsewhere.
- By fax, dial +1-925-737-2110.
- By email, send mail as follows:

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

PortMaster Training Courses

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

Subscribing to PortMaster Mailing Lists

Lucent maintains the following Internet mailing lists for PortMaster users:

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

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

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

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

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

Solving Hardware Problems 1

Use Table 1-1 to identify and diagnose common hardware problems.

Table 1-1 Common Hardware Problems

Problem	**Possible Cause**	**Possible Solution**
The **show** *S0* command shows two different port states on an asynchronous port.	Asynchronous ports were configured before cables and modems were attached.	Verify the port state as explained on page 1-2.
The **show** *S0* or **show** *W1* command shows a high number of line errors occurring on a synchronous or asynchronous port.	• Cable or connector failure. • Too much distance between the devices on the network. • Incorrect cables are installed.	Use **show** *S0* or **show** *W1* to determine that line errors are present (see page 1-2), and follow the steps in "Diagnosing Line Errors" on page 1-4.
The Ethernet port is not communicating with the network.	Incorrect configuration on the Ethernet port.	See "Diagnosing Ethernet Port Problems" on page 1-7.
Unspecified Ethernet problems are occurring.	Incorrect DIP switch position.	See "DIP Switch Position" on page 1-8 for a list of settings.
Ethernet port and DIP switch configuration is correct, but the Ethernet is still not working.	Malfunctioning external hardware.	See "Diagnosing Faulty Ethernet Hardware" on page 1-9.
The network is slow.	Overloaded network.	See "Diagnosing an Overloaded Ethernet Network" on page 1-12.
Data arrives at its destination in a corrupted state.	Overloaded network.	See "Diagnosing an Overloaded Ethernet Network" on page 1-12.

Table 1-1 Common Hardware Problems *(Continued)*

Problem	Possible Cause	Possible Solution
All external Ethernet hardware is functioning correctly, but the Ethernet is still not working.	Loose Ethernet daughterboard.	See "Diagnosing Ethernet Daughterboard Problems" on page 1-14.

Diagnosing Synchronous and Asynchronous Port Problems

The PortMaster records statistics and keeps a count of errors detected on its synchronous and asynchronous ports. Use **show** commands to display the current error count and status on a port, and correct problems as instructed in the following sections.

Disable a synchronous hardwired port (see page 1-6), if necessary.

Displaying Port Errors and Status

The **show** *W1* command displays status information for synchronous ports, and the **show** *S0* command displays status information for asynchronous ports. Analyze the type and number of port errors to help diagnose port problems. For more information on **show** command output, see the *PortMaster Command Line Reference*.

Sample synchronous port output:

```
Command> show w1
---------------------- Current Status - Port W1 ---------------------
          Status:   ESTABLISHED
           Input:   915287284                    Abort Errors:   56/1
          Output:   3214289999                     CRC Errors:   27
         Pending:   0                           Overrun Errors:   0
       TX Errors:   0                             Frame Errors:   15
    Modem Status:   DCD+  CTS+
```

Sample asynchronous command output:

```
Command> show s10
---------------------- Current Status - Port S10 --------------------
           Status:   ESTABLISHED
            Input:   1392900                      Parity Errors:   0
           Output:   453743                          CRC Errors:   27
          Pending:   0                            Overrun Errors:   0
        TX Errors:   0                              Frame Errors:   0
     Modem Status:   DCD+  CTS+                     Abort Errors   0
```

Data integrity is directly related to the integrity of OSI Layers 1 (physical) and 2 (data link). High abort, CRC, and frame error rates result in a loss of data integrity and degraded service. Low data link integrity can cause serious connection difficulties.

Abort Errors (Synchronous Port Only)

An abort error occurs when a connection was not established on the synchronous port and the user is trying to connect again. Each time a connection attempt is unsuccessful, the error count increments by 1.

Abort errors are sometimes displayed as two counts separated by a slash:

Abort Errors: *frame errors/ device errors*

- The frame error count increments when
  - The receiver chip reports a frame error.
  - The receiver chip reports an unsuccessful connection attempt.
- The device error count increments when
  - Frame size is 0.
  - Frame size is greater than the maximum size of a Point-to-Point Protocol (PPP) frame.
  - Frames overlap each other.

Frame Errors

Asynchronous frame errors occur when a frame is corrupted in transit—usually because of a hardware failure in a line or modem. A frame is considered invalid if it does not terminate with at least 1 stop bit. If a frame error occurs, the counter is incremented and the PortMaster automatically attempts to resynchronize by identifying the incorrect stop bit as the start bit for the next character. A new character is then constructed beginning with this new start bit.

Synchronous frame errors occur when there is a malfunctioning clock, for example, clock slippage. On synchronous ports, frame errors are sometimes displayed as two numbers separated by a slash:

```
Frame Errors: small packet errors/ large packets errors
```

- The small packet error count increments when the PortMaster receives a packet with too few characters for the frame size.
- The large packet error count increments when the PortMaster receives a packet that is too large for the frame size.

Diagnosing Line Errors

Line errors encompass frame errors, abort errors, and CRC errors. Use the following steps if a large number of line errors appear in the **show** command output:

1. **Determine the rate of line errors.**

   Are line errors incrementing at a constant rate? A constant increase in line errors indicates a hardware failure (cables, connectors, and so on). If the line errors happened all at once, they were probably caused by a single event. For example, unplugging a serial cable from the PortMaster results in a sudden, one-time burst of frame errors.

2. **Determine if the line errors are limited to one port.**

   If you notice that a particular port has numerous line errors, replace the serial cable, device—modem or channel service unit/digital service unit (CSU/DSU), and/or telephone wire with that of another port. If the problem remains on the port, check the PortMaster. If the problem follows the line, begin replacing cables, modems, and so on, to isolate the source of the line errors.

3. **Verify the modem or CSU/DSU.**

   Modems and CSU/DSUs can cause line errors if they are defective or misconfigured. You can use two bit error rate tester (BERT) sets to isolate the problem as well as determine the direction of the errors.

4. **Check the environment.**

   Other devices cause noise that can result in line errors. Be sure to keep your data cables away from fluorescent lights, monitors, magnets, televisions, arc welders, air conditioners, vacuum cleaners, and other noise-producing devices. If possible, identify the communication media the telephone company is using (microwave, satellite, and so on). Different media are affected by weather conditions such as snow, lightning, and fog. These weather effects can include line errors.

5. **Check your serial cables.**

   Ensure that the cable (and possibly the connectors and adapters) between the PortMaster and peripheral devices (such as a modem or a CSU/DSU) is shielded to minimize the noise from other serial cables and power connectors. If the errors are occurring on a synchronous port, verify that you are using Lucent V.35 cables. If the errors are occurring on an asynchronous port, verify that you are using flat ribbon cables—and not Category 5 unshielded twisted pair (UTP) cables. Ensure that cable lengths are within the standard industry recommendations.

6. **Try replacing the cable and/or adapters.**

   Cables and adapters can be faulty. Verify cable, connector, and pin integrity visually, and ensure correct pinout specifications as specified in the hardware installation guide that was shipped with your PortMaster. When replacing cable hardware, change only one part at a time so you can more easily pinpoint the source of the problem. Use store-bought cables, if possible, to prevent human error. Be especially suspicious of DB-25-to-RJ-45 connectors because these often have problems. If you have a synchronous hardwired port, disable it before replacing cables. See “Disabling a Synchronous Hardwired Port” on page 1-6.

7. **Verify the telephone wire and punchdown block.**

   Check the wiring in your building, in the punchdown block, and from the punchdown block to the modem or CSU/DSU. If wiring is faulty (for example, connections are loose or wires are crossed), or you have bare copper or ordinary telephone wiring running for a few feet, the PortMaster is more susceptible to line errors.

8. **Have your lines tested for noise.**

   Telephone lines are susceptible to noise originating at the telephone company. This noise is often the cause of line errors. The telephone company might conduct a noise test for free. Noise can be intermittent, so make a note of when the line errors are occurring. Intermittent noise can be related to the environment, such as rain seeping into poorly sealed cables.

   Keep accurate records of line tests from the day of line commissioning to identify any changes or trends in line integrity that might require a call to the telephone company. If line errors occur during 0.5 and 1 percent of line use, notify the telephone company and request that they run line tests.

Verifying Port State for Old and New Cards

If you configure asynchronous ports before you attach cables and modems, you might see two different port states when you use the **show** *S0* command. Ports on the main system card might show a status of IDLE, while ports on older expansion cards might show a status of USERNAME.

This behavior is normal. On older expansion cards, the value of carrier detect (CD) signal floats high in contrast to the carrier detect signal on the main system card. On more recent expansion cards, the carrier detect signal is pulled low as it is on the main system card.

On both old and new cards, a port should show a status of IDLE when modems are attached with hardware flow control set **and** modem control turned on for the port.

Disabling a Synchronous Hardwired Port

You might need to disable a synchronous hardwired port to diagnose problems with the port. For example, disable a hardwired port when you are replacing cables to diagnose line errors. (See “Diagnosing Line Errors” on page 1-4.)

To disable a synchronous hardwired port, use the following commands:

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

Command> set W1 destination 0.0.0.0
Port W1 destination changed from 255.255.255.255 to 0.0.0.0
```

```
Command> reset W1
Resetting port W1

Command> save all
```

Diagnosing Ethernet Port Problems

When troubleshooting an Ethernet port, use the following procedure:

1. **Ensure that the Ethernet port has an IP address on the same IP network as the rest of your network by using the** show ether0 **command:**

```
Command> show ether0
     Ethernet Status:  IP - Enabled                IPX - Enabled
      Interface Addr:  pm2.edu.com (192.168.96.6)
             Netmask:  255.255.255.0
   Broadcast Address:  192.168.96.0
         IPX Network:  FEEDFEFE
      IPX Frame Type:  ETHERNET_802.3
    Ethernet Address:  00:c0:05:01:06:20
             Routing:  Broadcast, Listen (On)
        Input Filter:
       Output Filter:
```

2. **Ensure that the Ethernet port is using the same netmask as the rest of the network.**

   Connect to another router on the same subnet and check that router's configuration.

3. **Verify the Ethernet address.**

   The Ethernet address shown in the **show ether0** output displays the Ethernet hardware media access control (MAC) address. All PortMaster products have 00:c0:05 as the first three pairs of characters. If the address does not show these characters, or consist of all zeros, the PortMaster EPROM could be faulty. In addition, a faulty network interface card (NIC) on a PC has been known to cause the PortMaster to display all zeros.

4. **If necessary, set the IP address and netmask with the following commands:**

   ```
   Command> set ether0 address Ipaddress
   ```

   ```
   Command> set ether0 netmask Ipmask
   ```

5. **If you are using IPX verify the following:**

   – The IPX network number is the same for all devices attached to the Ethernet port.

   – The IPX frame type is the same for all devices attached to the Ethernet port.

   – IP and/or IPX protocols are enabled.

6. **If necessary, set the IPX network number and frame type with the following commands:**

   ```
   Command> set ether0 ipxnet Ipxnetwork
   ```

   ```
   Command> set ether0 ipxframe
   ethernet_802.2|ethernet_802.2_ii|ethernet_802.3|ethernet_ii
   ```

7. **If necessary, re-enable IP or IPX, use the following commands:**

   ```
   Command> set ether0 ip enabled
   ```

   ```
   Command> set ether0 ipx enabled
   ```

DIP Switch Position

If you are experiencing Ethernet problems, check the DIP switches to ensure that they are in the correct position:

DIP 4	DIP 5	Ethernet
Up	Up	10BaseT (twisted pair)
Up	Down	AUI (10Base5)
Down	Down	BNC (10Base2)

If the DIP switches are not in the correct position, reset them and turn the power off and on.

Note – Office Router models do not have DIP switches 4 and 5. To specify the Ethernet type on an Office Router, set DIP switch 3 down to use AUI or up to use 10BaseT. BNC is not supported on Office Router models.

Try pinging another host on the network and checking the Address Resolution Protocol (ARP) requests to see if you have network connectivity. See "Verifying Network Connections" on page 3-9 for instructions. You can also try pinging the Ether0 interface to verify that it is active.

Diagnosing Faulty Ethernet Hardware

If you suspect faulty hardware is the cause of your Ethernet problem, use the **show netstat** command to display network statistics. If **show netstat** command output points to faulty hardware—cables, connectors, hub, or network interface card (NIC), for example—use the procedures in the following sections to help you isolate the problem. If possible, use Category 5 wire to assure a quality connection.

To use network statistics to determine Ethernet hardware health, do the following:

1. **Enter the following command:**

```
Command> show netstat
  Name      Ipkts     Ierrs     Opkts     Oerrs     Collis    Resets    Queue

  ether0    207757    0         215161    0         223       0         0
```

2. **Note the statistics:**

   – Incoming packet errors (**Ierrs**) and outgoing packet errors (**Oerrs**) can indicate poor conductors—for example, a malfunctioning connector, 10BaseT cable, or AUI transceiver or a faulty BNC terminator.

   – Collisions (**Collis**) greater than 5 percent of total output (**Opkts**) can indicate problems with a cable, hub, NIC, or other Ethernet hardware. Runt packets can result from collisions.

     These statistics can also indicate an overloaded Ethernet network. See "Diagnosing an Overloaded Ethernet Network" on page 1-12.

   – **Resets** can be caused by a malfunctioning Ethernet NIC, hub, or other device, or by a large number of collisions.

Note – A high number of resets in a remote LAN usually indicate that the PortMaster is not properly connected to an Ethernet LAN because DIP switches are not set for the type of Ethernet you are using. See "DIP Switch Position" on page 1-8 to fix this problem.

3. **If network statistics indicate faulty Ethernet hardware, use the procedures in the following sections to isolate and solve the problem.**

   In most of these procedures, you isolate the failure by replacing each possibly faulty component with one that you know is working. If you have a combination of Ethernet types, you must verify each type separately.

4. **If replacing Ethernet hardware does not solve the problem, try using another Ethernet type, if possible—for example, replace 10BaseT with BNC (10Base2).**

   The PortMaster might have a faulty Ethernet bus on its network interface card (NIC). Because AUI (10Base5) and BNC use a different Ethernet bus from 10BaseT, these types can function when 10BaseT does not, and vice versa.

   If this behavior occurs, call Lucent Remote Access Technical Support.

Checking 10BaseT (RJ-45, Twisted Pair) Hardware

Use the following procedure to check 10BaseT Ethernet external hardware. After each step, ping another host on the network and check for ARP requests. (See "Verifying Network Connections" on page 3-9)

1. **Verify that you are using a Category 5 twisted pair cable with an RJ-48C DB modular connector.**

2. **Verify that the link status LEDs on the PortMaster and the hub for the associated port are lit.**

   If the LEDs are not lit, there might be a problem with link integrity. Verify the following:

   – DIP switch positions are correct (see page 1-8).

   – 10BaseT cable is functioning and properly connected to the PortMaster and the hub.

3. **Replace the Ethernet cable with a working cable.**

4. **Move the Ethernet cable to a different, working port on the Ethernet hub.**

5. **Replace the hub with a working hub.**
6. **Make sure that the cables are securely crimped into their connectors.**

Checking BNC (10Base2, Coaxial, Thinnet) Hardware

Use the following procedure to check BNC Ethernet external hardware. After each step, ping another host on the network and check for ARP requests. (See "Verifying Network Connections" on page 3-9)

1. **Verify that you are using a RG-58 A/U 50-ohm coaxial cable, and that it is securely in place.**

   BNC connectors often come undone.

2. **Verify that you are using T-connectors on all BNC Ethernet connections.**
3. **Verify that 50-ohm terminator caps are installed on the ends of the Ethernet cable(s).**
4. **Replace T-connectors with working T-connectors.**
5. **Replace terminators with working terminators.**
6. **Replace cables with working cables.**

Checking AUI (10Base5, Ethernet D, Thicknet) Hardware

Use the following procedure to check AUI Ethernet external hardware. After each step, ping another host on the network and check for ARP requests. (See "Verifying Network Connections" on page 3-9.)

1. **Verify that you are using an RG-11 50-ohm coaxial cable with a DB-15 female connector.**
2. **Verify that DIP switches are correctly set.**
3. **Replace cables with working cables.**
4. **Make sure that any signal quality editor (SQE) switches on AUI transceivers are turned off.**
5. **Replace transceivers with working transceivers.**
6. **Make sure connections to transceivers are secure.**

Diagnosing an Overloaded Ethernet Network

To determine if an overloaded network is causing Ethernet problems, do the following:

1. **Enter the following command:**

```
Command> show netstat
  Name      Ipkts     Ierrs     Opkts     Oerrs     Collis    Resets    Queue
  ether0    207757    0         215161    0         223       0         0
```

2. **Check the collision (Collis) count and determine the collision rate.**

   Compute the collision rate (also known as the saturation rate) by using the following equation:

   number of collisions (Collis)/number of output packets (Opkts)

   A number of collisions greater than 5 percent of the total output (**Opkts**) indicates either an overloaded network or an Ethernet hardware failure—a problem with a cable, hub, or network interface card (NIC), for example.

   Table 1-2 helps you determine Ethernet condition from collision rates, errors, and resets.

Note – The Ethernet traffic throughput expressed in Table 1-2 is a percentage of the total possible throughput (10Mbps). Your LAN might be able to handle a collision rate of 30 percent to 60 percent during short traffic bursts, but might not be able to sustain this rate.

Table 1-2 Ethernet Conditions

show netstat **Output**					
Ierrs	**Oerrs**	**Resets**	**Collision Rate**	**Ethernet Traffic Throughput**	**Ethernet Condition**
0	0	0	Less than 1%	0% to 10%	**Excellent**
0	0	0	1 to 5%	10% to 25%	**Good**
0	0	0	5 to 10%		**Marginal**
1 to 9	1 to 9	1 to 9	Above 10%	Above 25%	**Poor**
10+	10+	10+	Above 10%		**Unsatisfactory**
10+	10+	1 or more/hour	Above 30%		**Inoperative**

3. **If necessary, verify that Ethernet hardware is operational.**

   See "Diagnosing Faulty Ethernet Hardware" on page 1-9.

4. **If the network is overloaded, do one of the following to reduce traffic on the network:**

   – If your Ethernet has a passive hub, install a switching hub instead. This type of hub causes the PortMaster to receive only broadcasts and packets specifically addressed to it. A switching hub has a 10Mbps network link and does not share the link as passive hubs do. The PortMaster does not monitor traffic for all the other hosts on the local network.

   – Remove hosts from the LAN.

   – Segment the network with routers.

Diagnosing Ethernet Daughterboard Problems

Note – The following procedure applies to the PM-2, PM-25, and IRX PortMaster models only.

Once you have verified all your other Ethernet hardware (port, cables, hubs transceivers, T-connectors, terminators), inspect the Ethernet daughterboard inside the PortMaster chassis.

Warning – Do not attempt this procedure if you are unfamiliar with servicing computer hardware.

To inspect the Ethernet daughterboard inside the PortMaster chassis, do the following:

1. **Turn off the PortMaster.**
2. **Unplug the PortMaster power cord.**
3. **Disconnect all cables from the PortMaster.**
4. **Remove the single screw at the top center of the back panel of the PortMaster with a Phillips screwdriver.**
5. **With both hands, gently push the cover forward to dislodge it from the PortMaster.**
6. **If you are checking a PortMaster 3, remove the motherboard by removing the two screws.**
7. **Visually inspect the Ethernet daughterboard mounted below the main board.**

   Check to see that it is securely mounted and that the Ethernet daughterboard is connected to the main board.
8. **If the Ethernet daughterboard appears to be loose, reseat it.**
9. **If you are checking a PortMaster 3, replace the motherboard and tighten the two screws.**
10. **Reinstall the cover on the PortMaster and replace the screw in the back panel.**
11. **Connect all required cables to the PortMaster.**
12. **Plug in the power cord and turn the PortMaster on.**

Solving Administrative Problems 2

Use to identify and diagnose common administrative problems.

Table 2-1 Common Administrative Problems

Problem	**Possible Cause**	**Possible Solution**
The PortMaster is behaving erratically.	• Corrupted configuration.	• Reset the configuration to factory defaults (page 2-4).
	• Corrupted NVRAM.	• Erase and reload ComOS (page 2-5).
Unusual output is displayed in **show** commands.	Corrupted ComOS.	Erase and reload ComOS (page 2-5).
The PortMaster does not display the **login:** prompt when booting.	Corrupted ComOS.	Netboot (page 2-7).
The PortMaster reports a checksum error when booting.	Corrupted ComOS.	• Erase and reload ComOS (page 2-5).
		• Netboot (page 2-7).
You have tried to upgrade ComOS without success.	Failing NVRAM.	Erase and reload ComOS (page 2-5). Try three times.
You have tried to upgrade ComOS three times without success.	Corrupted ComOS.	Netboot (page 2-7).
The PortMaster cannot boot.	Corrupted ComOS or configuration.	Boot from PROM (page 2-13).
You cannot remember the administrative password.		Override and replace the password (page 2-20).

Table 2-1 Common Administrative Problems *(Continued)*

Problem	Possible Cause	Possible Solution
Dial-in users are having trouble authenticating.	Incorrect user table configuration, misconfigured port, or RADIUS problem.	See "Diagnosing Authentication Problems" on page 2-21. To diagnose port configuration problems, use the **show** *S0* command and refer to the *PortMaster Configuration Guide*. For RADIUS problems, see the *RADIUS Administrator's Guide*.

Erasing the NVRAM, ComOS, or the Configuration

The operating system (ComOS) and configuration of the PortMaster are stored in nonvolatile RAM (NVRAM). The NVRAM (also referred to as Flash or Flash RAM) is divided into four partitions (also called "cells") that contain files. Partitions 0 (zero), 1, and 3 hold the ComOS, and partition 2 holds the configuration. This design allows you to upgrade ComOS without disturbing the configuration and to make changes to the configuration of the PortMaster without disturbing ComOS.

You can back up the configuration file if you are confident that it is not corrupted. Occasionally, downgrading ComOS to an earlier version can corrupt the configuration. If you downgrade ComOS, you must back up your configuration first. See Step 5 on page 2-16 for information on backing up the configuration.

Warning – Be extremely careful when erasing NVRAM. You can quickly remove all configuration information and the operating system from the PortMaster, making it difficult to restore and possibly inoperable. Read the entire erasure procedure before beginning to ensure that you understand the effects of the **erase** commands.

If you erase the cells holding ComOS and reboot your PortMaster, you must netboot to restore the operating system and get your PortMaster functioning again.

If you reformat the NVRAM cell where the configuration is stored and reboot your PortMaster, your PortMaster is reset to factory defaults. You must connect a console to the S0 or C0 port for initial configuration after rebooting.

Although ComOS might still be running in dynamic RAM (DRAM), after you erase the ComOS cells, most **show** commands do not display useful output. Instead you will see system messages, which are stubs for the actual messages displayed on the console screen.

For example:

```
Command> show all
SYSMSG489 SYSMSG1029 SYSMSG71 SYSMSG52
SYSMSG603 SYSMSG210 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120
SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120
SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG120 SYSMSG208 SYSMSG459

Command> show global
SYSMSG1071 SYSMSG1030 SYSMSG1031
SYSMSG1070 SYSMSG1035 SYSMSG1072
SYSMSG1068 SYSMSG1037  Maximum PMconsole: 1
SYSMSG1038
SYSMSG1039 SYSMSG1270 PPP Authentication: PAP: on     CHAP: on
Disabled Modules: SNMP OSPF BGP
```

Reasons for Erasing and/or Reformatting NVRAM

The following are reasons to erase and/or reformat NVRAM:

- Returning the configuration to factory defaults

  By reformatting the partition of NVRAM where the configuration resides you can return the PortMaster to factory defaults. See "Resetting the Configuration to Factory Defaults" on page 2-4.

- Restoring a corrupted ComOS

  A corrupted ComOS can cause the PortMaster to behave erratically. If you see unusual output when using any of the **show** commands, ComOS might be corrupted. See "Erasing and Reloading ComOS" on page 2-5.

- Restoring a corrupted configuration

  A corrupted configuration can prevent the PortMaster from booting up normally or from performing correctly. See "Erasing ComOS and the Configuration" on page 2-6.

- Upgrading ComOS

  The **pminstall** utility and PMconsole automatically reformat ComOS and system message partitions before upgrading ComOS.

Resetting the Configuration to Factory Defaults

ComOS and all configuration settings on the PortMaster are stored in NVRAM. You can return the PortMaster to factory defaults by using the following commands.

Warning – Be extremely careful when erasing NVRAM. You can quickly remove all configuration information and the operating system from the PortMaster, making it difficult to restore and possibly inoperable. Read the entire erasure procedure before beginning to ensure that you understand the effects of the **erase** commands.

1. **Set the console and the debug value.**

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

   Command> set debug 0x72
   Setting debug value to 0x72
   ```

2. **Enter the** erase configuration **command.**

   ```
   Command> erase configuration
   Erasing FLASH cell 2 - 28F010 ... Succeeded in 82 tries
   Successfully erased FLASH configuration
   ```

3. **Reboot the PortMaster.**

   ```
   Command> reboot
   ```

Note – When you erase the configuration and reboot your PortMaster, it is returned to factory defaults. You must connect a console to the S0 or C0 port to perform initial configuration after rebooting.

Erasing and Reloading ComOS

If ComOS is corrupted, the PortMaster might behave erratically. You can erase ComOS by using the following procedure:

Warning – Be extremely careful when erasing NVRAM. You can quickly remove all configuration information and the operating system from the PortMaster, making it difficult to restore and possibly inoperable. Read the entire erasure procedure before beginning to ensure that you understand the effects of the **erase** commands.

1. **Set the console and the debug mask.**

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

Command> set debug 0x72
Setting debug value to 0x72
```

2. **Enter the** erase comos **command,**

```
Command> erase comos
Erasing FLASH cell 0 - 28F010 ... Succeeded in 75 tries
Erasing FLASH cell 1 - 28F010 ... Succeeded in 78 tries
Erasing FLASH cell 3 - 28F010 ... Succeeded in 69 tries
sys_msginit: Missing System Messages
Successfully erased ComOs
```

   The "sys_msginit: Missing System Messages" message appears when the partition holding the system messages is erased.

3. **Take note of how many tries are required to erase the NVRAM (FLASH) cells.**

   – On a PortMaster 2 or an IRX, the attempts to erase NVRAM is measured in tries. If more than 150 tries are needed, contact Lucent Remote Access Technical Support.

   – On a PortMaster 3 or an Office Router, the attempts are measured in seconds. The seconds measurement does not provide the same indication of NVRAM health deterioration. Instead, the unit immediately displays a "Panic Watchdog Timer" message if erasing NVRAM takes too many seconds.

   If you encounter any problems while erasing ComOS, contact Lucent Remote Access Technical Support.

Note – If you reboot your PortMaster after erasing ComOS, you must netboot to restore the operating system and get your PortMaster functioning again. See "Netbooting" on page 2-7 for instructions.

4. **After you have erased ComOS, reload it by running the** pminstall **utility.**

   See "Installing a New ComOS Using pminstall" on page 2-16 for instructions.

   If you encounter problems while reloading the ComOS, verify the following:

   – You downloaded the upgrade image in binary format.

   – You have the correct upgrade image for the PortMaster platform you are using. For example, a PortMaster 2 image will not work on a PortMaster 25.

   – The downloaded file size is the same as the file on the FTP site. If the downloaded file is smaller than the file on the FTP site, the entire file was not downloaded.

   – The checksum and block size of the downloaded file are the same as the file on the FTP site. You can determine these values on the downloaded file by using the **sum** command (on Sun Solaris or Linux hosts) or an applicable utility (on Windows NT and Windows 95 hosts). You must contact Lucent Remote Access Technical Support to verify these values for the file on the FTP site.

Erasing ComOS and the Configuration

You can erase all the NVRAM in the PortMaster including the configuration and ComOS by using the following procedure.

Warning – Be extremely careful when erasing NVRAM. You can quickly remove all configuration information and the operating system from the PortMaster, making it difficult to restore and possibly inoperable. Read the entire erasure procedure before beginning to ensure that you understand the effects of the **erase** commands.

1. **Set the console and the debug value.**

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

Command> set debug 0x72
Setting debug value to 0x72
```

2. **Enter the** erase all-flash **command.**

```
Command> erase all-flash
Erasing FLASH cell 0 - 28F010 ... Succeeded in 72 tries
Erasing FLASH cell 1 - 28F010 ... Succeeded in 76 tries
Erasing FLASH cell 2 - 28F010 ... Succeeded in 76 tries
Erasing FLASH cell 3 - 28F010 ... Succeeded in 66 tries
sys_msginit: Missing System Messages
Successfully erased all FLASH
```

   The "sys_msginit: Missing System Messages" message indicates that the partition holding the system messages has been erased.

3. **Take note of how many tries are required to erase the NVRAM (FLASH) cells.**

   – On a PortMaster 2 or an IRX, the attempts to erase NVRAM is measured in tries. If more than 150 tries are needed, contact Lucent Remote Access Technical Support.

   – On a PortMaster 3 or an Office Router, the attempts are measured in seconds. The seconds measurement does not provide the same indication of NVRAM health deterioration. Instead, the unit immediately displays a "Panic Watchdog Timer" message if erasing NVRAM takes too many seconds.

4. **After you have erased ComOS, reload it by running the** pminstall **utility.**

Note – If any NVRAM cells are physically corrupted, the PortMaster "locks up" when that cell is erased, and must be rebooted. If you have already erased ComOS when the PortMaster locks up, you must netboot instead of performing a regular reboot to restore the operating system. See the next section, "Netbooting" for instructions. If you have erased the configuration on the PortMaster, you need a console connection to boot from PROM.

Netbooting

Netbooting allows you to boot a PortMaster with a damaged NVRAM by downloading a temporary ComOS, either with a network connection via a TFTP host, or via the serial port.

The NVRAM might be damaged if any of the following occur:

- Your PortMaster never displays the **login:** prompt during self-diagnostics when DIP switch 1 is up. This behavior indicates that the configuration area of the NVRAM is probably damaged.
- A checksum error on the ComOS is reported during the diagnostic boot process. See the hardware installation guide that came with your PortMaster for more information about the diagnostic boot process.
- You have had three unsuccessful upgrade attempts on a PortMaster running ComOS version 3.0.4 or earlier or IRX ComOS version 3.0.1R or earlier. In this case, ComOS has run out of file descriptors.

To netboot, you must have a host that is on the same Ethernet network as the PortMaster and that supports the Trivial File Transfer Protocol (TFTP). If you do not have a TFTP-capable host, or if you do not have a network connection, you must use the **download** command to boot from the PROM monitor via the serial port.

Use the following steps to boot a PortMaster with a damaged NVRAM:

1. **Access the Lucent Remote Access FTP site and download the appropriate GENERIC file.**

   See the next section, "Accessing the Lucent Remote Access FTP Site."

2. **If you have a network connection and a TFTP host, download a GENERIC ComOS image.**

   Use the procedure in "Netbooting with a Network Connection" on page 2-11.

3. **If you do not have a network connection or a TFTP host, download a GENERIC ComOS from another host via the serial port.**

   Use the procedure in "Booting from PROM (Booting without a Network Connection)" on page 2-13.

4. **When the PortMaster has successfully netbooted a temporary ComOS, download a new, permanent ComOS.**

   Use the procedure in "Installing a New ComOS Using pminstall" on page 2-16.

Accessing the Lucent Remote Access FTP Site

If you are using Microsoft Windows 95 or Windows NT, use an appropriate TFTP software package to access the Lucent Remote Access FTP site and download a GENERIC ComOS.

If you are using a UNIX host to access the Lucent Remote Access FTP site, use the following procedure to download the appropriate files in preparation for netbooting:

1. **Access the Lucent Remote Access FTP site, and download the README.NETBOOT file.**

   Enter the following commands from your Ethernet TFTP boot host:

   ```
   % ftp ftp.livingston.com
   Name: anonymous
   Password: your email address
   ftp> binary
   ftp> cd pub/livingston/netboot
   ftp> get README.NETBOOT
   ftp> quit
   ```

2. **Read the README.NETBOOT file to determine which netbootable ComOS to download.**

   Replace *GENERIC.OS* with one of the filenames in Table 2-2.

Table 2-2 Netbootable ComOS Filenames

PortMaster Model	Filename
Any PM2 model except PM-25	**GENERIC.PM2**
PM-25	**GENERIC.P25**
Any OR model except OR-AP	**GENERIC.PMO**
OR-AP	**GENERIC.OR2**
Any IRX model	**GENERIC.IRX**
Any PM3 model	**GENERIC.PM3**

3. **Access the Lucent Remote Access FTP site again, and download the appropriate ComOS.**

Enter the following commands from your Ethernet TFTP boot host, replacing *GENERIC.OS* with the appropriate filename from Table 2-2:

```
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd pub/le/netboot
ftp> get GENERIC.OS
ftp> quit
```

Note – The *GENERIC.OS* file must be downloaded in binary format.

4. **Set up TFTP on your boot host.**

   Enter the following commands, replacing *GENERIC.OS* with the appropriate filename (see Table 2-2):

   ```
   % umask 22
   % mkdir /tftpboot
   % mv GENERIC.OS /tftpboot/GENERIC.OS
   % cd /tftpboot
   % ln -s . tftpboot
   ```

5. **Using a text editor, uncomment the** tftp **command entry in the** /etc/inetd.conf **file.**

   To have the **inetd** daemon reread the **/etc/inetd.conf** file, send a SIGHUP to the **inetd** process.

   This step applies to most UNIX systems. However, the procedure for enabling TFTP on your system might vary. Consult your system documentation.

6. **Do one of the following:**

   – If you have a network connection, continue with the procedure in "Netbooting with a Network Connection" on page 2-11.

   – If you do not have a network connection, continue with the procedure in "Booting from PROM (Booting without a Network Connection)" on page 2-13.

Netbooting with a Network Connection

Any host capable of TFTP can be used to boot a PortMaster from the network.

- If your system supports **rarpd**, follow the procedure in "Netbooting with rarpd" on page 2-11.
- If your system does not support **rarpd**, follow the procedure in "Netbooting without rarpd" on page 2-12.

Caution – A *GENERIC.OS* ComOS downloaded during a netboot is only temporarily running in DRAM. You must load a fully functional ComOS into the NVRAM by following the procedure in "Installing a New ComOS Using pminstall" on page 2-16.

Netbooting with rarpd

If your system supports **rarpd**, use the following procedure on the TFTP host after you have downloaded the appropriate *GENERIC.OS* file to the **/tftpboot** directory.

Note – The Reverse Address Resolution Protocol (RARP) server must be on the same subnet as the PortMaster.

1. **Enter the Ethernet address of the PortMaster in the** /etc/ethers **file or the Network Information Service (NIS) map.**
2. **Start** rarpd **by entering the following command:**

   ```
   % rarpd -a
   ```

Note – The command might vary, depending on your operating system. Refer to your system manual for more information about running **rarpd**.

3. **Turn the PortMaster off and on.**

   The temporary *GENERIC.OS* ComOS is automatically downloaded to the PortMaster from the TFTP host.

4. **Download a new ComOS into NVRAM by using the procedure in Step 6 on page 2 -17.**

Netbooting without rarpd

If your system does not support **rarpd**, use the following procedure on the TFTP host after you have downloaded the appropriate *GENERIC.OS* file to the **/tftpboot** directory.

Note – When you enter a command correctly, the PortMaster responds with **OK**. If you enter a command incorrectly, the PortMaster responds with a question mark (**?**).

1. **Turn the PortMaster off.**
2. **Place the PortMaster in diagnostic boot mode by setting DIP switches 1 and 2 up.**
3. **Attach a terminal to the console port of the PortMaster.**
4. **Turn the PortMaster on.**
5. **When the PortMaster starts to use RARP, press the** Esc **key.**

   An angle bracket (>) prompt appears.

   You can also type a caret and a left square bracket (**^[**) to display the prompt.

   Commands available from the PROM are shown in Table 2-3 on page 2-13.
6. **Enter the IP address of the PortMaster Ethernet port:**

   ```
   > address Ipaddress
   ```
7. **Set the netmask and gateway, if needed.**

   You must set the gateway if the TFTP server is not on the local network. The netmask is set to 24 bits by default.

   ```
   > netmask Netmask
   > gateway Ipaddress
   ```
8. **Use the following command to load the PortMaster:**

   ```
   > tftp Ipaddress
   ```

   Enter the IP address of the TFTP host that has the *GENERIC.OS* software. The PortMaster makes a TFTP request from that host, and the server responds by sending the netboot image to the PortMaster.
9. **When the PortMaster has successfully netbooted, set DIP switch 2 down.**

10. Download a fully functional ComOS into NVRAM.

Use the procedure in Step 6 on page 2 -17.

Booting from PROM (Booting without a Network Connection)

If you do not have a network connection, or a TFTP host, you must boot the PortMaster from PROM through the serial port using the following procedure.

Note – This procedure works only with PROMs of level F or higher. The PROM version is displayed in the diagnostic messages when the PortMaster is booted with DIP switch 1 up (diagnostic mode). See the hardware installation guide that came with your PortMaster for more information about diagnostic messages.

Beginning with PROM level F, you can boot your PortMaster remotely from any host with TFTP capability in one of the following ways by using the PROM:

- Boot from the **tftpd** daemon (See "Booting from the tftp Daemon" on page 2-13).
- Send a ComOS version from your workstation to the console port on the PortMaster over a serial cable or modem and boot from that (See "Downloading ComOS through a Serial Port" on page 2-15).

Caution – A ComOS downloaded during a netboot is only temporarily running in DRAM. You must load a new ComOS into NVRAM by following the procedure in "Installing a New ComOS Using pminstall" on page 2-16.

Booting from the tftp Daemon

Table 2-3 explains the commands you use to boot the PortMaster from PROM. The following procedure explains how to use the commands.

Table 2-3 PROM Commands

Command	Description
address	Sets the address of the Ethernet interface.
netmask	Sets the netmask of the Ethernet interface. The default is 24-bit (255.255.255.0).
gateway	Sets the default gateway in order to boot from a server on another network.

Table 2-3 PROM Commands *(Continued)*

Command	Description
tftp	Causes the PortMaster to issue the TFTP request to the boot server.
download	Downloads ComOS using the serial port.
continue	Causes the PortMaster to continue attempting to boot using the Reverse Address Resolution Protocol (RARP).

1. **Turn the PortMaster off.**
2. **Place the PortMaster in diagnostic boot mode by setting DIP switches 1 and 2 up.**
3. **Configure the host computer for 9600 baud, 8 data bits, 1 stop bit and no parity. Turn on XON/XOFF software flow control.**
4. **Turn the PortMaster on.**
5. **When the PortMaster starts to use RARP, press the** Esc **key.**

   An angle bracket (>) prompt appears.

   You can also type a caret and a left square bracket (**^[**) to display the prompt.

   Commands available from the PROM are shown in Table 2-3 on page 2-13.

6. **Enter the address of the PortMaster Ethernet port:**

   > **address** *Ipaddress*

7. **Set the netmask and gateway, if needed.**

   The netmask is set to 24 bits by default.

   > **netmask** *Netmask*
   > **gateway** *Ipaddress*

8. **Use the following command to load the PortMaster:**

   > **tftp** *Ipaddress*

   Enter the IP address of the TFTP host that has the *GENERIC.OS* software. The PortMaster makes a TFTP request from that host, and the server responds by sending the netboot image to the PortMaster.

9. **When the PortMaster has successfully netbooted, set DIP switch 2 down.**
10. **Download a fully functional ComOS into NVRAM.**

    Use the procedure in Step 6 on page 2 -17.

Downloading ComOS through a Serial Port

To install a bootable ComOS on the PortMaster from a host without file transfer capability, do the following:

1. **Turn off the power on the PortMaster.**
2. **Set DIP switches 1 and 2 up.**
3. **Attach a null modem serial cable to the host and to the serial port on the PortMaster.**

   On a PC, attach the cable to port COM1 or COM2.

4. **Configure the host computer for 9600 baud, 8 data bits, 1 stop bit, and no parity. Turn on XON/XOFF software flow control.**
5. **If you are using a PC to boot the PortMaster, download the *GENERIC.OS* image to the hard drive.**

   a. From the Microsoft Windows Terminal program select **Transfers** from the menu bar and then **Send Text File** from the submenu.

   b. Turn on the PortMaster.

   c. Press **Esc** and enter **download** *Number,* replacing *Number* with the size in bytes of the *GENERIC.OS* image.

   d. Uncheck the **Strip LF** option and find the file in the browse box. See Table 2-2 on page 2-9 for the correct filename for your PortMaster model. Press the **OK** button when ready to download.

   The process takes 5-6 minutes and the PortMaster automatically reboots when done.

6. **If you are using a UNIX host to boot the PortMaster, transfer the file as follows:**

   a. Enter **{cu,tip} /dev/***ttyxx* in one session window, replacing *ttyxx* with the serial port tty.

b. Turn on the PortMaster.

c. Press **Esc** and enter **download** *Number*, replacing *Number* with the size in bytes of the *GENERIC.OS* image.

d. From another session window, enter **cat** *GENERIC.OS* **> /dev/ttyxx**, replacing *GENERIC.OS* with the correct filename for your PortMaster model (see Table 2-2 on page 2-9).

When the PortMaster receives *Number* bytes, it runs ComOS.

7. **When the booting process is complete, set DIP switch 2 down.**

8. **Load a fully functional ComOS into NVRAM.**

   Use the procedure in Step 6 on page 2 -17.

Installing a New ComOS Using pminstall

To download a new ComOS to the PortMaster by using the **pminstall** utility, do the following:

1. **Turn the PortMaster off.**

2. **Set DIP switch 1 to up, and DIP switch 2 to down so that the PortMaster does not netboot each time it is turned on.**

3. **Turn the PortMaster on.**

4. **Log in as** !root**.**

5. **Do one of the following:**

   – Save your configuration if you are confident that it did **not** corrupt the ComOS you are replacing.

     To save the configuration to an output file before reformatting NVRAM, enter the following command on your UNIX host:

     ```
     % /usr/portmaster/pmreadconf Pmname Pmpassword Outputfilename
     ```

     On a PC, use PMconsole for Windows to save your configuration.

   – Erase and reconfigure NVRAM on your PortMaster if you suspect that your configuration corrupted the ComOS you are replacing.

See "Resetting the Configuration to Factory Defaults" on page 2-4 for instructions.

6. **Download the appropriate version of** pminstall **and the new ComOS via FTP from the Lucent Remote Access FTP site:**

   ftp://ftp.livingston.com/pub/le/software/*System*/*Tarfile.tar.Z*.

   Replace *System* and *Tarfile.tar.Z* with the names of the files. You can retrieve the upgrade image at the same time. The following example illustrates how to retrieve the SunOS **pminstall** and PortMaster 3 upgrade image:

```
% umask 22
% mkdir /usr/portmaster
% cd /usr/portmaster
% ftp ftp.livingston.com
Name: anonymous
Password: your email address
ftp> binary
ftp> cd /pub/le/software/sun4
ftp> get pm_3.5.3_sun4.tar.Z pm.tar.Z
ftp> cd /pub/le/upgrades
ftp> get pm3_3.7.2c3
ftp> quit
% uncompress pm.tar.Z
% tar xvf pm.tar
% rm pm.tar
% mv pm3_3.7.2c3 data
```

7. **Install the new ComOS into the NVRAM by using the** pminstall **utility.**

```
% pminstall
```

8. **After the new ComOS is installed, prepare the PortMaster for operation.**

   See "Preparing the PortMaster for Operation" on page 2-18 for instructions.

9. **If your PortMaster has problems during or after the netboot, troubleshoot them.**

   See "Troubleshooting Netbooting" on page 2-18 for instructions.

Preparing the PortMaster for Operation

Use the following procedure to prepare the PortMaster for operation after you have downloaded a new ComOS into NVRAM:

1. **Turn off the power on the PortMaster.**
2. **Remove the terminal from the console port.**
3. **Return the DIP switches to their normal operating positions.**
4. **Reboot the PortMaster by turning on the power.**
5. **If the PortMaster is running properly, reenter your PortMaster configuration settings if necessary.**

   For more information, see the *PortMaster Configuration Guide*.

Troubleshooting Netbooting

Table 2-4 lists some of the common problems encountered during or after a netboot and recommends possible solutions.

Table 2-4 Common Netboot Errors and Solutions

Problem	Recommended Action
The PortMaster does not reboot after netboot.	Verify the byte count of the image file on the PortMaster against the file on the FTP site. If the file sizes do not match, download the image file again. If the file sizes match, use a Sun Solaris or Linux host to do a checksum on the file with the **sum** command. This command verifies that the checksum and block size are the same for both files. If they are not the same, transfer the file again with FTP and do another checksum until you can verify file integrity.
The green LED on the PortMaster is solidly on or off.	If the green LED next to the DIP switches does not flash off once every 5 seconds, contact Lucent Remote Access Technical Support.

Table 2-4 Common Netboot Errors and Solutions *(Continued)*

Problem	Recommended Action
Nothing is displayed on the console.	• Make sure the PortMaster is turned on and plugged in with the null modem cable firmly attached to S0 and to the terminal. • Make sure DIP switch 1 is up. Try turning off the PortMaster and flipping DIP switch 1 up and down a few times and then rebooting with DIP switch 1 up. • If the PortMaster is connected to a PC, make sure you have the correct COM port selected. If the PortMaster is connected to a UNIX host, verify that the tty setting is correct. • Make sure the single green LED next to the DIP switches blinks off once every 3 to 5 seconds. • Replace the null modem cable. • Verify the pinout of the COM port on the terminal. • Change the COM port on the terminal. • Use another terminal program. • Use another hardware device as your console. • Program a modem for 9600 baud, 8 data bits, 1 stop bit, no parity, and for autoanswer, and dial in to the modem. • If you have other PortMaster products, connect your terminal to those devices and use the console. If the terminal works on another PortMaster product but not this one, contact Lucent Technical Support.
You can see the PortMaster boot diagnostics and the prompt, but you cannot enter commands.	• Verify you are using a null modem cable. • Replace the null modem cable. • Use an alternate serial port or COM port on the host computer. • Check flow control settings. • Verify that the keys on your keyboard are working properly.

Table 2-4 Common Netboot Errors and Solutions *(Continued)*

Problem	Recommended Action
Output on the console is unreadable	• Make sure that your terminal is set to 9600 baud. • Verify that the output is from this PortMaster. If you have another device that is using the interrupt request (IRQ) level of your COM port, you will see unreadable data from the other device. • Use a different COM port. • Replace the null modem cable with one you know is working. • Use another hardware device for your terminal.
The error message "Panic Watchdog Timer" appears.	Have your console ready on S0, and contact Lucent Remote Access Technical Support. This message might indicate a problem with the NVRAM.
The error message "shared memory error" appears.	Have your console ready on S0, and contact Lucent Remote Access Technical Support.

Replacing Forgotten Passwords

Follow these steps if you have forgotten the administrative password:

1. **Place the PortMaster in diagnostic mode by setting DIP switch 1 up.**
2. **Log in to the PortMaster at the PortMaster console** login: **prompt using** !root **and a password of** override**.**

   A case-sensitive, 16-character encrypted challenge appears.
3. **Contact Lucent Remote Access Technical Support for the appropriate 16-character one-time encrypted response.**
4. **Log in to the PortMaster as** !root**, and enter the 16-character encrypted response given by Lucent Remote Access Technical Support as the password.**

Note – Both the challenge and the response are case-sensitive.

5. **Change the administrative password using the** set password **command.**
6. **Enter the** save all **command to save the new password to NVRAM.**

Diagnosing Authentication Problems

If users are having trouble being authenticated by the PortMaster and you are using RADIUS, see the *RADIUS Administrator's Guide* for troubleshooting information.

If you are **not** using RADIUS, do either or both of the following to diagnose authentication problems:

- Use the **set debug 0x51** command to monitor the authentication process. See "Debugging and Interpreting PPP Negotiation" on page 4-2.

  See the *PortMaster Command Line Reference* for more information on this command.

- Use the **show table user** command to verify that your users are configured correctly.

```
Command> show table user

Name       Type               Address/Host          Service      RIP
--------   ----------------   -------------------   ----------   ---
katia      Login User         10.10.10.2            Telnet
byron      Netuser            Negotiated            ffffffff     No
```

For more information on the user table and how to configure users, see the *PortMaster Configuration Guide*.

Solving Networking Problems 3

Use Table 3-1 to identify diagnose common networking problems. For more in-depth discussion on troubleshooting routing protocols such as OSPF and BGP, see the *PortMaster Routing Guide*.

Table 3-1 Common Networking Problems

Problem	**Possible Cause**	**Solution**
Unspecified problem on a **local** PortMaster seems to be network related.	• Faulty hardware or software. • Incorrect DIP switch setting. • Overloaded network	See the following sections for preliminary diagnostics: • "Using Console Messages to Troubleshoot" on page 3-3. • "Determining the ComOS Version" on page 3-8. • "Verifying Network Connections" on page 3-9. See "DIP Switch Position" on page 1-8. See "Diagnosing an Overloaded Ethernet Network" on page 1-12.
Unspecified problem on a **remote** PortMaster seems to be network related.	Faulty hardware or software.	• Establish an administrative Telnet session to the PortMaster to help diagnose the problem (page 3-4). • If you cannot telnet to the PortMaster, dial in with a modem.

Table 3-1 Common Networking Problems *(Continued)*

Problem	Possible Cause	Solution
No connectivity exists between the PortMaster and other nodes.	• Faulty hardware or software. • Incorrect DIP switch setting.	• Use the **ping** command (page 3-9) and the **ptrace** command (page 3-12) to determine if the PortMaster can communicate with any of the nodes on its network. • See "DIP Switch Position" on page 1-8.
All hardware connections are correct, but the PortMaster still cannot communicate with other nodes.	• Incorrect configuration. • Incorrect DIP switch position.	• Use the **ifconfig** command to verify the configuration of the active interfaces on the PortMaster (page 3-10) and temporarily change them if necessary. • See "DIP Switch Position" on page 1-8.
The idle timer is not timing out connections.	RIP packets maintaining the link.	Verify IP traffic on the port with **ptrace** (page 3-14).
The Domain Name System (DNS) not functioning as expected.	Primary DNS server malfunction.	Use **ptrace** to verify which DNS is being accessed (page 3-15).
Packets are not reaching their destination.	• Incorrect static route in the IP routing table. • Incorrect routing.	• Verify routes with the **show routes** command (page 3-20). • Use **ptrace** to trace RIP packets as they pass through the PortMaster (page 3-19).
A **ping** echo request reaches its destination, but the echo reply does not return.	• Incorrect routing. • Default gateway is not set on the remote device.	• Use **ptrace** to trace ping packets to isolate the routing problem (page 3-18). • Verify the default gateway setting on the remote device.

Table 3-1 Common Networking Problems *(Continued)*

Problem	Possible Cause	Solution
The network can no longer access the Internet.	Routing has stopped.	Use the **traceroute** command to isolate the routing problem (page 3-19).
The **traceroute** command reaches its target but **ping** does not, or vice versa.	• Incorrect routing. • Incorrect filtering on a router between the source and destination. • Default gateway not set on the target device.	• Use the **show routes to-dest** command to determine the routing (page 3-22). This is a common routing problem over Frame Relay connections. • Check filters on routers between the source and destination. For more information on configuring filters, see the *PortMaster Configuration Guide*. • Check the default gateway setting on the target device.

Note – You can access the command line from a console terminal regardless of network condition.

Using Console Messages to Troubleshoot

To troubleshoot a PortMaster by checking console messages, you must connect to its console port in one of the following ways:

- Telnet to the PortMaster via a network connection. See "Using Administrative Telnet Sessions" on page 3-4" for instructions.
- Attach a terminal or workstation to the PortMaster console port (port S0 or C0) with a null modem cable. Use this method if you cannot create a network connection via Telnet.

  If you use this method, attach a terminal or workstation in terminal emulation mode for 9600 baud, 8 data bits, 1 stop bit, no parity, and software flow control (XON/XOFF) off. For more information, refer to the hardware installation guide that came with your PortMaster.

- Use a modem to dial in to the PortMaster. This method can sometimes be used when Telnet does not work.

When you have connected to the console port, do the following:

1. **Set DIP switch 1 on the back of the PortMaster to the up position.**

   DIP switch 1 is the leftmost switch. Refer to your hardware installation guide for detailed information about the PortMaster DIP switches.

2. **Turn the PortMaster off and on.**

3. **Observe the diagnostic output.**

   – If the PortMaster completes its diagnostics and produces a **PortMaster Console login:** prompt, the PortMaster booted correctly.

   – If not, you might need to boot the PortMaster from the network. See "Netbooting" on page 2-7 for instructions.

   Refer to the troubleshooting chapter of your hardware installation guide for more information on diagnostic boot messages.

Using Administrative Telnet Sessions

You can establish an administrative Telnet session to a remote PortMaster. The PortMaster supports up to four simultaneous administrative Telnet connections.

Establishing a Telnet Session

To establish an administrative Telnet session, telnet to your PortMaster and log in as **!root** with your administrative password. If you are using RADIUS, you can use an administrative user account. Refer to the *RADIUS Administrator's Guide* for more information.

If you have problems establishing a Telnet session, see "Troubleshooting the Session" on page 3-5.

Displaying Console Messages

Use the **set console** command to set the port used for an administrative Telnet session as the console port. This configuration allows you to display messages that are sent to the port on the console terminal or workstation. To release the Telnet port from console use, enter the **reset console** command. Lucent Remote Access recommends that you reset the console at the end of every Telnet session.

To display Telnet messages to the console, enter the following command:

```
Command> set console
Setting CONSOLE to admin session
```

When you are finished, enter the following command:

```
Command> reset console
Console RESET
```

Troubleshooting the Session

If you are having trouble establishing an administrative Telnet session, follow these steps on the PortMaster:

1. **Verify the TCP port used for Telnet access with the** show global **command.**

   See the *PortMaster Command Line Reference* for an explanation of command output.

```
Command> show global
         System Name:   pm2e
        Default Host:   192.168.1.70
     Alternate Hosts:
          IP Gateway:   192.168.96.2
      Gateway Metric:   1
     Default Routing:   Quiet (Off)
       OSPF Priority:   0
      OSPF Router ID:   192.168.96.6
        Name Service:   DNS
         Name Server:   192.168.1.70
              Domain:   livingston.com
  Telnet Access Port:   23
```

```
            Loghost:   0.0.0.0
 Maximum PMconsole:   10
  Assigned Address:   192.168.93.200  (Pool Size 3)
     RADIUS Server:   192.168.64.26
  Alternate Server:   0.0.0.0
 Accounting Server:   192.168.64.26
Alt. Acct. Server:   0.0.0.0
PPP Authentication:   PAP: on     CHAP: off
  Disabled Modules:   BGP
```

2. **Check for Telnet sessions by using the** show netconns **command and looking for administrative connections to that port.**

   Use the following explanation of the output:

```
Command> show netconns

 Hnd     Recv-Q   Send-Q   Local Address         Foreign Address       (state)
 47      0        0        192.187.195.1.23      0.0.0.0.0             LISTEN
 46      0        0        192.187.195.1.1041    192.187.195.2.53      UDP
 37      0        2        192.187.195.1.23      128.165.32.27.32872   ESTABLISHED
 11      0        0        192.187.195.1.1011    192.187.195.2.1642    ESTABLISHED
 7       0        0        192.187.195.1.67      0.0.0.0.0             UDP
 5       0        0        192.187.195.1.1643    0.0.0.0.0             LISTEN
 4       0        0        192.187.195.1.161     0.0.0.0.0             UDP
 1       24       0        192.187.195.1.520     192.187.195.0.520     UDP
```

   The preceding **show netconns** output is from a PortMaster with an IP address of **192.187.195.1**. The output shows an **established** state on the third line (shown in **bold** for this example).

   The Local Address column shows the PortMaster address as **192.187.195.1.23**—the **.23** indicates the listening socket. Telnet listens on socket 23 by default. This output indicates that an active Telnet session exists between the PortMaster and a remote host.

For a list of services and their associated port numbers, see Table 3-2.

Table 3-2 Services and Associated Port Numbers

Port Number	Service
23	telnet
53	Domain Name System (DNS)
67	BOOTP
161	SNMP
512	**syslog**
520	RIP
1642	**pmd**
1643	**pmconsole**, **pmcommand**, **pminstall**, PMVision, and other management applications
1645	RADIUS
1646	RADIUS accounting
1647	ChoiceNet
1649	Multichassis PPP

The remote host address (**128.165.32.27.32872)** is shown in the Foreign Address column. The number 32872 is a random number greater than 1023, which is used by most TCP client applications. The 128.165.32.27 is the IP address of the remote host calling the PortMaster.

The first column labeled **Hnd** is the network handle. A network handle is a number assigned to an active socket that can be used to close that socket manually, rather than by a request from the client. You can reset the Telnet session between the remote host and the PortMaster by entering the **reset n37** command (37 is the network handle for the Telnet session).

3. **Reset any unused connections with the** reset n*Handle* **command.**

```
Command> reset n37
```

Note – Although you can have up to four concurrent Telnet sessions, you can have only one **pmcommand**, **pmconsole**, **pminstall**, or **pmreadconf** program running at one time with a given PortMaster unless you use the **set maximum pmconsole** *Number* command to increase the default to a number between 1 and 10.

Determining the ComOS Version

You often need to know the version of ComOS that is running on the PortMaster. For example, if the PortMaster is running an older version of ComOS, upgrading to the most current version might solve the problem. The **version** command also reports the system uptime since the last reboot.

Note – You must know the ComOS version when contacting Lucent Remote Access Technical Support.

To determine the version of ComOS on your PortMaster, log in as **!root** and enter the following command:

```
Command> version
Livingston Enterprises PortMaster version 3.7
System uptime is 21 days 15 hours 24 minutes
```

Depending on the version of ComOS you are running, you might see this type of output instead:

```
Command> version
Livingston PortMaster PM-3 ComOS 3.8b2/9710211203
System uptime is 1 hours 20 minutes
```

The ComOS in the second example was built using version 3.8 as its base; the **b2** indicates a beta release. A **c** would indicate a maintenance patch release. The date and time stamp after the version number indicates exactly when the version was released. In this example, the ComOS was released in 1997 (97) on October 21 (1021), at 12:03 p.m. (1203).

Verifying Network Connections

Use the **ping** command to verify connectivity between your PortMaster and devices on your network. The **ping** command sends an Internet Control Message Protocol (ICMP) echo request to the host specified and listens for the corresponding echo reply from the specified host. If a reply is received, connectivity between the PortMaster and the device is at least minimally sound.

If no reply is received, connectivity is failing somewhere on your network between the machine issuing the **ping** request and the specified device.

To ping a device on your network, use the following command:

```
Command> ping Ipaddress
```

To stop the ping process, enter the command with no IP address or hostname.

If you do not receive a response to the **ping** command, do the following:

- Use the **show netstat** command (page 1-12) to verify that the **ping** request is using the Ether0 interface.
- Verify that the host you pinged is running and connected to the Ethernet.
- If you suspect an Ethernet problem, use the **show arp ether0** command**.** If you cannot ping another host on the Ethernet network, see if the PortMaster is getting ARP requests. An unsuccessful **ping** still produces an ARP request.

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

  If you see ARP requests as shown in this example, the Ethernet hardware is working, but you probably have a configuration or routing problem.
- Verify that all cables are connected to the PortMaster properly.
- If the machine you pinged is on another subnet, verify that the machine has the correct subnet mask, and that you have the correct gateway setting.
- Watch LED activity. See the hardware installation guide that came with your PortMaster for more information.

Using ifconfig

If you have verified that everything is connected properly, check the configuration of your PortMaster interfaces using the **ifconfig** command.

Verifying the PortMaster's Configuration

The **ifconfig** command allows you to view the active configuration of each network interface.

In the following example, **ifconfig** is used to verify the Ethernet parameters.

In **ifconfig** command output, netmasks are shown in hexadecimal format. Table 3-3 on page 3-11 shows equivalent dotted decimal and classless interdomain routing (CIDR) formats for netmasks.

```
Command> ifconfig
ether0: flags=16<IP_UP,IPX_DOWN,BROADCAST>
inet 192.168.1.2 netmask ffff0000 broadcast 192.168.0.0 mtu 1500
```

This example **ifconfig** command output displays the following information about the Ethernet interface:

- The Ethernet interface (indicated by **BROADCAST**) is up and running the IP protocol (indicated by **IP_UP**). It is not running the IPX protocol (indicated by **IPX_DOWN**).
- The IP address is 192.168.1.2.
- The netmask is ffff0000 (in hexadecimal).

  To convert the netmask into dotted decimal format, refer to Table 3-3 on page 3-11. The hexadecimal ffff0000 is equivalent to 255.255.0.0 in dotted decimal format.
- The broadcast address of the interface—on Ethernet interfaces only—is 192.168.0.0.
- The maximum transmission unit (MTU) size for the interface is 1500 bytes.

See "Temporarily Changing the Configuration" on page 3-12 to modify the interface configuration, if necessary.

Table 3-3 32-Bit Netmask Formats

Binary	Hex	CIDR	Dotted Decimal
00000000 00000000 00000000 00000000	0x00000000	/0	0.0.0.0
10000000 00000000 00000000 00000000	0x80000000	/1	128.0.0.0
11000000 00000000 00000000 00000000	0xC0000000	/2	192.0.0.0
11100000 00000000 00000000 00000000	0xE0000000	/3	224.0.0.0
11110000 00000000 00000000 00000000	0xF0000000	/4	240.0.0.0
11111000 00000000 00000000 00000000	0xF8000000	/5	248.0.0.0
11111100 00000000 00000000 00000000	0xFC000000	/6	252.0.0.0
11111110 00000000 00000000 00000000	0xFE000000	/7	254.0.0.0
11111111 00000000 00000000 00000000	0xFF000000	/8	255.0.0.0
11111111 10000000 00000000 00000000	0xFF800000	/9	255.128.0.0
11111111 11000000 00000000 00000000	0xFFC00000	/10	255.192.0.0
11111111 11100000 00000000 00000000	0xFFE00000	/11	255.224.0.0
11111111 11110000 00000000 00000000	0xFFF00000	/12	255.240.0.0
11111111 11111000 00000000 00000000	0xFFF80000	/13	255.248.0.0
11111111 11111100 00000000 00000000	0xFFFC0000	/14	255.252.0.0
11111111 11111110 00000000 00000000	0xFFFE0000	/15	255.254.0.0
11111111 11111111 00000000 00000000	0xFFFF0000	/16	255.255.0.0
11111111 11111111 10000000 00000000	0xFFFF8000	/17	255.255.128.0
11111111 11111111 11000000 00000000	0xFFFFC000	/18	255.255.192.0
11111111 11111111 11100000 00000000	0xFFFFE000	/19	255.255.224.0
11111111 11111111 11110000 00000000	0xFFFFF000	/20	255.255.240.0
11111111 11111111 11111000 00000000	0xFFFFF800	/21	255.255.248.0
11111111 11111111 11111100 00000000	0xFFFFFC00	/22	255.255.252.0
11111111 11111111 11111110 00000000	0xFFFFFE00	/23	255.255.254.0
11111111 11111111 11111111 00000000	0xFFFFFF00	/24	255.255.255.0
11111111 11111111 11111111 10000000	0xFFFFFF80	/25	255.255.255.128
11111111 11111111 11111111 11000000	0xFFFFFFC0	/26	255.255.255.192
11111111 11111111 11111111 11100000	0xFFFFFFE0	/27	255.255.255.224
11111111 11111111 11111111 11110000	0xFFFFFFF0	/28	255.255.255.240
11111111 11111111 11111111 11111000	0xFFFFFFF8	/29	255.255.255.248
11111111 11111111 11111111 11111100	0xFFFFFFFC	/30	255.255.255.252
11111111 11111111 11111111 11111110	0xFFFFFFFE	/31	255.255.255.254
11111111 11111111 11111111 11111111	0xFFFFFFFF	/32	255.255.255.255

Temporarily Changing the Configuration

You can use **ifconfig** to modify the active Ethernet interface, but the change is only temporary until the next reboot. Therefore, Lucent Remote Access recommends that you use the **set** commands followed by **save all** and **reboot**.

In the following example, the **ifconfig** command is used to change the address of the Ether0 port and the netmask. This approach is useful when you want to quickly (and temporarily) try out a different setting on an interface.

```
Command> ifconfig ether0 address 192.168.100.1 netmask 255.255.255.0
ether0: flags=16<IP_UP,IPX_DOWN,BROADCAST>
inet 192.168.100.1 netmask ffffff00 broadcast 192.168.100.0 mtu 1500
```

To change the configuration of the PortMaster on a more permanent basis use the following commands:

```
Command> set ether0 192.168.100.1
Command> set ether0 netmask 255.255.255.0
Command> save all
Command> reboot
```

Displaying Network Statistics

You can determine if your problems are caused by an overloaded network by using the **show netstat** command. See "Diagnosing an Overloaded Ethernet Network" on page 1-12 for more information.

Tracing Packets

The **ptrace** command allows you to see packet information as it passes through the PortMaster. It is often used in conjunction with **ping** to isolate a routing problem.

The **ptrace** command uses the name of a filter as its argument. The filter narrows the output to only those packets of interest. All packets passing through the PortMaster are evaluated against the selected filter, except for User Datagram Protocol (UDP) and ICMP packets that are generated by the PortMaster itself.

Packets that are permitted by the filter appear on the console with the following packet information:

- Source address of the packet

- Destination address of the packet
- Protocol
- Other protocol-specific information, including source and destination port

To see source and destination packets, including packets generated by the PortMaster, use the following command:

```
Command> ptrace Filtername extended
```

Caution – Avoid making your packet trace filter too general. The packet information sent to the screen can overload the PortMaster because **ptrace** output to the console has a higher interrupt priority than actual data throughput.

To stop viewing packet trace information, enter the following command:

```
Command> ptrace
```

Note – If you are telneting to the PortMaster, you must filter out your own Telnet traffic on TCP port 23 or the **ptrace** output shows the cascading effect of your own output. See "Filtering Telnet Traffic for ptrace" on page 3-13 for more information.

Filtering Telnet Traffic for ptrace

The following is an example of a filter named **all** that denies all Telnet packets while allowing all other IP traffic for evaluation:

```
Command> add filter all
New filter successfully added

Command> set filter all 1 deny tcp src eq 23
Filter all updated

Command> set filter all 2 deny tcp dst eq 23
Filter all updated

Command> set filter all 3 permit
Filter all updated

Command> set console
Setting CONSOLE to admin session
```

```
Command> ptrace all
Packet Tracing Enabled
TCP from 128.165.96.6.1011  to 128.165.64.23.1642seq 7F,ack 0x0, win 4096,    SYN
TCP from 128.165.64.23.1642 to 128.165.96.6.1011 seq 0, ack 0x80,win 0,    RST ACK
UDP from 128.165.96.229.1649to 128.165.96.0.1649
UDP from 128.165.96.16.520  to 128.165.96.0.520
UDP from 128.165.96.135.520 to 128.165.96.0.520
UDP from 128.165.96.2.520   to 128.165.96.0.520
UDP from 128.165.96.2.520   to 128.165.96.0.520
TCP from 128.165.96.6.1011  to 128.165.93.2.1642 seq 7F,ack 0x0, win 4096,SYN
TCP from 128.165.1.93.1642  to 128.165.96.6.1011 seq 0, ack 0x80,win 0,    RST ACK
UDP from 128.165.96.76.520  to 128.165.96.0.520

   Command> ptrace
```

Tracing IP Packets

The following example uses a filter named **i** that shows all packets arriving at or passing through the PortMaster. Using this filter with the **ptrace** command helps to determine why the idle timer is **not** timing out a connection. RIP packets (UDP/520) are considered idle traffic and do not maintain a link that is configured to drop due to lack of traffic.

```
Command> add filter i
New Filter successfully added

Command> set filter i 1 permit
Filter i updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace i
Packet Tracing Enabled
```

Note – Do not use this filter if you are telneted into a PortMaster. See "Filtering Telnet Traffic for ptrace" on page 3-13 for more information.

Tracing DNS Packets

This packet filter shows all Domain Name System (DNS) packets arriving at or passing through the PortMaster. This tool is useful in debugging DNS problems because it shows a user's or host's DNS queries destined for the DNS server and the IP address of the DNS server being accessed. A secondary DNS server that is being accessed too often might indicate that the primary DNS server is having problems.

The PortMaster uses DNS to translate IP addresses into hostnames and for administrative programs like **telnet**, **rlogin**, **ping**, and **traceroute**. DNS runs on UDP port 53 for DNS queries and responses. DNS zone transfers run on TCP port 53.

```
Command> add filter dns
New Filter successfully added

Command> set filter dns 1 permit udp src eq 53
Filter dns updated

Command> set filter dns 2 permit udp dst eq 53
Filter dns updated

Command> set filter dns 3 permit tcp src eq 53
Filter dns updated

Command> set filter dns 4 permit tcp dst eq 53
Filter dns updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace dns
Packet Tracing Enabled

UDP from 192.168.1.2.53 to 192.168.1.3.1025
UDP from 192.168.1.2.53 to 192.168.1.3.1025
UDP from 192.168.1.2.53 to 192.168.1.154.1238
UDP from 10.41.69.222.1330 to 192.168.1.2.53
UDP from 192.168.1.2.53 to 10.41.69.222.1330
UDP from 192.168.1.137.1097 to 192.168.1.2.53
UDP from 192.168.1.2.53 to 204.192.168.1.137.1097
UDP from 192.168.1.137.1102 to 192.168.1.2.53
UDP from 192.168.1.2.53 to 192.168.1.137.110

Command> ptrace
```

Tracing IPX Packets

This packet filter shows all IPX packets passing through the PortMaster. It does **not** show IPX packets originating from the PortMaster.

```
Command> add filter seeipx
New Filter successfully added

Command> set ipxfilter seeipx 1 permit
Filter seeipx updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace seeipx
Packet Tracing Enabled

IPX from 00000008:0000C06F195C:0455 to 00000008: FFFFFFFFFFFF:0455
IPX from 00000008:0000C06F195C:0553 to 00000008: FFFFFFFFFFFF:0553
IPX from 00000008:0000C06F195C:0455 to 00000008: FFFFFFFFFFFF:0455
IPX from 00000008:0000C06F195C:0553 to 00000008: FFFFFFFFFFFF:0553

Command> ptrace
```

IPX packets are represented in the following format. All **F**s in a "to" address represent a broadcast to the entire network.

```
[8-digit network number]:[12-digit node address]:[4-digit socket number]
```

Tracing TCP Packets

This packet filter shows all TCP packets arriving at or passing through the PortMaster. TCP packets are used by applications such as HTTP (World Wide Web), FTP, Telnet and many others.

1. **Create a filter called** ctcp**:**

```
Command> add filter ctcp
New Filter successfully added

Command> set filter ctcp 1 permit tcp
Filter ctcp updated
```

2. **If you want to see only packets from TCP negotiations, add the** estab **keyword:**

```
Command> set filter ctcp 1 deny tcp estab
Filter ctcp updated

Command> set filter ctcp 2 permit tcp
Filter ctcp updated
```

3. **Set the console and issue the** ptrace **command:**

```
Command> set console
Setting CONSOLE to admin session

Command> ptrace ctcp
Packet Tracing Enabled
```

If you are telneting into the PortMaster, see "Filtering Telnet Traffic for ptrace" on page 3-13

Tracing UDP Packets

This packet filter shows all UDP packets arriving at or passing through the PortMaster. UDP packets are used by applications such as DNS, RADIUS, **finger**, **whois**, and **traceroute**.

```
Command> add filter cudp
New Filter successfully added

Command> set filter cudp 1 permit udp
Filter cudp updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace cudp
Packet Tracing Enabled

UDP from 128.165.96.16.520 to 128.165.96.0.520
UDP from 128.165.96.229.1649 to 128.165.96.0.1649
UDP from 128.165.96.135.520 to 128.165.96.0.520
UDP from 128.165.96.2.520 to 128.165.96.0.520
UDP from 128.165.96.2.520 to 128.165.96.0.520
```

```
UDP from 128.165.96.76.520 to 128.165.96.0.520
UDP from 128.165.96.16.520 to 128.165.96.0.520
UDP from 128.165.96.229.1649 to 128.165.96.0.1649

Command> ptrace
```

Tracing Ping Packets

This packet filter shows all pings arriving at or passing through the PortMaster. This tool is useful in debugging routing problems because a ping echo request often arrives at the destination host but the echo reply cannot return. Using this packet trace filter at different points along the path can help diagnose the problem.

```
Command> add filter p
New Filter successfully added

Command> set filter p 1 permit icmp
Filter p updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace p
Packet Tracing Enabled

Command> ptrace
```

The following example shows **ptrace** output of pings **arriving at** the PortMaster. (The PortMaster in this example has an IP address of 10.0.0.3.)

```
icmp from 192.168.148.1 to 10.0.0.3 type Echo Request
icmp from 192.168.148.1 to 10.0.0.3 type Echo Request
icmp from 192.168.148.1 to 10.0.0.3 type Echo Request
```

The following example shows **ptrace** output of pings **passing through** the PortMaster:

```
icmp from 192.168.148.1 to 10.0.0.15 type Echo Request
icmp from 10.0.0.15 to 192.168.148.1 type Echo Reply
```

Tracing RIP Packets

This packet filter shows all RIP packets arriving at the PortMaster.

RIP uses UDP port 520 to transmit routing information between hosts. UDP is one of the protocols the PortMaster uses to learn dynamic routing information and is useful in debugging routing problems. A host broadcasting RIP broadcasts its routing table at least once every 30 seconds.

For example, the following filter shows RIP packets being advertised by other routers or workstations:

```
Command> add filter rip
New Filter successfully added

Command> set filter rip 1 permit udp src eq 520
Filter rip updated

Command> set console
Setting CONSOLE to admin session

Command> ptrace rip
Packet Tracing Enabled

UDP from 192.168.1.5.520 to 192.168.1.255.520
UDP from 192.168.1.6.520 to 192.168.1.0.520
UDP from 192.168.1.6.520 to 192.168.1.0.520
UDP from 192.168.1.6.520 to 192.168.1.0.520
UDP from 192.168.1.13.520 to 255.255.255.255.520
UDP from 192.168.1.1.520 to 255.255.255.255.520
UDP from 192.168.1.8.520 to 192.168.1.0.520
UDP from 192.168.1.6.520 to 192.168.1.0.520
UDP from 192.168.1.13.520 to 255.255.255.255.520

Command> ptrace
```

Troubleshooting Routing

The following sections explain how to locate an incorrect static route and how to use the **traceroute** command to diagnose routing problems. For more detailed information on how to troubleshoot particular routing protocols such as BGP, OSPF or RIP, see the *PortMaster Routing Guide*.

Locating an Incorrect Static Route

If packets are not reaching their destination, an incorrect static route might be the cause. Examine the IP routing table with the **show routes** command. (In the following example, the optional keyword **local** limits the output to those routes that match the string **local**.)

```
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
```

Specifying an IP address and netmask displays routes only to that destination:

```
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
```

The **show routes** command output helps to verify that no static route exists for your local IP Ethernet network. A static route appears with the flag **NS**; a normal entry for the Ethernet network displays the **NL** flag and **ether0** as the interface. A static route overrides the default route and interferes with normal Ethernet routing.

To remove the route, use the following command. Replace the IP address with your IP network address—the destination shown in the routing table:

```
Command> delete route 192.168.7.0
```

If you are using the OSPF or BGP routing protocol, refer to the *PortMaster Routing Guide* for more troubleshooting information.

Note – If some types of packets reach their destination but others do not, a routing problem is not the cause. For example, if small packets reach their destination, but big packets do not, this behavior indicates a problem in Layer 1 or 2 of the Open Systems Interconnection (OSI) model.

Tracing a Route

Traceroute is a useful tool for debugging routing problems. You can use it to identify the routers used to reach a remote host. While **ping** checks only end-to-end connectivity, **traceroute** tries to characterize each hop in the path to a destination. The **traceroute** command sends UDP packets to the specified host and listens for ICMP messages returning. When you enter the hostname or IP address of the destination host with the **traceroute** command, a list of router addresses is displayed in the order they are encountered.

If a routing problem exists, packets often get to their destination but do not return. If you can determine via **ptrace** (see page 3-12) that packets are arriving at their destination, you can use **traceroute** from that destination back to the first router and see where the routes go off course.

To trace the route to a remote host, use the following command:

```
Command> traceroute Ipaddress
```

To stop **traceroute**, enter the command with no IP address:

```
Command> traceroute
```

If routing has stopped and a network can no longer connect to the Internet, do the following:

1. **Use the** traceroute **command from the isolated LAN to the router to display the last IP address seen.**

2. **Use the** traceroute **command from the router to the isolated LAN and note the last IP address.**

   The routing problem is usually located between the LAN and that address.

   ```
   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
   ```

   The **traceroute** command sends UDP packets until it gets an ICMP packet back from the specified IP address or host.

3. **If the destination is unreachable, terminate traceroute manually by entering the command without an IP address.**

The **traceroute** command shows IP addresses only (not hostnames) and does not show the times associated with each hop.

For more information on the **traceroute** command, see the *PortMaster Command Line Reference*.

Finding a Particular Route

If **traceroute** reaches its target and **ping** does not—or vice versa—check routing with the **show routes to-dest** command to determine if the two addresses are being routed differently. This is a common routing problem over Frame Relay connections.

The **show routes to-dest** command displays detailed information about which route in the routing table the PortMaster uses to send a packet to a particular destination. Contrast this command with the **show routes** command, which lists the PortMaster's entire routing table. Using **show routes to-dest** allows you to find a particular route without having to search the whole routing table manually.

The following is sample output from the **show routes** command:

```
Command> show routes

Destination       Mask  Gateway             Source  Flag Met  Interface
---------------- ----  ------------------- ------- ---- ---  --------
0.0.0.0           0     128.198.110.2       local   NS   1    ether0
128.165.110.64    27    128.165.110.4       rip     ND   2    ether0
128.165.0.0       27    128.165.110.9       rip     ND   3    ether0
128.165.110.0     27    128.165.110.3       local   ND   1    ether0
192.168.32.0      24    128.165.110.9       rip     ND   2    ether0
10.0.0.0          8     128.165.110.9       rip     ND   3    ether0
```

To find the particular route in the routing table that will forward an IP packet with a destination address of 128.165.110.68, use the **show routes to-dest** command as follows:

```
Command> show routes to-dest 128.165.110.68
Destination        Mask Gateway             Source  Flag Met  Interface
-----------------  ---- ------------------- ------- ---- ---  ---------
128.165.110.64     27   128.165.110.4       rip     ND   2    ether0
```

The route 128.165.110.64 is a **network** route with a 27-bit subnet mask. The route will deliver IP packets to any of the IP addresses between 128.165.110.65 and 128.165.110.94 (128.165.110.64 is the network address and 128.165.110.95 is the broadcast address). The PortMaster displays this route because 128.165.110.68 is a member of this subnet.

If the destination you specify is not in the routing table and a default route exists, the PortMaster uses the default route to forward the packet:

```
Command> show routes to-dest 192.168.10.2

Destination       Mask  Gateway              Source  Flag Met  Interface
----------------- ----  -------------------- ------- ---- ---  --------
0.0.0.0           0     128.165.110.2        local   NS   1    ether0
```

If the destination you specify is not in the routing table and no default route exists, the command output is the following:

```
Command> show routes to-dest 1.1.1.1

Destination       Mask  Gateway              Source  Flag Met  Interface
----------------- ----  -------------------- ------- ---- ---  ---------

Command>
```

Solving PPP Problems 4

Use Table 4-1 to identify and diagnose some common Point-to-Point Protocol (PPP) problems.

Table 4-1 Common PPP Problems

Problem	Possible Cause	Possible Solution
A connection fails while the PortMaster is negotiating PPP.	Authentication failure and/or protocol negotiation failure.	See "Debugging and Interpreting PPP Negotiation" on page 4-2.
Multichassis PPP is not functioning.	All the chassis used in Multichassis PPP are not on the same Ethernet segment.	See "Diagnosing Multichassis PPP Problems" on page 4-5.
When using Multichassis PPP, calls do not roll over to the next chassis.	Misconfigured endpoint discriminator.	See "Endpoint Discriminator Misconfiguration" on page 4-6.
A user cannot dial in to a PortMaster that is using Multichassis PPP.	A suspended session for a particular user.	See "Dial-In Problems with Multichassis PPP" on page 4-7
When using Multilink PPP or Multichassis PPP, calls do not roll over to the next chassis.	Incorrect configuration at the telephone company.	See "Diagnosing a Hunt Group Rollover Problem" on page 4-8.
Compression is not working correctly.	Compression history slots are not being released.	See "Troubleshooting Compression" on page 4-10.

Debugging and Interpreting PPP Negotiation

You can debug and interpret the PPP negotiation process using the commands and information in this section.

1. **To debug PPP negotiations, enter the following commands on the PortMaster:**

   ```
   Command> set console
   Command> set debug 0x51
   ```

   The **set debug 0x51** command allows observation of PPP negotiation, such as the following example:

```
Sending LCP_CONFIGURE_REQUEST to port S1 of 24 bytes containing:
01 01 00 18 02 06 00 00 00 00 05 06 d4 55 9b ea 07 02 08 02 03 04 c0 23
Received LCP_CONFIGURE_ACK on port S1 of 20 bytes containing:
02 01 00 18 02 06 00 00 00 00 05 06 d4 55 9b ea 07 02 08 02 03 04 c0 23
Received LCP_CONFIGURE_REQUEST on port S1 of 16 bytes containing:
01 03 00 14 02 06 00 00 00 00 05 06 2b 3a eb 57 07 02 08 02
Sending LCP_CONFIGURE_ACK to port S1 of 20 bytes containing:
02 03 00 14 02 06 00 00 00 00 05 06 2b 3a eb 57 07 02 08 02
S1: LCP Open
Received PAP_AUTH_REQ on port S1 of 24 bytes containing:
01 01 01 11 01 6b 71 73 6a 71 6f 72 2a 68 76 09 36 31 35 37 32 34 36 39
Sending PAP_AUTH_ACK to port S1 of 20 bytes containing:
02 01 00 14 0f 4c 6f 67 69 6e 20 53 75 63 63 65 65 64 65 64
Sending IPCP_CONFIGURE_REQUEST to port S1 of 16 bytes containing:
01 01 00 10 02 06 00 2d 0f 00 03 06 c0 a8 05 19
Received IPCP_CONFIGURE_REQUEST on port S1 of 12 bytes containing:
01 01 00 10 02 06 00 2d 0f 00 03 06 c0 a8 0a 20
Sending IPCP_CONFIGURE_ACK to port S1 of 16 bytes containing:
02 01 00 10 02 06 00 2d 0f 00 03 06 c0 a8 0a 20
Received IPCP_CONFIGURE_ACK on port S1 of 12 bytes containing:
02 01 00 10 02 06 00 2d 0f 00 03 06 c0 a8 05 19
S1: IPCP Open
LCP IPCP Open
```

```
Connection Succeeded
```

Caution – User IDs and passwords are transmitted at the "Received PAP_AUTH_REQ" message in PPP negotiation. Anyone can use the PPP Decoder Ring to translate user IDs and passwords. Therefore, you must protect PPP debug output as you would actual passwords.

2. **Enter 0x51 debug output into the Livingston PPP Decoder Ring (dring) located at** http://www.livingston.com/Tech/Support/debug-tools.shtml**.**

   The output in the previous example is decoded as follows:

```
Dring: Decoder Ring for Livingston Product PPP traces
-----------------------------------------------------

Sending LCP_CONFIGURE_REQUEST to port S1 of 24 bytes containing:

01 01 00 18 02 06 00 00 00 00 05 06 D4 55 9B EA 07 02 08
02 03 04 C0 23

    Packet Info:  Code: 01, ID: 01, 24 bytes.
    Async-Control-Character-Map [0x02], length: (6 bytes), [0x00000000]
    Magic-Number [0x05], length: (6 bytes), [0xD4559BEA]
    Protocol-Field-Compression [0x07], length: (2 bytes)
    Address-and-Control-Field-Compression [0x08], length: (2 bytes)
    Authentication-Protocol [0x03], length: (4 bytes), Password Authentication
    Protocol [0xC023]

Received LCP_CONFIGURE_ACK on port S1 of 20 bytes containing:
02 01 00 18 02 06 00 00 00 00 05 06 D4 55 9B EA 07 02 08
02 03 04 C0 23

    Packet Info:  Code: 02, ID: 01, 24 bytes.
    Async-Control-Character-Map [0x02], length: (6 bytes), [0x00000000]
    Magic-Number [0x05], length: (6 bytes), [0xD4559BEA]
    Protocol-Field-Compression [0x07], length: (2 bytes)
    Address-and-Control-Field-Compression [0x08], length: (2 bytes)
    Authentication-Protocol [0x03], length: (4 bytes), Password Authentication
    Protocol [0xC023]

Received LCP_CONFIGURE_REQUEST on port S1 of 16 bytes containing:
01 03 00 14 02 06 00 00 00 00 05 06 2B 3A EB 57 07 02 08 02
```

```
    Packet Info:  Code: 01, ID: 03, 20 bytes.
    Async-Control-Character-Map [0x02], length: (6 bytes), [0x00000000]
    Magic-Number [0x05], length: (6 bytes), [0x2B3AEB57]
    Protocol-Field-Compression [0x07], length: (2 bytes)
    Address-and-Control-Field-Compression [0x08], length: (2 bytes)

Sending LCP_CONFIGURE_ACK to port S1 of 20 bytes containing:
02 03 00 14 02 06 00 00 00 00 05 06 2B 3A EB 57 07 02 08 02

    Packet Info:  Code: 02, ID: 03, 20 bytes.
    Async-Control-Character-Map [0x02], length: (6 bytes), [0x00000000]
    Magic-Number [0x05], length: (6 bytes), [0x2B3AEB57]
    Protocol-Field-Compression [0x07], length: (2 bytes)
    Address-and-Control-Field-Compression [0x08], length: (2 bytes)
    **** S1: LCP Open

Received PAP_AUTH_REQ on port S1 of 24 bytes containing:
01 01 00 18 0A 6A 73 74 6F 72 6D 73 2D 67 77 08 31 32 33 34 35 36 37 38

    Packet Info:  Code: 01, ID: 01, 24 bytes.
    Login ID: bart (10 bytes), [0x6A73746F726D732D6777]
    Password: 12345678 (8 bytes), [0x3132333435363738]

Sending PAP_AUTH_ACK to port S1 of 20 bytes containing:
02 01 00 14 0F 4C 6F 67 69 6E 20 53 75 63 63 65 65 64 65 64

    Packet Info:  Code: 02, ID: 01, 20 bytes.
    Message:  Login Succeeded (15 bytes),
    [0x4C6F67696E20537563636565646564]

Sending IPCP_CONFIGURE_REQUEST to port S1 of 16 bytes containing:
01 01 00 10 02 06 00 2D 0F 00 03 06 C0 A8 05 19

    Packet Info:  Code: 01, ID: 01, 16 bytes.
    IP-Compression-Protocol  [0x02], length: (6 bytes), Van Jacobson
    Compressed TCP/IP  [0x002D0F00]
    IP-Address  [0x03], length: (6 bytes), [192.168.5.25]

Received IPCP_CONFIGURE_REQUEST on port S1 of 12 bytes containing:
01 01 00 10 02 06 00 2D 0F 00 03 06 C0 A8 0A 20

    Packet Info:  Code: 01, ID: 01, 16 bytes.
    IP-Compression-Protocol  [0x02], length: (6 bytes), Van Jacobson
    Compressed TCP/IP  [0x002D0F00]
    IP-Address  [0x03], length: (6 bytes), [192.168.10.32]
```

```
Sending IPCP_CONFIGURE_ACK to port S1 of 16 bytes containing:
02 01 00 10 02 06 00 2D 0F 00 03 06 C0 A8 0A 20

    Packet Info:  Code: 02, ID: 01, 16 bytes.
    IP-Compression-Protocol  [0x02], length: (6 bytes), Van Jacobson
    Compressed TCP/IP  [0x002D0F00]
    IP-Address  [0x03], length: (6 bytes), [192.168.10.32]

Received IPCP_CONFIGURE_ACK on port S1 of 12 bytes containing:
02 01 00 10 02 06 00 2D 0F 00 03 06 C0 A8 05 19

    Packet Info:  Code: 02, ID: 01, 16 bytes.
    IP-Compression-Protocol  [0x02], length: (6 bytes), Van Jacobson
    Compressed TCP/IP  [0x002D0F00]
    IP-Address  [0x03], length: (6 bytes), [192.168.5.25]

**** S1: IPCP Open

**** LCP IPCP Open

Connection Succeeded
```

3. **Turn off debugging:**

   ```
   Command> set debug off
   ```

For information about PPP frame formats, see Appendix B, "PPP Packet Formats."

Diagnosing Multichassis PPP Problems

All PortMaster 3 chassis used for Multichassis PPP must be connected to the same Ethernet segment. Two chassis can have a switch separating them on the segment if necessary, but not a router. If Multichassis PPP is not working, verify that all the chassis in the Multichassis PPP domain are connected to the same Ethernet segment, and that no routers are connected between chassis.

Multichassis PPP problems can be diagnosed with the following **show** commands:

- **show global**—displays the endpoint discriminator.
- **show session**—displays information about physical and virtual connections.
- **show mcppp**—displays neighbors of the PortMaster and information about physical slave or virtual connections.

See the glossary at the end of this guide for definitions of Multichassis PPP terms.

Endpoint Discriminator Misconfiguration

If connections to a Multichassis PPP domain are not rolling over from one PortMaster to another, a PortMaster might have a misconfigured endpoint discriminator. All chassis in a single Multichassis PPP domain must have the same endpoint discriminator.

To check the endpoint discriminator on each PortMaster in a Multichassis PPP domain, use the **show global** command:

```
Command> show global
                System Name:   pm3
               Default Host:   0.0.0.0
             Alternate Hosts:
                  IP Gateway:   174.154.96.2
              Gateway Metric:   1
             Default Routing:   Quiet (Off)
               OSPF Priority:   0
              OSPF Router ID:   174.154.96.68 (default)
                Name Service:   DNS
                 Name Server:   174.154.1.70
                      Domain:   livingston.com
          Telnet Access Port:   23
                    Loghost:   0.0.0.0
           Maximum PMconsole:   1
            Assigned Address:   0.0.0.0
               RADIUS Server:   0.0.0.0
            Alternate Server:   0.0.0.0
           Accounting Server:   0.0.0.0
           Alt. Acct. Server:   0.0.0.0
            ISDN Switch Type:   NI-1
              End Point Disc:   666600000000
            Disabled Modules:   SNMP
```

To change the endpoint discriminator, use the **set endpoint** command, replacing *Hex* with any hexadecimal number up to 12 digits long:

```
Command> set endpoint Hex
Command> save all
Command> reboot
```

Note – If you set the endpoint discriminator to a number less than 12 digits, the **show global** command output displays the number followed by as many zeros as needed to make a 12-digit number. For example, if you set the endpoint discriminator to **1**, the show global command output displays the endpoint discriminator as **100000000000**.

Dial-In Problems with Multichassis PPP

If a user cannot dial in to a PortMaster on a Multichassis PPP domain, a previous session for that user might still be running on the PortMaster. To display information about physical and virtual connections on a PortMaster, use the **show sessions** and **show mcppp** commands as described in the following sections.

If you find an active session for a user who has logged out, reset the session's port using the **reset** command:

```
Command> reset v0
Resetting port V0
```

Resetting a virtual port resets the corresponding physical port at the peer, as well. Resetting a physical port also resets the corresponding virtual port at the peer.

Displaying Port Usage Information

The **show sessions** command displays the current use of all ports. In the following example, the user **hassan** is connected to two physical ports and one virtual port corresponding to a physical port on a slave unit:

```
pm3> show sessions
Port   User      Host/Inet/Dest   Type      Dir   Status          Start    Idle
-----  ------    ----------------  ------    ---   --------        ------   -----
                 --                          -                   -        -
C0     -         -                Login     In    USERNAME        0        0
S0     hassan    174.154.32.35    Netwrk    In    ESTABLISHED     1:04     1:04
S1     hassan    174.154.32.35    Netwrk    In    ESTABLISHED     3        1:04
```

```
S2                                  Log/Net   In    NO-SERVICE      0       0
...
...
S23                                 Log/Net   In    NO-SERVICE      0       0
V0     hassan    174.154.32.35      Netwrk    In    ESTABLISHED     0       0
```

Displaying Multichassis PPP Information

The **show mcppp** command displays the IP addresses of PortMaster neighbors and any Multichassis PPP connections. The PortMaster in the following example has two neighbors (174.154.96.67 and 174.154.96.99) and one virtual connection for user **hassan** on port **V0** with the physical port residing at the peer (174.154.96.67):

```
pm3> show mcppp
Neighbors:
174.154.96.67
174.154.96.99

Port      User      Host/Inet/Dest   Type      Peer
-----     -------   --------------   -------   --------
V0        hassan    174.154.32.35    VIRTUAL   174.154.96.67
```

Diagnosing a Hunt Group Rollover Problem

If the hunt group is failing to roll over on PRI line, use the following steps to determine if the problem originates at the telephone company rather than with the PortMaster:

1. **From a Telnet (not a terminal) command line session, attach to the S0 port.**

   ```
   Command> attach s0
   Trying 192.168.1.1 ...

   Connected - Escape character is '^]'.
   ```

2. **Dial the PortMaster back into itself, replacing *Number* with the 7-digit telephone number of the PortMaster:**

   atdt*Number*
   ```
   Dialing...
   CONNECT 64000
   ```

The PortMaster is now connected to its own S1 port.

3. **Login as** !root **and enter the administrative password:**

```
login: !root
password: xxxxxx
```

4. **Ports S0 and S1 are now busy. Attach to the S2 port:**

```
Command> attach s2
Trying 192.168.1.1 ...
Connected - Escape character is '^]'.
```

5. **Dial the PortMaster back into itself:**

```
atdtNumber
Dialing...
CONNECT 64000
```

The PortMaster is now connected to its own S3 port.

6. **Repeat this process until all interfaces are connected.**

Use Table 4-2, if necessary, to identify the interfaces on your PortMaster.

Table 4-2 PortMaster Interfaces

Line Type	Model or Circuit	Ports
T1 Primary Rate Interface (PRI)	PM-3A-1T	S0 through S23
	PM-3A-2T	S0 through S22 S24 through S46
E1 PRI	PM-3A-1E	S0 through S29
	PM-3A-2E	S0 through S59
Channelized T1	One T1 circuit	S0 through S23
	Two T1 circuits	S0 through S47
Channelized E1	One E1 circuit	S0 through S29
	Two E1 circuits	S0 through S59

If the hunt group does not roll over to the next chassis, the telephone company has a problem with the provisioning. Contact your carrier for assistance.

Troubleshooting Compression

You can use the **set debug ccp-lzs** command to display Compression Control Protocol (CCP) information such as the allocation of compression data structures (called history slots), error messages, and reinitializations to the console. When compression is working, compression is freed and compression history slots are released when a user session is terminated, as shown in the following example:

```
Command> set console
Setting console to ADMIN session

Command> set debug ccp-lzs on

CCP 55230 for (S4) Pinahara slot 0
CCP 55230 freed by COMPORT S4
Releasing compression history slot 0
```

Solving ISDN Problems 5

Use Table 5-1 to identify and diagnose common ISDN problems.

Table 5-1 Common ISDN Problems

Problem	Possible Cause	Possible Solution
An ISDN Basic Rate Interface (BRI) or Primary Rate Interface (PRI) connection is slow, or data is corrupted in transit.	Excessive errors on the ISDN line.	Diagnose with the **show isdn** command. An error count greater than 20 indicates a problem at the telephone company. (See page 5-2 for BRI connections and page 5-5 for PRI connections.)
The PortMaster cannot establish or maintain an ISDN BRI connection.	An incorrect configuration on the port	Use the **show isdn** command to check the status and configuration of the port (page 5-3).
The PortMaster cannot establish or maintain an ISDN PRI connection.	• Failed circuit. • Failed D channel. • Incorrect configuration on the port. • No synchronization with the T1 switch. • PRI connection needs to be reset at the switch.	Use the procedure on page 5-5 to verify the status and configuration of an ISDN PRI port. Use the procedure on page 5-6 to determine if the PortMaster and the T1 switch are synchronized. Use the **set line0 loopback** command to reset the PRI connection at the switch (page 5-8)
The PortMaster cannot establish or maintain an ISDN connection.	Problems with ISDN negotiation or packet exchange.	Use the **set debug isdn** commands to display ISDN negotiation and packet exchange information to the console (page 5-9).

Troubleshooting an ISDN BRI Connection

If you are having trouble with an ISDN BRI connection, use the following procedures to diagnose the problem.

Verifying LEDs

Verify the LED state:

1. **Check the LED states as follows and compare its behavior to Table 5-2:**
   - On an Office Router OR-U, check the NT1 LED.
   - On a PortMaster 2E, PortMaster 2Ei, or PortMaster 2i, check the appropriate BRI status LED on the back of the five-BRI expansion board.

Table 5-2 ISDN BRI LED Indications

LED Behavior	Indication
Solidly lit	Synchronization and SPID registration
Flashing slowly	Synchronization only
Flashing rapidly	No synchronization or SPID registration

2. **If the LED indicates no SPID registration, check the SPID and directory number with the** show isdn *D0* **command.**

   Verify that the configured SPID and directory number match those given to you by the telephone company, as described in Step 3 on page 5-4.

3. **If the LED indicates no synchronization, check the state of the D channel.**

   Verify that the D channel is functioning properly by using the **show isdn** command. The interface state should be **F7**. If the interface state is not F7, do the following:
   - Check that the cables are properly installed.
   - Call the telephone company and ask them to check the line to ensure that it is functioning properly.

Checking the Physical Interface with show isdn

Follow these steps to check the physical interface of ISDN ports:

1. **Enter the** show isdn **command.**

   The output displays D channel status for the ISDN BRI ports.

```
Command> show isdn
D       Ports       Bri Layer1   Inits   Uptime   Change   In      Out     Err
----    -----       ----------   -----   ------   ------   ---     ----    ---
                                                                             -
D00     (S01/02)    F7-active    1       4days    4days    74974   79221   0
```

   See the *PortMaster Command Line Reference* for an explanation of this output.

2. **Check the D channel information.**

   You can display comprehensive information about each BRI port by using the **show isdn** command and specifying either a logical serial port number associated with the port or a D channel number. For example:

```
Command> show isdn d0
D00 status ----------------------(127) 88 89 --------- BRI_NI1

Interface state: F7- active
Init count:        1  uptime:  10days   last state change:  10days
recv count:  201647    xmit:  217352               errors:        0
numberplan              type:   Local                  plan: ISDN E.164

S0 ------------------------------------------------------------

Ces state: Connected    last change: 10days Port state: ESTABLISHED
Directory:          4684400   SPID:   510468440000  regs:      1
Called:                  Caller:                  Flags:  0x00
Connects:       1   last connect: 10days      b channel: 1 0
Setup: 04 03 08 00 10 18 02 01 01 34 01 4f 70 09 04 01
34 36 38 34 34 30 30 04 02 88 90 18 01 89 34 01

S1 ------------------------------------------------------------

 Ces state: Registered   last change: 10days Port state: IDLE
```

```
Directory:          4684401    SPID:    510468440101  regs:      1
Called:                     Caller:      5107352832 Flags:  0x02
Connects:      56    last connect:       0      b channel: 2 1
Setup: 04 03 08 00 10 18 02 01 02 34 01 4f 6c 0c 02 01
35 31 30 37 33 35 32 38 33 32 70 09 04 01 34 36

17210455: msg 5 Disconnect, cause 11 User Busy
17210753: msg 5 Disconnect, cause 1C Invalid Number Format
17268550: msg 5 Disconnect, cause 10 Normal Clearing
```

3. **Use the following information to diagnose ISDN BRI problems:**

   – **Interface state**—indicates the physical interface layer state. This can be **down**, **pending,** or **active**.

   – **CES state**—on an active ISDN connection, the connection establishment sessions (CES) state must be **connected**. If the CES state is **idle**, but the interface state is **active**, it indicates that the D channel is down.

   – **Directory** and **SPID**—Check these values against the information given to you by the telephone company. If either the directory number or service profile identifier (SPID) is not configured correctly, use the following commands to reconfigure them:

     ```
     Command> set S0 dn Number

     Command> set S0 spid Number
     ```

     For more information about configuring the PortMaster for ISDN, see the *PortMaster Configuration Guide*.

   – **Number plan** and **number type**—These are numbering formats for the telephone numbers the telephone company uses for ISDN connections. The PortMaster learns these automatically unless a particular number plan or number type has been entered manually with the following commands:

     ```
     Command> set isdn-numberplan Plan

     Command> set isdn-numbertype Type
     ```

     For more information about configuring the PortMaster for ISDN, see the *PortMaster Configuration Guide*. For more information about these commands, see the *PortMaster Command Line Reference*.

– **Cause Codes**—ISDN cause codes are standard messages that are received from networks conforming to the European Telecommunication Standards Institute (ETSI), ISDN2, and INS Net64 Japanese specifications. See Appendix A, "ISDN Cause Codes," for a full description.

Troubleshooting an ISDN PRI Connection

If you are having trouble with an ISDN PRI connection, use the following procedure to diagnose the problem:

1. **Use the** show isdn **command to display the status of the D channels for ISDN PRI ports.**

   The output shows

   – Whether the circuit is connected—active. The D channel must be in an **active** state.

   – Whether the D channel is operational—carrying data. If the **In** and **Out** columns display 0s, the D channel is not carrying data.

   – Whether an ISDN connection exists.

```
Command> show isdn

D  Ports    State      Change Start Up     Down   Time   Sess    In Out Err

-- ------- --------- ------ ----- ----- ----- ----- ------ ------- -------

0 Active     25days      0      4    504    504      61 0 0 0 0
```

   See the *PortMaster Command Line Reference* for an explanation of this output.

2. **Use the** show line0 **and** show line1 **commands to display information about the physical interface.**

The following example is from a PortMaster with a PRI EI line:

```
Command> show line0
---------------------- line0 - E1 Primary Rate ISDN  ----------------------
Status: DOWN         F3    Framing: FAS     Encoding: HDB3       PCM: a-law

                           Violations
                           --------------------------------
                           Bipolar          1209159
                           CRC4             0
                           E-bit            0
                           FAS              0
```

High numeric values indicate a possible configuration problem. Changing the framing and encoding with the following commands might solve the problem:

```
Command> set line0 framing esf|d4|crc4|fas
```

```
Command> set line0 encoding b8zs|ami|hdb3
```

For more information about these commands, see the *PortMaster Command Line Reference*.

Establishing Synchronization for an ISDN PRI Connection

Use the following procedure to see if the PortMaster and the PRI switch are synchronized:

1. **Set the console and turn on ISDN frame debugging:**

```
Command> set console
Setting CONSOLE to admin session
```

```
Command> set debug isdn-d
Setting ISDN debugging
```

The following debug output is from a PortMaster 3 with a nonfunctioning ISDN PRI circuit. Physical connectivity might exist between the digital facility demarcation point and the PortMaster 3, but the ISDN PRI D channel is still not operating. The

D0: send 00 01 7f pattern originates from the PortMaster 3 and is sent to the switch via the digital facility. The PortMaster 3 normally receives the **D0: recv 00 01 73** patterns in response from the switch.

```
D0: Data Link Down
D0: Data Link Down
D0: send 00 01 7f
D0: send 00 01 7f
D0: send 00 01 7f
D0: send 00 01 7f
D0: Data Link Down
D0: Data Link Down
D0: send 00 01 7f
D0: send 00 01 7f
D0: send 00 01 7f
D0: send 00 01 7f
```

2. **Check the red and green LEDs on the back of the PortMaster 3.**

   If the LEDs are solidly lit, the PortMaster is synchronized with the switch and the PRI facility is functioning.

3. **Confirm physical synchronization with the switch by using the** show line0 **or** show line1 **command:**

```
Command> show line0
------------------------ line0 - T1 Primary Rate ISDN  ---------
Status: UP            Framing: ESF    Encoding: B8ZS       PCM: u-law
Receive Level:        +2dB to -7.5dB
Alarms                                Violations
-----------------------------------   --------------------------------
Blue                  0               Bipolar             102
Yellow                0               CRC Errors          1
Receive Carrier       0               Multiframe Sync     9
Loss
Loss of Sync          0
```

   If the switch and the PortMaster are synchronized, the line status is **up** and the amplitude range for the receive level is approximately 9.5 decibels (dB). This command monitors only physical connectivity (PRI facility status).

If your command output shows that the PortMaster 3 PRI facility is synchronized with the switch, they can start the handshaking process to establish the D channel data link for the PRI. The PortMaster does not attempt to establish the D channel until it is physically connected to the switch.

If the PortMaster PRI facility is not connected to and synchronized with the switch, the **show line0** command provides no output.

Resetting a PRI Connection at the Switch

If a PRI connection is not functioning, and other troubleshooting measures have not solved the problem, you can reset the PRI connection at the switch by turning loopback mode on and then turning it off 15 seconds later. For example:

```
Command> set line0 loopback on
Loopback set ON for Line0

Command> set line0 loopback off
Loopback set OFF for Line0
```

Interpreting Send and Receive Patterns

Check the **set debug isdn-d** output (see page 5-6). If you **never** see a **recv** (receive) pattern, no connectivity exists between the switch and the PortMaster at the D channel level. The telephone service provider needs to investigate the problem.

If you see **recv** patterns **only** and no **send** patterns, a problem exists with the PortMaster 3. Try the following:

- Verify the line configuration. If you make any changes to the ISDN or to Line1 or Line0 configuration, you must use the **save all** command and reboot the PortMaster for the changes to take effect.
- Reset the D channel with the **reset** *D0* command.
- Reboot the PortMaster.

When a D channel becomes operational, the green LED is on and the red LED is off and **set debug isdn-d** output is similar to the following example:

```
D0: Data Link Down
D0: send 00 01 7f
D0: recv 00 01 73
```

```
D0: Data Link UP
D0: send 00 01 01 01
D0: recv 00 01 01 01
D0: send 00 01 01 01
D0: recv 00 01 01 01
D0: send 00 01 01 01
D0: recv 00 01 01 01
.
.
.
```

The following example shows normal PRI D channel activity with no incoming calls:

```
D0: send 00 01 01 2f
D0: recv 00 01 01 2f
D0: send 00 01 01 2f
D0: recv 00 01 01 2f
D0: send 00 01 01 2f
D0: recv 00 01 01 2f
```

This pattern repeats. Other data passes as calls are connected to B channels.

Using Debug ISDN Commands

The **set debug isdn** command sends debug information to the console. These commands toggle on and off. ISDN debugging options are:

set debug isdn	Displays ISDN debugging information on the console.
set debug isdn D0	Displays the status of a single BRI.
set debug isdn-d	Displays ISDN frame debugging information on the console.
set debug isdn-d D0	Displays ISDN frame debugging for a single BRI.
set debug termination	Displays detailed port termination information.
set debug off	Clears all debug settings—except ISDN debug settings for a specific D channel—currently active on the PortMaster.

The following is example output from the **set debug isdn d0** command:

```
Command> set debug isdn d0
Enabling isdn tracing d0

isdn_dial; S1 CRN7770
isdn_dodial S1 (0:1) Sending Call Request - 7770
0: Received Call Sent
07 00 01 80
S1 (0:1) DISCONNECT Unassigned Number
S1 (0:1) CALL_CLEAR
S1: Redialing at alternate 56Kbps rate
isdn_dodial S1 (0:1) Sending Call Request - 7770
0: Received Call Sent
07 00 01 80
S1 (0:1) DISCONNECT Unassigned Number
S1 (0:1) CALL_CLEAR
```

To disable ISDN debugging, issue the command again:

```
Command> set debug isdn d0
Disabling isdn tracing d0
```

By using the D0 keyword, you can specify a BRI line to debug:

```
Command> set debug isdn-d d0

Enabling isdn  D tracing d0
D0: send 00 f3 01 03
D0: recv 00 f3 01 03
D0: send 00 f1 01 0f
D0: recv 00 f1 01 0b
```

Solving Frame Relay Problems 6

Use Table 6-1 to identify and diagnose common Frame Relay problems.

Table 6-1 Common Frame Relay Problems

Problem	Possible Cause	Possible Solution
The Frame Relay connection is not establishing.	• Misconfiguration. • Incorrect data link connection identifiers (DLCIs).	See "Preliminary Frame Relay Troubleshooting" on page 6-2. See "Diagnosing Frame Relay Problems with the DLCI List" on page 6-5.
The **traceroute** command reaches its target but **ping** does not (or vice versa).	Incorrect routing.	Use the **show routes to-dest** command to determine the routing (page 6-3). This is a common routing problem over Frame Relay connections.
The **show** *W1* command shows that the Frame Relay port does not have an ESTABLISHED status.	The PortMaster detects LMI packets being sent but not receiving any from the telephone company switch.	See "Diagnosing an Inactive Frame Relay Connection" on page 6-8.
The Frame Relay port has an ESTABLISHED status, but the PortMaster cannot ping another node on the Frame Relay cloud.	• Misconfigured port. • Misconfigured signaling type. • Routing problem. • Incorrect gateway.	See "Determining Why You Cannot Ping Other Frame Relay Nodes" on page 6-10.

Table 6-1 Common Frame Relay Problems *(Continued)*

Problem	Possible Cause	Possible Solution
The PortMaster cannot detect IPX over the Frame Relay connection.	Incorrect routing table flag.	See "IPX and Frame Relay" on page 6-11.
You need to break a Frame Relay connection.		See "Diagnosing Subinterface Problems" on page 6-12.
Problems with Frame Relay subinterfaces.	• Incorrect DLCIs. • LMI or Annex-D packets not being sent or received. • Misconfigured Cisco router at the remote end.	See "Diagnosing Subinterface Problems" on page 6-12.

Preliminary Frame Relay Troubleshooting

If you are having trouble with a Frame Relay connection, do the following:

1. **Wait a few moments.**

   The process of establishing a Frame Relay link, learning the DLCI list, and learning the IP address through Inverse ARP can sometimes take a few moments.

2. **Use the** show *W1* **command on the Frame Relay port to check the following:**

   – Verify that the port is configured correctly (the IP address is correct, DLCIs are correct, and the protocol is set for Frame Relay).

   – Verify that error counters are 0 except for abort errors. If your counters are nonzero, there might be a problem external to the PortMaster.

   For information about configuring a PortMaster for Frame Relay, see the *PortMaster Configuration Guide*.

3. **Verify that you are using the correct cables and that they are attached securely to the correct PortMaster port.**

Not all WAN ports are capable of the same speeds. On an IRX-114 ports S1 and S3 can support up to T1/E1 speeds, while ports S2 and S4 can support only speeds up to 64Kbps.

4. **On the IRX and PortMaster 2R, verify the following:**
   - The DIP switch setting corresponds to the cable type you are using.
   - The PortMaster is plugged into the correct interface on your CSU/DSU.
5. **Verify that the CSU/DSU is providing the clock signal to the PortMaster.**

   The CSU/DSU can generate the clock signal or receive it from the carrier.
6. **Verify that the CSU/DSU is configured properly.**
7. **Monitor the Local Management Interface (LMI) or Annex-D keepalive packets.**

   See "Monitoring LMI or Annex-D Packets" on page 6-4.
8. **If you have a Cisco router on the other end of the Frame Relay connection, verify that the following has been done:**
   - The Cisco router is set for Internet Engineering Task Force (IETF) encapsulation on the serial interface. Use the following Cisco IOS interface configuration command on the Cisco router to do so:

     ```
     encapsulation frame-relay ietf
     ```
   - The Cisco destination protocol address is mapped to the PortMaster DLCI. To do so, use the **frame-relay map** interface configuration command with the **ietf** keyword on the Cisco router.

Diagnosing Frame Relay Routing Problems

Because **traceroute** (UDP) takes its source address from the outbound interface and **ping** (ICMP) takes its source address from the Ether0 interface, routing can become confused. If either **traceroute** or **ping** reaches its target and the other does not, use the **show route-to-dest command** to determine if the outbound interface address and the Ether0 address are being routed differently. This is a common routing problem over Frame Relay connections.

For more information about this command, see "Finding a Particular Route" on page 3-22, or the *PortMaster Command Line Reference*.

Monitoring LMI or Annex-D Packets

The output from the **set debug 0x51** command shows LMI or Annex-D packets being sent and received. Three successful exchanges of packets (sent and received) are required for a PortMaster to establish a Frame Relay connection.

To check packet transmissions, do the following:

1. **Make a note of the current keepalive timer setting. Then change the keepalive timer to once per second to speed up the troubleshooting process:**

   – Use the following command for LMI packets:

   ```
   Command> set w1 lmi 1
   LMI keepalive timer for W1 changed from 10 to 1
   ```

   – Use the following command for Annex-D packets:

   ```
   Command> set w1 annex-d 1
   ANNEX-D keepalive timer for W1 changed from 10 to 1
   ```

2. **Set the administrative console and the debug value:**

   ```
   Command> set console
   Setting CONSOLE to admin session

   Command> set debug 0x51
   Setting debug value to 0x51
   ```

3. **Check the debug output:**

   The following is sample output from a successful LMI packet exchange:

   ```
   (W1) LMI: Sending Sequence Exchange - Sequence 174
   (W1) LMI: Received Sequence Exchange - Sequence 173
   (W1) LMI: Sending Sequence Exchange - Sequence 175
   (W1) LMI: Received Sequence Exchange - Sequence 174
   (W1) LMI: Sending Full Status Enquiry - Sequence 176
   (W1) LMI: Received Full Status - Sequence 175
   DLCI List: 16

   (W1) LMI: Sending Sequence Exchange - Sequence 177
   (W1) LMI: Received Sequence Exchange - Sequence 176
   (W1) LMI: Sending Sequence Exchange - Sequence 178
   (W1) LMI: Received Sequence Exchange - Sequence 177
   ```

If you see only "Received Sequence Exchange" messages, the PortMaster is receiving packets from the remote end of the connection, but is unable to respond. The source of the problem is likely to be a misconfigured port, or a problem with the CSU/DSU. Use the **show W1** command to verify that the modem status is DCD+ CTS+, and that the clock speed is correct. See the *PortMaster Command Line Reference* for more information about the **show W1** command.

If you see only "Sending Sequence Exchange" messages, the PortMaster is sending packets to the remote end of the connection, but is not receiving a response. The source of the problem is likely to be with the remote end of the connection.

4. **Turn off debugging:**

```
Command> reset console
Console RESET

Command> set debug off
```

5. **Reset the keepalive timer interval to 10 seconds, or to the setting you noted in Step 1.**

   The 10-second setting lessens traffic for other users of the frame switch at the telephone company:

```
Command> set w1 lmi 10

Command> set w1 annex-d 10
```

Diagnosing Frame Relay Problems with the DLCI List

Use the DLCI list to help you diagnose problems with a Frame Relay connection:

- Compare the DLCI numbers given to you by the telephone company with the DLCI list that is actually in use.
- Determine if the DLCIs and permanent virtual circuits (PVCs) have been associated with one another correctly. The list shows you the DLCI numbers for all PVCs except your own.
- Verify whether the telephone company switch is sending DLCI information via LMI or Annex-D.

You can get a DLCI list from the telephone company, from **set debug 0x51** output, or from **show arp** *Interface* output.

Getting the DLCI List from the Telephone Company

Because Frame Relay terminology can be confusing, you can easily get the wrong DLCI numbers. Confirm with the telephone company that you have the correct DLCI numbers for each end.

If you are using static DLCIs, swap the DLCIs used at either end of the connection to see if this establishes a connection.

For example, if you are using DLCI 16 on the local router with an IP address of 192.168.20.2, and DLCI 17 on the remote router with an IP address of 148.168.65.34, do the following:

1. **Reconfigure the local router to use DLCI 17:**

   ```
   Command> set W1 dlcilist 17:192.168.20.2

   Command> reset W1
   ```

2. **Reconfigure the remote router to use DLCI 16:**

   ```
   Command> set W1 dlcilist 16:148.168.65.34

   Command> reset W1
   ```

Getting the DLCI List from set debug 0x51 Output

To get the DLCI list from **set debug 0x51** output, do the following:

1. **Set the administrative console and the debug value:**

   ```
   Command> set console
   Setting CONSOLE to admin session

   Command> set debug 0x51
   Setting debug value to 0x51
   ```

2. **Check the debug output.**

   After approximately six exchanges, the Frame Relay switch returns all the DLCI numbers programmed into it.

The following sample output illustrates LMI packet exchange. The DLCI number is 16:

```
(W1) LMI: Sending Sequence Exchange -Sequence 174
(W1) LMI: Received Sequence Exchange -Sequence 173
(W1) LMI: Sending Sequence Exchange -Sequence 175
(W1) LMI: Received Sequence Exchange -Sequence 174
(W1) LMI: Sending Full Status Enquiry -Sequence 176
(W1) LMI: Received Full Status - Sequence 175
DLCI List: 16
(W1) LMI: Sending Sequence Exchange -Sequence 177
(W1) LMI: Received Sequence Exchange -Sequence 176
(W1) LMI: Sending Sequence Exchange -Sequence 178
(W1) LMI: Received Sequence Exchange -Sequence 177
```

3. **Turn off debugging:**

```
Command> set debug off

Command> reset console
Console RESET
```

Getting the DLCI List with show arp

This command shows the static or dynamic DLCI numbers associated with their IP addresses. The DLCIs in the following example are **18**, **19** and **17**. The **frm1** and **frm4** keywords identify Frame Relay interfaces.

```
Command> show arp frm1
162.154.110.227 at 04:21  (18)
162.154.110.228 at 04:31  (19)


Command> show arp frm4
162.154.110.234 at 04:11  (17)
```

Diagnosing Frame Relay Problems with ifconfig

To verify that Frame Relay interfaces are operational, use the **ifconfig** command. The following example shows that the Frame Relay interfaces **frm1** and **frm4** are both operational:

```
Command> ifconfig

ether0: flags=1106<IP_UP,IPX_UP,BROADCAST,PRIVATE,OSPF>
inet 162.154.110.5 netmask fffffffe0 broadcast 162.154.110.31
area 0.0.0.0 ospf-state DR
ipxnet 95C66E00 ipxframe ETHERNET_802.2 mtu 1500

frm1: flags=1814<IP_UP,IPX_UP,FRAME_RELAY>
inet 162.154.110.225 netmask fffffff8
ipxnet 95C66EE0 mtu 1500

frm4: flags=198c<IP_UP,IPX_UP,FRAME_RELAY,PRIVATE,COMPRESS>
inet 162.154.110.233 netmask fffffffc
ipxnet 95C66EE8 mtu 1500
```

Diagnosing an Inactive Frame Relay Connection

If **show** *W1* command output does not show a status of ESTABLISHED for the Frame Relay port, the connection is not active. (See "Displaying Port Errors and Status" on page 1-2, and the *PortMaster Command Line Reference* for information on the **show** *W1* command.)

Do the following to set up debugging on the Frame Relay port:

1. **Set the polling interval for the keepalive timer to once per second to speed up the troubleshooting process:**

   – Use the following command for LMI packets:

   ```
   Command> set w1 lmi 1
   LMI keepalive timer for W1 changed from 10 to 1
   ```

   – Use the following command for Annex-D packets:

   ```
   Command> set w1 annex-d 1
   ANNEX-D keepalive timer for W1 changed from 10 to 1
   ```

2. Set the administrative console and the debug value:

```
Command> set console
Setting CONSOLE to admin session

Command> set debug 0x51
Setting debug value to 0x51
```

3. Check the debug output

The output allows you to monitor LMI activity. If the PortMaster can detect that LMI packets are being sent but is not receiving any from the telephone company switch, the output looks like the following example:

```
Enabling port S1
(S1) LMI: Sending Full Status Enquiry - Sequence 2
(S1) LMI: Sending Full Status Enquiry - Sequence 3
(S1) LMI: Sending Full Status Enquiry - Sequence 4
```

4. If the PortMaster is detecting, but not receiving, LMI packets, verify that the PortMaster can send and receive data.

Put the CSU/DSU into a local loopback to cause each packet sent to the CSU/DSU to be looped back to the Frame Relay WAN port. This configuration is for testing purposes only; the line will not function while the CSU/DSU is in a local loopback.

5. Look for the message "LMI: Apparent Loop."

If you see the message, the following is true:

- The WAN port on the PortMaster is sending and receiving data.
- The cable and connectors between the PortMaster and the CSU/DSU are functional.
- The DTE port on the CSU/DSU is functional.
- The PortMaster is functioning properly.

6. If you do not see the "LMI: Apparent Loop" message, do the following:

a. If you are using an IRX, PortMaster 2R, or PortMaster 2ER check that the RS-232-V.35 DIP switch (located next to the WAN port) is set correctly.

b. Verify that all cables are securely connected and that interface pinouts match the cable in points and directions. See the cable specifications in the hardware installation guide that came with your PortMaster.

c. Verify that the cable that came with the unit is attached to the PortMaster.

d. Replace hardware such as cables, CSU/DSU, and so on, with hardware you know is working correctly.

e. Check the ComOS release version. If a ComOS release prior to 3.7 is in use, upgrade to the current ComOS version. See the downloading instructions at **http://www.livingston.com.**

7. **If you get apparent loops and the port status is not ESTABLISHED, do the following:**

   a. Check that the CSU/DSU is set for external clocking. The telephone company provides the clock signal. You should also verify your CSU/DSU settings with the manufacturer.

   b. Have the telephone company test the line, and ask for a printed copy of the test results.

Determining Why You Cannot Ping Other Frame Relay Nodes

If the **show** *W1* command shows a state of ESTABLISHED but you still cannot ping other nodes on the Frame Relay cloud, you might have a connectivity problem. Use the following steps to determine the cause of the problem:

1. **Double-check the configuration for the port.**

   a. Make sure the same network number is in use for the entire cloud.

   b. Verify that you have the proper netmask on the interface.

2. **Make sure you have the right signaling type (either LMI or Annex-D).**

   Reset the port after each setting.

3. **Use the** traceroute **command as follows.**

   a. Trace the route from your workstation to a router in the Frame Relay cloud.

   b. Trace the route from the router in the cloud to your workstation.

   c. Check for a gap in the list of router addresses displayed by the two traceroute commands.

   See "Tracing a Route" on page 3-21 for instructions on using **traceroute**.

4. **Make sure the gateway is set to the next upstream router.**

The gateway should never be more than one hop away.

5. **Use** ping **again.**

   If you can ping the closest upstream link but nothing further, you might have a routing problem. See Chapter 3, "Solving Networking Problems."

IPX and Frame Relay

If you cannot detect IPX over a Frame Relay link or cannot get a list of NetWare servers via SLIST or NLIST, do the following to diagnose the problem:

1. **List the IPX routing table to see a list of IPX routes and where they are being routed.**

```
Command> show ipxroute
Network     Gateway                 Flag    Met     Ticks    Interface
--------    ---------------         ----    ----    ------   ---------
00000000    00000008:00C005001C19   NS        1       0      ether0
00000008    00000008:00C005001C19   NLC       1       1      ether0
0A000100    0A000100:00C005001C19   NLC       1       1      ether0
```

   See the *PortMaster Command Line Reference* for an explanation of **show ipxroute** command output.

2. **Check for an NS flag in the first entry.**

   This flag indicates a static network route. If you see this flag, do the following:

   a. Reset your IPX gateway:

```
Command> set ipxgateway Ipxaddress
IPX gateway reset
```

   b. Reboot the PortMaster to clear the routing table:

```
Command> save all
Command> reboot
```

   c. Repeat Step 1.

      If no NS flag appears, the PortMaster is configured correctly.

Note – The ComOS requires that all IPX networks be known. The default network is not supported.

3. **Show the Service Advertising Protocol (SAP) table and check for entries from other servers and routers.**

   Use the **Interface** column to identify the interface through which the SAP packet entered the PortMaster and determine the packet's source—the Frame Relay network, the Ethernet, or the PortMaster itself.

```
Command> show sap
Server         Svc     Network       Host             Sock    Hops    Interface
--------       ---     ----------    -------------    ----   ------   ----------
tie            5F2     000000AA:     00C0050101B2:    066B      1      frm1
ywing          5F2     00000008:     00C0050161A7:    066B      1      ether0
xwing          5F2     00000008:     00C00501200E:    066B      1      ether0
falcon         5F2     000000AA:     00C005021D12:    066B      1      frm1
calamari       5F2     00000008:     00C005001C19:    066B      1      Internal
```

   If you see SAPs from the other side, your PortMaster is configured correctly.

4. **Set up IPX packet traces on both ends of the Frame Relay connection and observe exactly what the packets are doing.**

   See "Tracing IPX Packets" on page 3-16 for instructions.

Diagnosing Subinterface Problems

Packets received on a subinterface can be identified as belonging to that subinterface only if the DLCI is properly entered in the DLCI table for that location. If you are having problems, do the following:

1. **Wait a few moments.**

   Subinterfaces come up after the primary interface. This process can take a few moments.

2. **Use the** ifconfig **command to verify that the primary interface and the subinterface are functioning.**

   In the following example, both **frm1** (the primary interface) and **frm3** (the subinterface) are functioning as indicated by the IP_UP and FRAME_RELAY flags:

```
Command> ifconfig

ether0: flags=6<IP_UP,IPX_DOWN,BROADCAST,LISTEN>
inet 149.198.64.250 netmask ffffff00 broadcast 149.198.64.255 mtu 1500

ether1: flags=12<IP_DOWN,IPX_DOWN,BROADCAST>
inet 0.0.0.0 netmask ffffff00 broadcast 0.0.0.255 mtu 1500

frm1: flags=814<IP_UP,IPX_DOWN,FRAME_RELAY>
inet 192.168.152.17 netmask fffffff8 mtu 1500

frm3: flags=98c<IP_UP,IPX_DOWN,FRAME_RELAY,PRIVATE,COMPRESS>
inet 192.168.152.33 netmask fffffffc mtu 1500
```

3. **Use the** show *S0* **command to check the errors on the port being used by the primary interface.**

   Abort, cyclic redundancy check (CRC), or frame errors indicate a possible problem with the primary interface, which must be resolved before you can troubleshoot the subinterface. See "Displaying Port Errors and Status" on page 1-2 for more information.

   In the following example, port S1 shows no errors.

```
Command> show s1

---------------------- Current Status - Port S1 --------------------------

Status: ESTABLISHED
Input: 681                          Abort Errors: 0
Output: 1408                           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 56000                    Ext Clock
Modem Control: off                           off
Local Address: 192.168.152.17             192.168.152.17
Netmask: 255.255.255.248             255.255.255.248
Interface: frm1 (FRM,Routing)          (FRM,Routing)
Mtu: 1500                           0
Dial Group: 10
LMI Poll Int: 10 (seconds)

IP DLCI's:  DLCI    Address
-----  ------------
16      192.168.152.18


Sub-Interface:
```

4. **Use the** show location **command to verify the following:**

   – You have entered the correct DLCIs for the subinterface. If you enter the wrong DLCI for the subinterface while LMI or Annex-D is in use, the DLCI for the subinterface is applied to the primary interface.

   – The protocol is set for **Frame Relay**, and the type is **Sub-Interface**.

   – No DLCIs are missing.

   In the following example, the DLCI for the subinterface is 17:

```
Command> show location sub1
Location: sub1                          Type: Sub-Interface
IP Address: 192.168.152.33           Netmask: 255.255.255.252
Protocol: Frame Relay               Options: Quiet, VJ-Comp
Group: 10                              Mtu: 1500

IP DLCI's:  DLCI    Address
-----  ------------
17      192.168.152.34
```

5. **Check the packet count and errors on the subinterface with the** show netstat **command:**

```
Command> show netstat
Name        Ipkts      Ierrs     Opkts     Oerrs     Collis    Resets    Queue
ether0        72         0         39        0         0         0         0
ether1         0         0         0         0         0         0         0
frm1           0         0         1         0         0         0         0
frm3           0         0         0         0         0         0         0
```

6. **Verify that each DLCI has an associated IP address.**

   Replace *Interface* with the name of the Frame Relay interface. A list of interfaces can be shown with the **ifconfig** command (see Step 2). Verify that each DLCI has an associated IP address.

   ```
   Command> show arp frm1
   162.154.110.227 at 04:21  (18)
   162.154.110.228 at 04:31  (19)


   Command> show arp frm4
   162.154.110.234 at 04:11  (17)
   ```

   See the *PortMaster Configuration Guide* for information about how to configure the DLCI list.

7. **Reset the port if you change the DLCI list.**

8. **Monitor the LMI or Annex-D keepalives.**

   This verifies that the DLCI you have entered are correct. See "Getting the DLCI List from set debug 0x51 Output" on page 6-6.

9. **If you have a Cisco router on the other end of your connection, verify that one of the following has been done:**

   – The Cisco router has been set for Internet Engineering Task Force (IETF) encapsulation on the serial interface. Use the following Cisco IOS interface configuration command on the Cisco router to do so:

   ```
   encapsulation frame-relay ietf
   ```

   – The Cisco destination protocol address is mapped to the PortMaster DLCI. To do so, use the **frame-relay map** interface configuration command with the **ietf** keyword on the Cisco router.

ISDN Cause Codes A

ISDN cause codes are standard messages that are received from networks conforming to the European Telecommunication Standards Institute (ETSI), ISDN2 and INS Net64 Japanese specifications.

The cause is divided into three fields:

- The most significant bit (bit 8) is always coded as 1.
- The class (bits 5 through 7) indicates the general nature of the event. The value within the class (bits 1 through 4) indicates the event.
- Classes and values are coded as shown in Table A-1 through Table A-7. Some cause elements might also include an optional diagnostic octet.

Table A-1 Class 000 and 001 (Normal Events) Cause Codes

	Bit			
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 0 0	0 0 0 1	81	1	**Unallocated (unassigned) number**. The ISDN number was presented in a valid format but is not currently assigned to any destination equipment.
0 0 0	0 0 1 0	82	2	**No route to specified transit network.** The ISDN exchange was requested to route the call through an unrecognized intermediate network.
0 0 0	0 0 1 1	83	3	**No route to destination.** The call was routed through a network that does not serve the destination address.
0 0 0	0 1 1 0	86	6	**Channel unacceptable.** The specified channel is unable to accept the connection due to poor line quality.

Table A-1 Class 000 and 001 (Normal Events) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 0 0	0 1 1 1	87	7	**Call awarded and delivered in an established channel**. The incoming call is being connected to an established channel.
0 0 1	0 0 0 0	90	16	**Normal clearing**. No action is required.
0 0 1	0 0 0 1	91	17	**User busy**. The called system has acknowledged the connection request but is unable to accept the call because the B channels are in use.
0 0 1	0 0 1 0	92	18	**No user responding**. The destination did not respond to the call, and the connection cannot be completed.
0 0 1	0 0 1 1	93	19	**No answer from user (user alerted)**. The destination has responded to a connection request but timed out before completing the connection. This code indicates a problem at the remote end.
0 0 1	0 1 0 1	95	21	**Call rejected**. The destination is capable of accepting the call (the remote end is not busy or incompatible with the local end) but rejected the call for some reason.
0 0 1	0 1 1 0	96	22	**Number changed**. The ISDN number used to set up the call is no longer assigned. An alternate address (if one is used) might be displayed in the message.
0 0 1	1 0 1 0	9A	26	**Nonselected user clearing**. The destination was capable of accepting the call but rejected it because the call was not awarded to the user.

Table A-1 Class 000 and 001 (Normal Events) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 0 1	1 0 1 1	9B	27	**Destination out of order**. The destination cannot be reached because the interface and signaling message are malfunctioning. This code indicates that equipment is offline.
0 0 1	1 1 0 0	9C	28	**Invalid number format**. The connection cannot be established because the destination address is in an unrecognized format or is incomplete.
0 0 1	1 1 0 1	9D	29	**Facility rejected**. The facility requested by the user cannot be provided by the network. This code might indicate a subscription problem.
0 0 1	1 1 1 0	9E	30	**Response to status enquiry**. This status message was generated in response to an earlier status enquiry message.
0 0 1	1 1 1 1	9F	31	**Normal, unspecified**. No action is required.

Table A-2 Class 010 (Network Congestion) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 1 0	0 0 1 0	A2	34	**No circuit/channel available**. A connection cannot be established because all appropriate channels are unavailable.
0 1 0	0 0 1 1	A3	35	**Call queued** (AT&T only).
0 1 0	0 1 1 0	A6	38	**Network out of order**. The network problem is expected to last a relatively long time, and an immediate reconnection attempt is likely to fail.

Table A-2 Class 010 (Network Congestion) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 1 0	1 0 0 1	A9	41	**Temporary failure**. The network problem is expected to be resolved shortly.
0 1 0	1 0 1 0	AA	42	**Switching equipment congestion**. The destination cannot be reached because the switching equipment is overloaded
0 1 0	1 0 1 1	AB	43	**Access information discarded**. The network cannot provide the requested access information.
0 1 0	1 1 0 0	AC	44	**Requested circuit or channel not available**. The remote equipment cannot provide the requested channel for an unknown reason.
0 1 0	1 1 1 1	AF	47	**Resources unavailable, unspecified**. The requested channel or service is unavailable for an unspecified reason.

Table A-3 Class 011 (Service or Option Not Available) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 1 1	0 0 0 1	B1	49	**Quality of service unavailable**. The requested quality of service cannot be provided by the network. This code indicates a possible subscription problem.
0 1 1	0 0 1 0	B2	50	**Requested facility not subscribed**. The requested supplementary service is available, but the requestor is not a subscriber.
0 1 1	0 1 0 0	B4	52	**Outgoing calls barred** (AT&T only).
0 1 1	0 1 1 0	B6	54	**Incoming calls barred**.

Table A-3 Class 011 (Service or Option Not Available) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
0 1 1	1 0 0 1	B9	57	**Bearer capability not authorized**. The user is requesting a bearer capability that he or she is not authorized to use.
0 1 1	1 0 1 0	BA	58	**Bearer capability not presently available**. The user is requesting a bearer capability that is normally available, but is not currently available due to either a network or a subscription problem.
0 1 1	1 1 1 1	BF	63	**Service or option not available, unspecified**. The network is unable to provide the requested service for an unspecified reason, possibly due to a subscription problem.

Table A-4 Class 100 (Service or Option Not Implemented) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 0 0	0 0 0 1	C1	65	**Bearer capability not implemented**. The requested bearer capability is not available on the network.
1 0 0	0 0 1 0	C2	66	**Channel type not implemented**. The requested channel type is not available on the network or the destination equipment.
1 0 0	0 1 0 1	C5	69	**Requested facility not implemented**. The requested facility is not available on the remote equipment.

Table A-4 Class 100 (Service or Option Not Implemented) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 0 0	0 1 1 0	C6	70	**Only restricted digital information bearer capability is available**. The network cannot provide unrestricted digital information bearer capability.
1 0 0	1 1 1 1	CF	79	**Service or option not implemented, unspecified**. The network is unable to provide the requested service for an unspecified reason, possibly due to a subscription problem.

Table A-5 Class 101 (Invalid Message) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 0 1	0 0 0 1	D1	81	**Invalid call reference value**. The remote equipment has received a call reference that is not being used by the user-network interface.
1 0 1	0 0 1 0	D2	82	**Identified channel does not exist**. The equipment receiving the call does not have the requested channel activated.
1 0 1	0 0 1 1	D3	83	**A suspended call exists, but this call identity does not**. The network received a call resume request that is already in use for a suspended call.
1 0 1	0 1 0 0	D4	84	**Call identity in use**. The network received a call resume request that is already in use for a suspended call.

Table A-5 Class 101 (Invalid Message) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 0 1	0 1 0 1	D5	85	**Invalid digit value for number**. OR **No call suspended**. The network received an unnecessary call resume request (no calls were suspended at the time of the request). Retrying the call might clear the problem.
1 0 1	0 1 1 0	D6	86	**Call having the requested call identity has been cleared**. The network received a call resume request indicating a suspended call that has been cleared or timed out.
1 0 1	1 0 0 0	D8	88	**Incompatible destination**. An attempt was made to connect to a non-ISDN device—for example, an analog telephone line.
1 0 1	1 0 1 1	DB	91	**Invalid transit network selection**. The ISDN exchange was requested to route the call through an unrecognized intermediate network.
1 0 1	1 1 1 1	DF	95	**Invalid message, unspecified**. This code most likely indicates D channel error. Contact your authorized telephone service provider if this error persists.

Table A-6 Class 110 (Protocol) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 1 0	0 0 0 0	E0	96	**Mandatory information element is missing**. This code most likely indicates a D channel error. Contact your authorized telephone service provider if this error persists.
1 1 0	0 0 0 1	E1	97	**Message type nonexistent or not implemented**. The message type received was either invalid or not implemented on the receiving device. This code indicates a problem with either the D channel or the configuration of the remote device.
1 1 0	0 0 1 0	E2	98	**Message not compatible with call state, or message type nonexistent or not implemented**. An invalid message was received and no standard cause applies. This code most likely indicates a D channel error. Contact your authorized telephone service provider if this error persists.
1 1 0	0 0 1 1	E3	99	**Information element does not exist or is not implemented**. An invalid message was received containing unrecognized information elements. This code most likely indicates a D channel error. Contact your authorized telephone service provider if this error persists.
1 1 0	0 1 0 0	E4	100	**Invalid information element contents**. This code indicates a D channel error. The remote equipment received a message containing an invalid information element.
1 1 0	0 1 0 1	E5	101	**Message not compatible with call state**. This code indicates a D channel error. The remote equipment received a message that did not correspond to the current call state.

Table A-6 Class 110 (Protocol) Cause Codes *(Continued)*

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 1 0	0 1 1 0	E6	102	**Recovery on timer expiry**. A timeout has initiated an error-handling procedure.
1 1 0	1 1 1 1	EF	111	**Protocol error, unspecified**. An unspecified D channel error has occurred.

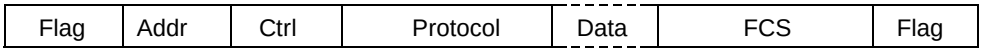
Table A-7 Class 110 (Protocol) Cause Codes

Bit				
7 6 5	**4 3 2 1**	**Hex**	**Value**	**Description**
1 1 1	1 1 1 1	FF	127	**Internetworking, unspecified**. This code might indicate an error. A network event has occurred resulting in certain unspecified actions.

PPP Packet Formats B

The following information describes the formats and configuration options for Point-to-Point Protocol (PPP). See "Debugging and Interpreting PPP Negotiation" on page 4-2 for information about displaying negotiation information that can be analyzed using the packet formats contained in this appendix, or by using the Decoder Ring located on the Lucent Remote Access website (**http://www.livingston.com**).

PPP Frame Format



All values shown in the fields are in hexadecimal format. Adjacent frames can be separated by a single flag. Address and control bytes are omitted in non-Link Control Protocol (LCP) frames if Address-and-Control-Field-Compression is negotiated.

If the first byte of the Protocol field is zero, it is omitted in non-LCP frames if Protocol-Field-Compression is negotiated. On asynchronous links, special characters—flags, escape characters, and control characters selected in the negotiated remote Async-Control-Character-Map—between the flags are replaced by an escape character (7D) and the original byte with bit 6 inverted (XOR'ed with 0x20).

Table B-1 shows values that can appear in the Protocol field of a PPP frame. The Network Control Protocol (NCP) value is used to establish a connection for the associated data transfer protocol. See RFC 1700, *Assigned Numbers*, for a complete list of protocol values.

Table B-1 Protocol Values

Protocol	Value	NCP Value
Internet Protocol (IP)	0021	8021
OSI Network Layer	0023	8023
DECnet Phase IV	0027	8027
AppleTalk	0029	8029
Novell IPX	002B	802B

Table B-1 Protocol Values *(Continued)*

Protocol	Value	NCP Value
Van Jacobson Compressed TCP/IP	002D	
Van Jacobson Uncompressed TCP/IP	002F	
Banyan VINES	0035	8035
Link Control Protocol (LCP)		C021
Password Authentication Protocol (PAP)		C023
Link Quality Monitoring (LQM)		C025
Challenge Handshake Authentication Protocol (CHAP)		C223

Formats for LCP Packets

LCP Packet Formats

Configure-Request

01	ID	Length	Configuration Options

Configure-Nak

03	ID	Length	Configuration Options

Terminate-Request

05	ID	Length	Data

Code-Reject

07	ID	Length	Rejected-Packet

Echo-Request

09	ID	Length	Magic-Number	Data

Discard-Request

0b	ID	Length	Magic Number	Data

Configure-Ack

02	ID	Length	Configuration Options

Configure-Reject

04	ID	Length	Configuration Options

Terminate-Ack

06	ID	Length	Data

Protocol-Reject

08	ID	Length	Rejected-Protocol	Rejected-Info

Echo-Reply

0a	ID	Length	Magic-Number	Data

LCP Configuration Options

Maximum Receive Unit (MRU)

01	04	MRU	Default is 1520 decimal

Authentication-Protocol

03	Length	Authentication	Protocol	Data	Default is no authentication
	04	c0	23		PAP
	05	c2	23	05	CHAP using MD5
	05	c2	23	80	MS-CHAP

Magic-Number

05	06	Magic-Number	Default is no magic number

Address-and-Control-Field-Compression

08	02	Default is no compression

Async-Control-Character-Map

02	06	Async-Map	Default is FFFFFFFF

Quality-Protocol

04	Length	Quality	Protocol	Data	Default is no LQM
	08	c0	25	Reporting-Period	

Protocol-Field-Compression

07	02	Default is no compression

IPCP Configuration Options

The IP Control Protocol (IPCP) is similar to LCP except that only codes 1 through 7 are used.

IP-Addresses

01	0a	Source-IP-Address	Deprecated
Destination-IP-Address			

IP-Address

03	06	IP-Address	No default

IP-Compression-Protocol

02	Length	Compression	Protocol	Data	Default is no compression
	06	00	2d	Max-Slot-ID	Comp-Slot-ID (Van Jacobson Compressed TCP/IP)

PAP Packet Formats

Authenticate-Request

01	ID	Length	IDLen	Peer-ID
PwLen	Password			

Authenticate-Nak

03	ID	Length	MsgLen	Message

Authenticate -Ack

02	ID	Length	MsgLen	Message

CHAP Packet Formats

Challenge

01	ID	Length	ValSize	Value
Name				

Success

03	ID	Length	Message

Response

02	ID	Length	ValSize	Value
Name				

Failure

04	ID	Length	Message

Formats for IPXCP Packets

This section illustrates the packet formats and configuration options of IPX Control Protocol (IPXCP) that are found in the IPX NCP layer during the PPP negotiation process. More information on this subject can be found in RFC 1552, *The PPP Internetwork Packet Exchange Control Protocol* (*IPXCP)*.

IPXCP Packet Formats

Configure-Request

01	ID	Length	Configuration Options

Configure-Ack

02	ID	Length	Configuration Options

Configure-Nak

01	ID	Length	Configuration Options

Configure-Reject

04	ID	Length	Configuration Options

Terminate-Request

05	ID	Length	Data

Terminate-Ack

05	ID	Length	Data

Code-Reject

06	ID	Length	Data

IPXCP Configuration Options

IPX-Network-Number

01	06	IPX-Network-Number

IPX-Node-Number

02	08	IPX-Node-Number

IPX-Compression-Protocol

03	Length	IPX-Compression-Protocol (2 bytes)

Data:

- 00 02 Telebit Compressed IPX
- 02 35 Shiva Compressed NCP/IPX

IPX-Routing-Protocol

04	Length	IPX-Routing-Protocol (2 bytes)

Data:

- 0 = No routing protocols
- 1 = RESERVED
- 2 = Novell RIP/SAP required
- 3 = Novell Netware Link Services Protocol (NLSP) required

IPX-Router-Name

05	Length	Name ...

IPX-Configuration-Complete

06	02

Formats for CCP Packets

The Compression Control Protocol (CCP) is similar to LCP with two additional codes.

CCP Packet Formats

Reset-Request

14	ID	Length	Configuration Options...

Reset-Ack

15	ID	Length	Configuration Options...

CCP Configuration Options

Type	Length	Values

Compression types:

- 0x0 Organization Unique Identifier (OUI)
- 0x1 Predictor type 1
- 0x2 Predictor type 2
- 0x3 Puddle Jumper
- 0x10 Hewlett-Packard packet-by-packet compression (PPC)
- 0x11 Stac Electronics LZS

- 0x12 Microsoft PPC
- 0x13 Gandalf FZA
- 0x14 V.42bis compression
- 0x15 BSD LZW compression

Note – PortMaster products supporting compression support only Stac LZS. Packets compressed with other compression types are dropped by the PortMaster.

Termination Causes C

Use either of the following debug commands to help you view termination causes. Remember to turn off debug routines with **set debug off** when you are finished.

- **set debug 0x54** output—when this debug command is active, you can see the last two termination causes on a particular port by using the **show** *S0* command:

```
Command> set debug 0x54
Command> show S17
.
.
.
[omitted]
Session termination history:
0 min - Cause Unknown
```

- **set debug termination** output—when this debug command is active and the console is set, termination causes are sent to the console as they occur. Termination causes are also sent to RADIUS accounting logs.

```
Command> set console
Command> set debug termination
Command> [097:18:40:03:20] S17: Session Terminated - Cause Unknown
```

The following termination causes relate to ISDN, asynchronous, and synchronous connections:

Termination Cause	Description
Admin Reset	A **reset S0** command was issued on that port.
Callback—User Requested	The incoming call is for a dialback user, the PortMaster terminated the connection to call back the user.
Host Request	The user requested to reset the port.
Host Request (PMD)	The user requested to reset the port using the **in.pmd** service.

Termination Cause	Description
Idle Timeout	The user was disconnected by the idle timer.
Login Timeout	The user did not respond to the **login:** prompt in the time specified by the login timer.
Lost Carrier	The session terminated when the local modem dropped the Data Carrier Detect (DCD) signal for some reason. For example: • The remote user or modem hung up the telephone. No problem exists. • The line was dropped or received interference too severe for the modem to recover from.
Lost Service—Interface Down	The logical interface is down.
Lost Service—Interface Error	An unspecified interface error occurred.
Lost Service—LMI	The PortMaster lost connectivity to the Frame Relay switch.
Lost Service—No Netbufs	The PortMaster has run out of network buffers. Contact Lucent Remote Access Technical Support.
NAS Request—Modem Config Complete	The PortMaster 3 modem initialization is complete.
NAS Request—PPP Maximum Retransmissions	The PortMaster sent a specified number of PPP packets with no response, and has determined that the remote PPP stack has disappeared.
Port Error—Exceeded LAPM retrans limit	The PortMaster exceeded the Link Access Procedure for Modems (LAPM) retransmission limit.
Port Error—Exceeded MNP retrans limit	The PortMaster either exceeded the Microcom Networking protocol (MNP) retransmission limit (12 retries) or the idle timer expired waiting for Link Request (1 second) or Link Acknowledge (5 seconds).
Port Error—PPP could not send	The PortMaster was trying to send PPP and could not for an unknown reason.

Termination Cause	Description
Port Error—PPP loop detected	The PortMaster is receiving its own data, possibly due to a CSU/DSU malfunction.
Port Error—Spurious Interrupts	A Clear To Send (CTS), Data Set Ready (DSR) and/or Data Carrier Detect (DCD) signal was toggling more than 10,000 times in a 1-second window, so the PortMaster reset the port.
Port Error—Wrong Type	The port is set for network connections only, and a login user attempted to connect.
Service Unavailable—Access Denied	A login user attempted to access a host, or service was denied by an access filter.
Service Unavailable—Auth Failed	The user entered an incorrect ID or password.
Service Unavailable—Device Unavailable	An outbound connection could not connect because the host did not reply.
Service Unavailable—Dial Script Failed	The dial script on an outbound connection failed.
Service Unavailable—Failed to detect V.42 Remote	The remote end of a connection does not support V.42bis compression.
Service Unavailable—Host Unavailable	An inbound connection could not connect because the host did not reply.
Service Unavailable—Master Out of Sync	A master point-to-point (PTP) list is not synchronized with slave PortMaster products in a Multichassis PPP bundle.
Service Unavailable—Out of Assigned Addresses	The assigned addresses pool has fewer addresses than available ports because of a misconfiguration of the address pool.
Service Unavailable—PPP Auth Failed	The user entered an incorrect password.
Service Unavailable—PPP CHAP Auth Failed	The user entered an incorrect CHAP password or ID.
Service Unavailable—PPP No Protocol	A protocol could not be negotiated.

Termination Cause	Description
Service Unavailable—PPP Outbound PAP Auth Failed	A user dialed out with Password Authentication Protocol (PAP) and received a negative acknowledgment (NAK) from the remote end.
Service Unavailable—PPP PAP Auth Failed	The user entered an incorrect PAP password or ID.
Session Timeout	The user was disconnected by the session timer.
User Error—Bad parameter in MNP lr neg	The PortMaster received a incorrect parameter in the link request negotiation.
User Error—Failed to complete V.42 neg	V.42 negotiation failed to establish MNP or LAPM for a reason other than open distributed processing (ODP), automatic data processing (ADP), exchange ID (XID), or set asynchronous balanced mode extended (SABME) timeout.
User Error—Local link rates do not match remote	The rate negotiated for the downstream connection is smaller than the minimum connection speed parameter specified by the host.
User Error—Non LR received in MNP init	The PortMaster received a zero-length link rate.
User Error—LAPM negotiation timeout	The timer has expired while trying to detect an XID or SABME command. The timeout value is 30 seconds for K56Flex connections, and 5 seconds otherwise.
User Error—PPP NCP active to reply	The PortMaster received a reply during an active PPP session.
User Error—PPP NCP active to request	The PortMaster received a request for a connection during an active PPP session.
User Error—PPP LCP Protocol Reject	The connection was refused at the Link Control Protocol (LCP) layer.
User Request—Admin Quit	The user typed **exit** at the command prompt.

Termination Cause	Description
User Request—PPP TERM ACK	The PortMaster sent a session termination request (TERM_REQ), and the remote end replied with a termination acknowledgment (TERM_ACK).
User Request—PPP TERM REQ	The remote end sent a TERM_REQ.
User Request—Normal	A normal disconnection occurred.
User Request—Modem Disconnect	On a PortMaster with external modems, DCD was dropped.
User Request—Normal LAPM Disconnect	The LAPM on the remote modem requested a disconnect.
User Request—Call Circuit Closed	The telephone company dropped the digital signal level 0 (DS0) circuit that user was on for one of the following reasons: • Remote modem in an on-hook condition • Three invalid login attempts • Sudden line termination • Remote modem turned off

Glossary

A

abort error

An error indicating an attempted and failed connection.

acceptance policy

A set of rules that determine the path and route information the PortMaster accepts from a BGP peer for further processing. See also **policy**.

address

A number used to identify a computer or other device on a network or internetwork. See also **IP address**; **MAC address**.

address resolution

A method for translating one type of address into another—for example, an IP address into a media access control (MAC) address.

Address Resolution Protocol

See **ARP**.

adjacency

A relationship between two routers on the same physical network or between the endpoints of a virtual link that controls the distribution of routing protocol packets by limiting their exchange to those routers or endpoints.

advertisement policy

A set of rules that determine the path and route information the PortMaster advertises to a BGP peer. See also **policy**.

agent

A software program installed in a managed network device. An agent stores management information and responds to the manager's request for this information.

aggregation

The process of combining multiple prefixes from one or several routes so that a single prefix and route can be advertised. Route aggregation reduces the amount of information that a device running BGP must store and exchange with its BGP peers. See also **summarization**.

Annex-D

The ANSI T1.617 Frame Relay Annex-D version of the Local Management Interface (LMI) protocol. The Annex-D protocol has a more robust feature set than the proprietary Cisco/Stratacom LMI, but was developed later. Recent versions of the PortMaster software support either type of LMI. Earlier versions supported only the Cisco/Stratacom version. See also **LMI**.

area

In OSPF, a contiguous collection of networks and hosts. Each area runs a separate copy of the shortest-path-first (SPF) algorithm and has its own topological database.

area border router

In OSPF, a router that attaches to the backbone and one other area. An area border router runs separate copies of the shortest-path-first (SPF) algorithm for each area it attaches to. Area border routers condense the topological information of their attached areas and distribute it over the backbone to the other areas.

ARP

Address Resolution Protocol. A protocol that discovers the unique physical hardware address of a node or a LAN from its IP address. When an ARP request is sent to the network, naming the IP address, the machine with that IP address returns its physical address so that it can receive the transmission.

ASCII

American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.

autonomous system

A collection of routers under the control of a single technical administration, using one or more Interior Gateway Protocols (IGPs)—such as OSPF—to route packets within itself, and an Exterior Gateway Protocol (EGP)—such as BGP—to route packets to other autonomous systems. An autonomous system typically uses a common BGP policy and always presents a consistent view of network reachability to other autonomous systems.

autonomous system border router

In OSPF, a router that exchanges information with routers from other autonomous systems. Autonomous system border routers are also used to import routing information about RIP, direct, or static routes from non-OSPF attached interfaces.

autonomous system path list

In BGP, the list of autonomous systems that a packet must traverse to reach a given set of IP address destinations located within a single autonomous system destination. The list can consist of **sequences**, which are series of autonomous systems that must be traversed in the order specified, and **sets**, which are collections of autonomous systems one of more of which must be traversed in any order to the destination.

For example, an autonomous system path list might consist of *Sequence 1, 2, 3, Set 4, 5, Sequence 6, 7*. This list indicates that a packet traverses autonomous systems 1, 2, and 3 in order, then one or both of autonomous systems 4 and 5 in any order, and finally autonomous systems 6 and 7 in order. Autonomous system 7 is the destination autonomous system.

B

backbone

A network topology consisting of a single length of cable with multiple network connection points.

backbone area

In OSPF, an area consisting of networks and routers not contained in any area and autonomous system border routers. The backbone area is responsible for distributing routing information between areas. This backbone area must be contiguous either physically or through a virtual link. The number reserved for the backbone area is 0.0.0.0.

backbone router

In OSPF, a router that has an interface into the backbone area by a direct attachment or a virtual link.

Basic Rate Interface

See **BRI**.

baud

The number of discrete signal events per second occurring on a communications channel. Although not technically accurate, baud is commonly used to mean bit rate.

B channel

Bearer channel. A 64Kbps synchronous channel that is part of an ISDN Basic Rate Interface (BRI).

BGP

Border Gateway Protocol. A routing protocol for exchanging network reachability information among autonomous systems. A routing device can use this information to construct a "map" of autonomous system connectivity. Version 4 of this protocol (BGP-4), which supports classless interdomain routing (CIDR) and route aggregation, is the predominant routing protocol used to propagate routes between autonomous systems on the Internet. BGP uses TCP as its transport protocol.

BGP-4

Version 4 of BGP. See also **BGP**.

BONDING

Bandwidth on Demand Interoperability Group. A method for combining two B channels into a single 128Kbps channel.

booting

The process in which a device obtains information and begins to process it to attain a state of normal operation.

Border Gateway Protocol

See **BGP**.

bps

Bits per second. A unit for measuring the data rate.

BRI

Basic Rate Interface. An ISDN interface that consists of two 64Kbps B channels for voice or data and one 16Kbps D channel for signaling. Compare **PRI**.

broadcast address

A special address reserved for sending a message to all stations. Generally, a broadcast address is a media access control (MAC) destination address of all 1s (ones).

broadcast packets

Packets that are sent to all network nodes.

C

callback

A port configuration allowing the PortMaster to call back dial-in users before providing access. Callback provides an extra layer of security and can simplify telephone charges.

CCITT

Consultative Committee for International Telegraph and Telephone. International organization formerly responsible for the development of communications standards. Now called the ITU-T. See also **ITU-T**.

CD

Carrier Detect. A signal that indicates whether an interface is active. Also, a signal generated by a modem indicating that a call has been connected.

Challenge Handshake Authentication Protocol

See **CHAP**.

channelized T1

An access link operating at 1.544Mbps that is subdivided into 24 channels of 56Kbps each for dial-in use.

channel service unit

See **CSU**.

CHAP

Challenge Handshake Authentication Protocol. A Point-to-Point Protocol (PPP) authentication method for identifying a dial-in user. CHAP does not itself prevent unauthorized access, it merely identifies the remote end. See also **PAP**.

CIDR

Classless interdomain routing. A technique supported by BGP-4 that eliminates the necessity for network address classes by explicitly advertising the length (netmask) associated with each prefix.

CIR

Committed information rate. The minimum bandwidth guaranteed to be available if required on a virtual circuit. This value is also known as *guaranteed bandwidth*.

classless interdomain routing

See **CIDR**.

client/server environment

An environment where a computer system or process requests a service from another computer system. For example, a workstation can request services from a file server across a network.

cluster

A group of internal BGP peers that share a common set of route reflectors. See also **cluster ID**; **route reflection**; **route reflector**. Compare **confederation**.

cluster ID

An identifier, in dotted decimal format, that uniquely identifies a BGP route reflection cluster within an autonomous system. All route reflectors within the cluster must be configured with the same cluster ID. Internal peers that are not reflectors within the cluster must not be configured with a cluster ID. The cluster ID is typically set to the BGP router ID of one of the route reflectors within the cluster. See also **cluster**; **route reflection**; **route reflector**.

CMAS

Confederation member autonomous system. A subdivision of an autonomous system that is recognized only by other peers within the confederation and not by peers external to the confederation. Within the confederation, each BGP peer treats only the peers in its own CMAS as internal peers. Peers in different CMASs are treated as external peers.

committed information rate

See **CIR**.

community

A label that identifies a group of BGP destinations for the purpose of policy enforcement. Assembling destinations into identifiable "communities" lets BGP peers base policy decisions on the identity of the group rather than on individual destinations. The community identifier, which consists either of one 32-bit value or two 16-bit values, is advertised in update messages between BGP peers.

community string

A character string assigned to a Simple Network Management Protocol (SNMP) agent to restrict read and write access to the SNMP variables.

ComOS

The operating system for PortMaster communications servers, routers, and access servers.

confederation

In BGP, an autonomous system that has been subdivided into smaller autonomous systems called *confederation member autonomous systems*. (CMASs). A confederation appears like a single autonomous system to other autonomous systems and is recognized only by other confederation members. Subdivision of an autonomous system into a confederation changes the peer relationships of confederation members in different CMASs from internal to external. Use of confederations in an autonomous system requires that all routers in the autonomous system belong to a CMAS; however, the policies used by BGP peers can change across confederation boundaries.

Confederations are one method for avoiding the overhead of having all peers within an autonomous system fully communicate to—be fully meshed with—each other. Route reflection clusters provide an easier method, but require the use of identical policies on all peers within the autonomous system. See also **route reflection**.

confederation member

Any router running BGP and recognizing that its autonomous system is subdivided into smaller autonomous systems called *confederation member autonomous systems*. (CMASs). The CMASs are recognized only by confederation members and not by peers external to the confederation. Subdivision of an autonomous system into a confederation changes the peer relationships of confederation members in different CMASs from internal to external.

confederation member autonomous system

See **CMAS**.

console port

A serial port on a PortMaster attached to a terminal or PC through which you enter commands to communicate with ComOS.

CRC error

Cyclic redundancy check error. These errors can indicate problems with source station hardware, receivers, retiming modules and/or repeaters, bridges, cabling, or transceivers.

CSU

Channel service unit. An ancillary device needed to adapt the V.35 or X.21 interface to a port on a telephone carrier switch. The CSU is placed between the data terminal equipment (DTE) and the switch.

cyclic redundancy check

See **CRC error**.

D

data communications equipment

See **DCE**.

data link connection identifier

See **DLCI**.

data service unit

See **DSU**.

Data Set Ready

See **DSR**.

data terminal equipment

See **DTE**.

Data Terminal Ready

See **DTR**.

DCE

Data communications equipment. Devices and connections of a communications network that make up the network end of the interface between the network and the user. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal to synchronize data transmission between DCE and DTE devices. Modems and interface cards are DCEs.

DDE

Dynamic data exchange. A form of interprocess communication that uses shared memory to exchange data between applications. Applications can use a one-time data transfer or ongoing exchanges.

degree of preference

In BGP, an arbitrary rating number that the PortMaster assigns to every route it receives from a BGP peer. A higher numbers indicates a greater preference for a route when more than one exists to a destination. A route from an internal peer is assigned the local preference number that the PortMaster learned with the route. For a route learned from an external peer, the PortMaster calculates a number based on the autonomous system path length; the shortest path is preferred. You can use a routing policy rule to override the calculated or learned value and assign your own degree of preference to a route. See also **local preference**.

destination

In BGP, the final autonomous system in the autonomous system path whose IP address prefixes and associated netmasks are reported in the network layer reachability information (NLRI) field of an update message. A destination and its path comprise a BGP route. See also **path**; **route**.

dialback

See **callback**.

dial group

A number that is used to associate dial-out locations with ports.

digital service unit

See **DSU**.

direct memory access

See **DMA**.

DHCP

The underlying protocol for a network administration software tool that enables network managers to set up servers to automatically supply IP addresses and configuration settings to clients. DHCP extends and enhances the BOOTP protocol by providing reusable IP addresses and allocating IP addresses based on subnet, client ID string, or media access control (MAC) address.

DLCI

Data link connection identifier. A unique number that represents a particular permanent virtual circuit (PVC) on a particular physical segment of the Frame Relay network. As the frame is passed through each switch, the DLCI is remapped automatically by the switch as necessary.

DMA

Direct memory access. Transfer of data from a peripheral device, such as a hard disk drive, into a computer memory without mediation by a microprocessor.

DNS

Domain Name System. The system used on the Internet for translating the names of network hosts into IP addresses.

DRAM

Dynamic random access memory. A type of semiconductor random access memory (RAM) that stores information in integrated circuits containing capacitors.

DSR

Data Set Ready. The circuit that is activated when data communications equipment (DCE) is powered up and ready for use. See also **DCE**.

DSU

Digital service unit or data service unit. An ancillary device needed to adapt the physical interface on a data terminal equipment (DTE) device—such as a V.35 interface on a port—to a transmission facility—such as leased line or a Frame Relay switch. If the DTE lacks complete digital line interface capability, the DSU can be located with the channel service unit (CSU) on the customer's site and known as a CSU/DSU. See also **CSU**.

DTE

Data terminal equipment. A device at the user end of the interface between the network and the user. The DTE connects to a data network through a data communications equipment (DCE)—such as a modem or an interface card. DTEs convert user information into data signals for transmission, and reconvert received data signals into user information. Compare **DCE**.

DTR

Data Terminal Ready. The circuit that is activated to inform the data communications equipment (DCE) when the data terminal equipment (DTE) is ready to send and receive data. See also **DCE**; **DTE**.

dynamic data exchange

See **DDE**.

Dynamic Host Configuration Protocol

See **DHCP.**

dynamic random access memory

See **DRAM**.

E

E1

Digital WAN carrier facility used predominantly in Europe that carries data at a rate of 2.048Mbps. E1 lines can be leased for private use from common carriers. Compare **T1**.

easy-multihome

A specialized, predefined BGP policy that simplifies the use of PortMaster routers in straightforward multihomed environments. When you define easy-multihome for a peer, you restrict what the PortMaster handles from the peer to information that is no more than two autonomous system hops away from the PortMaster. Only information that meets this criterion is accepted from the peer, put into the routing table used to forward packets to their destinations, and advertised to other peers. If you define easy-multihome for a peer, you must also define a default route on each router in your autonomous system to point them to destinations more distant than two hops. See also **multihome routing**; **policy**.

EBGP

Exterior BGP. The BGP used between peers in different autonomous systems, or, when confederations are in use, between peers in different confederation member autonomous systems (CMASs). Unlike internal BGP peers, EBGP peers need not have full connectivity with one another.

echo test

A diagnostic test used to check network reachability in which an Internet Control Message Protocol (ICMP) Echo Request packet or Simple Network Management Protocol (SNMP) test packet is sent to elicit a standard response.

endpoint discriminator

A 12-digit identifier used to associate multiple chassis in a Multichassis PPP domain.

Ethernet

A network communications system developed and standardized by Digital Equipment Corporation, Intel, and Xerox using baseband transmission, carrier sense multiple access/carrier detect (CSMA/CD) access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration of Ethernet into the Open System Interconnection (OSI) model and extends the physical layer and media with repeaters and implementations that operate on fiber optic cable, broadband, and unshielded twisted pair.

Exterior BGP

See **EBGP**.

external peer

A peer that resides in a different autonomous system—or, when confederations are in use, in a different confederation member autonomous system (CMAS)—from the current PortMaster.

F

File Transfer Protocol

See **FTP**.

filter

Generally, a process or device that screens network traffic for certain characteristics, such as source address, destination address, or protocol, and determines whether to forward or discard that traffic based on the established criteria.

filter table

A database used to store filters.

Flash RAM

See **nonvolatile RAM**.

flow control

A technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed. Flow control can be software-based, or hardware-based.

FRAD

Frame Relay access device. A network device that links any non-Frame Relay connection to a Frame Relay WAN.

frame

A packaging structure for network data and control information. A frame consists of a destination address, source address, length field, data, padding, and frame check sequence. The 802.3 standard for Ethernet specifies that the minimum size data frame is 64 bytes and the maximum size data frame is 1518 bytes.

Frame Relay

An industry-standard switched data link layer protocol that handles multiple virtual circuits using high-level data link layer control (HDLC) encapsulation between connected devices. It is used across the interface between user devices (for example, hosts and routers) and network equipment (for example, switching nodes). Frame Relay is more efficient than X.25, the protocol it replaced.

Frame Relay access device

See **FRAD**.

FTP

File Transfer Protocol. A TCP/IP protocol used to transfer files between network hosts.

G

gateway

A device that connects two or more networks that use different protocols. Gateways provide address translation services, but do not translate data. Gateways must be used in conjunction with special software packages that allow computers to use networking protocols not originally designed for them.

graphical user interface

See **GUI**.

GUI

Graphical user interface. A software interface based on pictorial representations and menus of operations and files.

H

hardwired

A continuous connection between two sites. A port on a PortMaster that is configured for hardwired use cannot be simultaneously used for any other type of connection.

hello

Protocol used by OSPF routers to acquire neighbors and to synchronize their topological databases.

high-water mark

The number of bytes of queued network traffic required to open an additional dial-out line to a remote location.

hop

The transmission of a data packet between two network nodes—for example, between two routers.

hop count

Measurement of the distance between a source and destination that is used as a metric to compare routes. If a packet traverses six routers between source and destination nodes, the hop count for the packet will be 6 when it arrives at its destination node.

host

A single, addressable device on a network. Computers, networked printers, and routers are hosts.

hunt group

A group of multiple telephone circuits that allows telephone calls to find an idle circuit to establish a link.

I

IBGP

Interior BGP. The BGP used between peers in the same autonomous system, or, when confederations are in use, between peers in the same confederation member autonomous system (CMAS). All IBGP peers must maintain direct BGP connections to—be **fully meshed** with—every other internal peer, but need not be physically attached to one another.

ICMP

Internet Control Message Protocol. The part of the Internet Protocol (IP) that allows for generation of error messages, test packets, and informational messages related to IP. This protocol is used by the ping function to send an ICMP Echo Request to a network host, which replies with an ICMP Echo Reply.

in-band signaling

Signaling over the data path.

injection policy

A set of rules that determine the path and route information the PortMaster takes from BGP and places into its routing table used to forward packets to their destinations. The PortMaster uses the information to determine how packets it receives are forwarded to their ultimate destinations. See also **policy**.

Integrated Services Digital Network

See **ISDN**.

interface

Connection and interaction between hardware, software, and the user. The interface between components in a network is called a protocol. On the PortMaster, the virtual connection between a PortMaster port and the network to which it is connected is called an interface. The connection can be permanent as with the Ethernet interface or network hardwired ports, or it can be temporary, as with ports used for dial-in or dial-out connections.

Interior BGP

See **IBGP**.

internal peer

A peer that resides in the same autonomous system—or, when confederations are in use, in the same confederation member autonomous system (CMAS)—as the current PortMaster.

internal router

In OSPF, a router with all of its directly connected interfaces or physical networks belonging to the same area and containing no virtual connections to the backbone area.

International Organization for Standards

See **ISO**.

Internet

The world-wide internetwork consisting of several large national backbone networks and several regional and campus networks.

Internet Control Message Protocol

See **ICMP**.

Internet Network Information Center

See **InterNIC**.

Internet Protocol

See **IP**.

internetwork

A network of networks.

InterNIC

Internet Network Information Center. An organization that provides information and services related to networking technologies.

IP

Internet Protocol. The protocol defined in RFC 791.

IP address

A 32-bit number assigned by the system administrator, usually written in the form of four decimal fields separated by periods—for example, 192.9.200.1. Any computing device that uses IP must be assigned an Internet or IP address. Part of the Internet address is the IP network number (IP network address), and part is the host address (IP host address). All machines on a given IP network use the same IP network number, and each machine has a unique IP host address. The system administrator sets the subnet mask to specify how much of the address is network number and how much is host address.

IP address prefix

An IP address number that, when paired with a netmask length, represents a range of addresses rather than a single IP network. For example, the prefix and netmask length 128.0.0.0/8 describe all networks whose IP addresses begin with 128. See also **netmask length**.

IP Control Protocol

See **IPCP**.

IPCP

IP Control Protocol. A protocol used by the Point-to-Point Protocol (PPP) for establishing and configuring an IP link over PPP.

IPX

Internet Packet Exchange. Internet protocol defined by Novell, Inc.

IPXWAN

IPX Wide Area Network protocol. The protocol used to establish and configure an IPX link over the Point-to-Point Protocol (PPP), as described in RFC 1634.

IPX Wide Area Network

See **IPXWAN**.

ISDN

Integrated Services Digital Network. A digital communications standard designed to allow the transmission of voice, data, images, and video over existing copper phone lines.

ISO

International Organization for Standards. The international organization that sets standards for network communication protocols.

ITU-T

International Telecommunication Union Telecommunication Standardization Sector. International organization that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT. See also **CCITT**.

K

KB

Kilobyte(s). 1024 bytes.

Kb

Kilobit(s). 1024 bits.

Kbps

Kilobits per second.

keepalive message

A periodic message sent between BGP peers to keep their BGP sessions open. If a preset amount of time elapses between keepalive messages from a peer, the PortMaster identifies the peer as no longer operational and drops the session—and any information learned from that peer.

L

LAN

Local area network. A local collection, usually within a single building or several buildings, of personal computers and other devices connected by cabling to a common transmission medium, allowing users to share resources and exchange files. Compare **WAN**.

latency

1) The delay between the time a device requests access to a network and the time it is granted permission to transmit. 2) The delay between the time when a device receives a frame and the time that frame is forwarded out the destination port.

LCP

Link Control Protocol. The protocol used by the Point-to-Point Protocol (PPP) for establishing, configuring, and testing the data link connection.

LED

Light-emitting diode.

line speed

The speed of the physical wire attached to the interface or interface hardware. The line speed is 10Mbps for Ethernet and 1.544Mbps for T1. Fractional T1 is often implemented with a wire speed of T1 (1.544Mbps) and a lower port speed. Upgrading line speed is generally a hardware change. See also **port speed**.

Link Control Protocol

See **LCP**.

link state advertisement

See **LSA**.

LMI

Local Management Interface. A protocol used to communicate link status and permanent virtual circuit (PVC) status in Frame Relay. Two types of LMI are available on Frame Relay: the original proprietary Cisco/Stratacom LMI, and the ANSI T1.617 Annex-D LMI. Although the PortMaster supports both, LMI on the PortMaster refers to the Cisco/Stratacom implementation. See also **Annex-D**.

local area network

See **LAN**.

Local Management Interface

See **LMI**.

local preference

In BGP, the degree-of-preference number that the PortMaster assigns to every external route it advertises to an internal or confederation-member BGP peer. A higher number indicates a greater preference for a route when more than one exists to a destination. Internal and confederation-member peers receiving this route use this local preference rather than calculating their own degree of preference for a route. You can use a routing policy rule to override this value and assign your own local preference to a route you advertise. See also **degree of preference**.

location

A dial-out destination.

location table

A database on the PortMaster where location settings are stored. See **location**.

lockstep

A feature of BGP on the PortMaster that ensures consistency of routing information between the BGP and non-BGP routers within its autonomous system. Lockstep forces the PortMaster to advertise a route learned from an internal BGP peer only when it has learned the same route via an Interior Gateway Protocol (IGP)—OSPF or RIP—or a static route. See also **transit service**.

LSA

Link state advertisement. The state of the router links (interfaces), networks, summaries, or autonomous system external links of an OSPF router that it periodically advertises. Link states are also advertised when a link state changes.

M

MAC address

Media access control address. A unique 48-bit binary number—usually represented as a 12-digit hexadecimal number—encoded in the circuitry of a device to identify it on a LAN.

Management Information Base

See **MIB**.

management station

A workstation or PC capable of retrieving and analyzing statistical information from networked Simple Network Management Protocol (SNMP) agents.

master

In Multichassis PPP, the PortMaster through which an initial connection for a given user is made. Every master also has a corresponding slave. Masters are for a given connection only, and a PortMaster that functions as a master for one user's connection can be a slave for a different user's connection. See also **slave**.

maximum transmission unit

See **MTU**.

MB

Megabyte(s). 1,048,576 bytes.

Mbps

Megabits per second. A unit for measuring data rates.

MD5

Message digest algorithm 5. The algorithm used for message authentication in Simple Network Management Protocol (SNMP) v.2. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. ComOS uses the RSA Data Security, Inc. MD5 Message-Digest Algorithm.

media access control address

See **MAC address**.

message digest algorithm 5

See **MD5**.

MIB

Management Information Base. A set of variables that a Simple Network Management Protocol (SNMP)-based management station can query from the SNMP agent of a network device.

modem

Modulator-demodulator. A device that converts the digital signals used by computers to analog signals that can be transmitted over telephone lines.

modem table

A database resident on the PortMaster containing configuration information for commonly used modems.

MTU

Maximum transmission unit. The largest frame or packet that can be sent through a port on a PortMaster without fragmentation.

Multichassis PPP

Multilink PPP over two or more chassis.

multiexit discriminator

In BGP, an arbitrary rating number that the PortMaster can use to enforce the use of preferred exit and entry points when multiple connections exist between its autonomous system and another. The PortMaster assigns the multiexit discriminator to any route that it advertises to its external peers, and forwards any multiexit discriminator it learns from its external peers on to its internal peers. A lower number indicates a greater preference for a route when more than one exists to a destination through multiple peers within the same neighboring autonomous system. You can use a routing policy rule to override this value and assign your own multiexit discriminator to a route that you learn or advertise.

multihome routing

In BGP, the process of choosing among multiple exit points to route packets out of a single autonomous system, typically to the Internet. Routers in a multihomed autonomous system usually store large amounts of network reachability information to help them select the best exit point. See also **easy-multihome**.

multiline load balancing

The ability of a PortMaster to add additional lines when network traffic is heavy. If more than one line to a remote location is established, the PortMaster balances the traffic among the lines. Multiline load balancing is distinct from Multilink PPP.

Multilink PPP

A protocol defined in RFC 1990 that allows a PortMaster to automatically bring up additional ISDN B channels as bandwidth needs increase. See also **Multichassis PPP**.

N

name server

A server connected to a network that resolves hostnames into network addresses.

name service

The software system that provides a database of authorized users for a computer, subnet, or network. The system can reside on one device, or be distributed across several devices in a network.

neighbor

(1) In OSPF, two routers that have interfaces to a common network are neighbors. On multiaccess networks, neighbors are dynamically discovered by the OSPF Hello protocol.

(2) In Multichassis PPP, PortMaster products in the same Multichassis PPP domain.

netmask

A 32-bit number that distinguishes the portion of an IP address referring to the network or subnet from the portion referring to the host. Compare **subnet mask**.

netmask length

A number between 0 and 32 preceded by a slash (/) and following an IP address prefix. The netmask length indicates the number of high-order bits in the prefix that an IP address must match to fall within the range indicated by the prefix. For example, the prefix and netmask length 128.0.0.0/8 describe all networks whose IP addresses begin with 128. See also **IP address prefix**.

network

A collection of computers, terminals, and other devices and the hardware and software that enable them to exchange data and share resources over short or long distances.

network handle

A number assigned to an active socket that can be used to close the socket manually, rather than by a request from the client.

Network Information Service

See **NIS**.

network interface card

See **NIC**.

network layer reachability information

See **NLRI**.

network management

In the Open System Interconnection (OSI) model, the five functional application areas of accounting management, configuration management, fault management, performance management, and security management.

NIC

Network interface card. A card that provides network communication capabilities to and from a computer system. A NIC is also known as an *adapter*.

NIS

Network Information Service. A protocol developed by Sun Microsystems for the administration of network-wide databases.

NLRI

Network layer reachability information. The part of a BGP route containing the IP address prefixes and associated netmask lengths that are reachable via the path described in the route. The networks indicated by these prefixes and netmasks reside in the destination autonomous system—the final one listed in the path.

node

A device, such as a PC, server, switching point, bridge, or gateway, connected to a network at a single location. A node can also be called a *station*. See **host**.

nonvolatile RAM

See **NVRAM**.

notification message

A message sent between BGP peers to inform the receiving peer that the sending peer must terminate the BGP session because an error occurred. The message contains information that explains the error. See also **keepalive message**; **open messag**e; **update message**.

not-so-stubby-area

See **NSSA**.

NSSA

Not-so-stubby-area. In OSPF, an area similar to a stub area except that Type 1 and Type 2 external routes can be learned from it. Any external routes learned from an NSSA are translated into Type 1 and Type 2 external routes for the backbone area or other areas that accept external routes. Like stub areas, NSSAs can have default costs set for them but cannot have external routes advertised into them.

NT1

Network termination 1 device. The device that provides an interface between the ISDN Basic Rate Interface (BRI) line used by the telephone company and a customer's terminal equipment. The NT1 also provides power for the terminal equipment, if necessary. In North America, where ISDN BRI is a U loop, the customer must supply the NT1 device; in Japan and the European countries where BRI is an S/T bus, the telephone company supplies the NT1. The PortMaster integrates the NT1 device into its ISDN BRI ports that are U interfaces.

NVRAM

Nonvolatile random access memory. Nonvolatile storage that can be erased and reprogrammed electronically, allowing software images to be stored, booted, and rewritten as necessary.

O

ODI

Open Datalink Interface. A Novell specification that isolates the protocol stack from the network adapter drivers to provide hardware independence for network connectivity.

Open Datalink Interface

See **ODI**.

open message

A message sent between BGP peers to establish communication. See also **keepalive message**; **notification message**; **update message**.

Open Shortest Path First

See **OSPF**.

OSPF

Open Shortest Path First. A link-state interior gateway routing protocol designed for a hierarchical routing structure. OSPF chooses routes on a best-path, least-cost basis and supports variable-length subnet masks (VLSMs) for "classless" networking, allows up to 255 hops between routers, and provides packet authentication. See also **RIP**.

out-of-band connection

A remote connection, or a connection outside connected networks, established over a modem. This type of connection is useful when network communications are not available.

P

packet

A unit of data sent across a network.

PAP

Password Authentication Protocol. An authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike the Challenge Handshake Authentication Protocol (CHAP), PAP passes unencrypted passwords. PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. See also **CHAP**.

parity check

A process for checking the integrity of a character. A parity check appends a bit to a character or word to make the total number of binary 1 digits in the character or word (excluding the parity bit) either odd (for odd parity) or even (for even parity).

partition

Electronic isolation of an Ethernet device from network communications.

Password Authentication Protocol

See **PAP**.

path

In BGP, a autonomous system path list and a collection of attributes that provide descriptions of and explain how to reach a given collection of IP address destinations in a single autonomous system. A path and its destination comprise a BGP route. See also **destination**; **autonomous system path list**; **route**.

peer

(1) In BGP, a router with which a BGP speaker exchanges open messages, notification messages, update messages, and keepalive messages. A PortMaster can have both internal and external peers. See also **internal peer**; **external peer**.

(2) In Multichassis PPP, the relationship between a master and slave. A peer is distinct from a *neighbor*.

permanent virtual circuit

See **PVC**.

physical circuit

A physical connection between two devices.

ping

Packet Internet Groper. A program that is useful for testing and debugging networks. Ping sends an ICMP echo packet to the specified host and waits for a reply. Ping reports success or failure and sometimes statistics about its operation.

Point-to-Point Protocol

See **PPP**.

policy

In BGP, the rule or set of rules the PortMaster follows for accepting, injecting, and/or advertising BGP routes to its BGP internal and external peers. You assign policies to a peer when you add it to the PortMaster during configuration. You can use the default policy **easy-multihome**, or create and assign your own policies. One policy can handle all three functions, or you can create separate policies for acceptance, injection, and advertisement. See also **acceptance policy**; **advertisement policy**; **injection policy**.

port

The physical channel or connection through which data flows.

port speed

The rate at which data is accepted by the port at the end of the wire. For example, when a T1 line exists between a site and a telecommunications provider, the telecommunications provider accepts only the number of bits per second ordered by the customer into the port on its equipment. Upgrading port speed is generally a software change.

PPP

Point-to-Point Protocol. A protocol that provides connections between routers and between hosts and networks over synchronous and asynchronous circuits. See also **SLIP**.

PRI

Primary Rate Interface. The ISDN interface to primary rate access. Primary rate access consists of a single 64Kbps D channel plus 23 (T1) or 30 (E1) 64Kbps B channels for voice or data. Compare **BRI**.

Primary Rate Interface

See **PRI**.

propagation

The process of translating and forwarding routes from one routing protocol into another. Route propagation is also known as route *redistribution*. Lucent Remote Access recommends using route filters in propagation rules to ensure that you redistribute information without creating routing loops. Compare **summarization**.

provisioning

The process of supplying telecommunications service and equipment to a user. In ISDN provisioning, for example, a telephone service provider configures its own switch that connects via an ISDN line to the user's ISDN hardware. Because switch configuration varies according to hardware, telephone company, switch, and available ISDN line, user and provider must work together to establish the correct settings.erc

proxy Address Resolution Protocol

See **proxy ARP**.

proxy ARP

Proxy Address Resolution Protocol. A variation of the ARP protocol in which a router or other device sends an ARP response to the requesting host on behalf of another node. Proxy ARP can reduce the use of bandwidth on slow-speed WAN links. See also **ARP**.

PVC

Permanent virtual circuit. A circuit that defines a permanent connection in a switched digital service such as Frame Relay. Frame Relay is the only switched digital service that uses PVCs supported by PortMaster products.

R

RADIUS

Remote Authentication Dial-In User Service. A client/server security protocol created by Lucent.

RARP

Reverse Address Resolution Protocol. A protocol used in network routers that provides a method for finding IP addresses based on media access control (MAC) addresses. Compare **ARP**.

Remote Authentication Dial-In User Service

See **RADIUS**.

Request for Comments

See **RFC**.

Reverse Address Resolution Protocol

See **RARP**.

RFC

Request for Comments. One of a series of documents that communicate information about the Internet. Most RFCs document protocol specifications, such as those for IP and BGP. Some RFCs are designated as standards.

RIP

Routing Information Protocol. A protocol used for the transmission of IP or IPX routing information.

rlogin

Remote login. A terminal emulation program, similar to Telnet, offered in most UNIX implementations.

route

A way for a packet to reach its target via the Internet. A BGP route provides a path of autonomous systems—plus any path attributes—to a single destination autonomous system that contains particular IP address prefixes and associated netmasks. Packets whose targets fall within the networks identified by these prefixes and netmasks can use this BGP route. BGP peers advertise routes to each other in **update messages**.

router

A device that connects two or more networks and can direct traffic based on addresses.

route reflection

In BGP, a method for maintaining path and attribute information across an autonomous system, while avoiding the overhead of having all peers within an autonomous system fully communicate to—be fully meshed with—each other. To reduce the number of links, all internal peers are divided into clusters, each of which has one or more route reflectors. A route received by a route reflector from an internal peer is transmitted to its clients, which are the other peers in the cluster that are not route reflectors. Route reflection requires that all internal peers use identical policies.

Confederations are another way to avoid configuring a fully meshed set of peers in a single autonomous system. In contrast to route reflection clusters, confederations require all routers in the autonomous system to operate as confederation members. However, confederations provide a finer control of routing within the autonomous system by allowing for policy changes across confederation boundaries. See also **cluster**; **cluster ID**; **confederation**; **route reflector**.

route reflector

A router configured to transmit routes received from internal BGP peers to one or more other internal peers within its same cluster. These peers are called the route reflector's *clients*. See also **cluster**; **cluster ID**; **route reflection**.

router ID

One of the interface addresses configured on a BGP speaker. The router ID is chosen as the address that uniquely identifies the BGP speaker on the Internet.

Routing Information Protocol

See **RIP**.

routing table

A database of routes to particular network destinations, stored on a router or other device. The routing table stored on the PortMaster contains the following information for each route: IP address and netmask length of the destination, IP address of the gateway, source of the route (if any), type of route, hop-count metric, and PortMaster interface used to forward packets along the route.

RS-232 interface

A standard for data communication using serial data and control signals.

runt packet

A packet with a frame size between 8 and 63 bytes with frame check sequence (FCS) or alignment errors. The runt packet is presumed to be a fragment resulting from a collision.

S

SAP

Service Advertisement Protocol. An IPX protocol that provides a means of informing network clients, via routers and servers, of available network resources and services. See also **IPX**.

Serial Line Internet Protocol

See **SLIP**.

serial port

A bidirectional channel through which data flows one bit as a time. Asynchronous serial ports most often use 10 bits for a character of data including 1 start bit, 8 data bits, and 1 stop bit.

server

A computer or a specialized device that provides and manages access to shared network resources, such as hard disks and printers.

Service Advertisement Protocol

See **SAP**.

service profile identifier

See **SPID**.

Simple Network Management Protocol

See **SNMP**.

slave

In Multichassis PPP, a PortMaster through which a subsequent connection for a particular user is made. (The port through which the connection is made is called the **slave port**.) Every slave has a corresponding master. Slaves are for a given connection only, and a PortMaster that functions as a slave for one user's connection can be a master for a different user's connection. See also **master**.

SLIP

Serial Line Internet Protocol. The protocol, obsoleted by the Point-to-Point Protocol (PPP), for point-to-point serial connections using TCP/IP. See also **PPP**.

SNMP

Simple Network Management Protocol. A protocol defined in RFC 1157, used for communication between management consoles and network devices.

speaker

A single BGP router that is able to communicate with other routers that run BGP. When two BGP speakers communicate with each other, they are called BGP *peers*.

SPID

Service profile identifier. A number used by some service providers to define the services to which an ISDN device subscribes. The ISDN device uses the SPID when accessing the switch that initializes the connection to a service provider.

station

See **host**.

stub area

In OSPF, an area into which no external routes are imported. A stub area cannot contain autonomous system border routers and cannot be a transit area for virtual links. Summary advertisements external to the area are by default imported into the stub area but might be squelched to further reduce area database size. In this case, the default route advertisement by the autonomous system border routers handle all routes external to the area.

subnet mask

A 32-bit netmask used to indicate the bits of an IP address that are being used for the subnet address. Compare **netmask**.

summarization

The process of combining routing information from one routing protocol into another for advertisement. For example, the PortMaster summarizes non-BGP route information it receives internally via the Interior Gateway Protocol (IGP) OSPF or RIP, or via a static route, into BGP for advertisement to BGP internal and external peers. Summarized routing information must comply with BGP advertisement policy rules before advertisement. Compare **propagation**.

SVC

Switched virtual circuit. A connection established between two physical circuits, such as an ordinary telephone call. The call creates a virtual circuit between the originator and the party called.

switched virtual circuit

See **SVC**.

T

T1

Digital WAN carrier facility used to transmit data formatted for digital signal level 1 (DS-1) at 1.544Mbps through the telephone-switching network, using alternate mask inversion (AMI) or binary 8-zero substitution (B8ZS) coding. Compare **E1**.

TCP/IP

An open network standard that defines how devices from different manufacturers communicate with each other over interconnected networks. TCP/IP protocols are the foundation of the Internet.

Telnet

The Internet standard protocol, described in RFC 854, for remote terminal connection service.

terminal adapter

A device that provides ISDN compatibility to non-ISDN devices. An asynchronous terminal adapter turns an asynchronous bit stream into ISDN and is treated by the PortMaster as if it were a modem. A synchronous terminal adapter takes a synchronous bit stream and turns it into ISDN, typically supports V.25bis dialing, and connects to a PortMaster synchronous port. Some terminal adapters can be configured for either synchronous or asynchronous operation.

terminal emulator

A program that makes a PC screen and keyboard act like the video display terminal of another computer.

TFTP

Trivial File Transfer Protocol. A simplified version of the File Transfer Protocol (FTP) that transfers files but does not provide password protection or user directory capability. TFTP can be used by diskless devices that keep software in ROM and use it to boot themselves. The PortMaster can be booted from the network by means of Reverse Address Resolution Protocol (RARP) and TFTP.

transit service

In BGP, the function provided by an autonomous system that is in the path of a route but not the origination or destination. To provide reliable transit service, an autonomous system must ensure that its BGP and non-BGP routers agree on the interior routes and exit and entry points for each transit route through the autonomous system. The PortMaster synchronizes routing information between the BGP and non-BGP routers within its autonomous system by means of the **lockstep** feature. See also **lockstep**.

Trivial File Transfer Protocol

See **TFTP**.

two-way

Relating to a port configuration that allows both incoming and outgoing calls.

U

UDP

User Datagram Protocol. A connectionless protocol defined in RFC 768. UDP exchanges datagrams but does not provide guaranteed delivery.

U interface

The ISDN interface defined as the connection between the network termination 1 device (NT1) and the telephone company local loop. The U interface standard is set by each country. The U interface described in PortMaster documentation refers to the U.S. definition.

UNIX

A multiuser, multitasking operating system originally developed by AT&T that runs on a wide variety of computer systems.

UNIX-to-UNIX Copy Program

See **UUCP**.

update message

A message sent between BGP peers to convey network reachability information in two parts. The first part lists the IP address prefixes and associated netmasks for one or more routes that the PortMaster is withdrawing from service because it can no longer reach them. The second part of an update message consists of a single BGP route. See also **route**.

User Datagram Protocol

See **UDP**.

UUCP

UNIX-to-UNIX Copy Program. Interactive communication system for connecting two UNIX computers to send and receive data.

V

V.120

An ITU-T standard for performing asynchronous rate adaptation into ISDN.

V.25bis

An ITU-T standard defining how to dial on synchronous devices such as ISDN or switched 56Kbps.

V.32bis

An ITU-T standard that extends the V.32 connection range from 4800bps to 14.4Kbps. V.32bis modems fall back to the next lower speed when line quality is impaired, and fall back further as necessary. They fall forward to the next higher speed when line quality improves.

V.34

An ITU-T standard that allows data rates as high as 28.8Kbps.

V.35

The ITU-T standard for data transmission at 48Kbps over 60kHz-to-108kHz group band circuits. It includes the 35-pin V.35 connector specifications normally implemented on a modular RJ-45 connector.

variable-length subnet mask

See **VLSM**.

virtual circuit

A logical connection between two endpoints on a switched digital network. Virtual circuits can be switched or permanent. A switched virtual circuit (SVC) is used when you make an ordinary telephone call, an ISDN connection, or a V.25 switched 56Kbps connection. A permanent virtual circuit (PVC) is used in Frame Relay. See also **PVC**; **SVC**.

virtual connection

In Multichassis PPP, a connection made when a slave forwards all the packets it receives for a particular connection to its corresponding master for processing.

virtual port

In Multichassis PPP, a port corresponding to the physical port of the slave.

virtual private network

See **VPN.**

VLSM

Variable-length subnet mask. A means of specifying a different subnet mask for the same network number on different subnets. VLSM often allows addresses to be assigned more efficiently. OSPF and BGP support “classless” or VLSM routes.

VPN

Virtual private network. A restricted network that uses public wires to connect nodes. A VPN provides a way to encapsulate, or "tunnel," private data cheaply, reliably, and securely through a public network, usually the Internet. IP packets are encapsulated in a VPN protocol. VPNs use encryption and other security mechanisms to prevent unauthorized users from accessing the network and intercepting the data.

W

WAN

Wide area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay is an example of a WAN. Compare **LAN**.

Subject Index

D

E

F

H

I

P

R

S

T

U

V

W

Command Index

T

V