PATHWORKS

digital

NetworkTroubleshooting Guide

PATHWORKS

Network Troubleshooting Guide

Order Number: AA–PAGVC–TK

August 1991

Revision/Update Information:	This document supersedes *Network Troubleshooting Guide*, Version 4.0, order number AA–PAGVB–TK.
Software Version:	PATHWORKS for VMS Version 4.1 PATHWORKS for ULTRIX Version 1.1 PATHWORKS for OS/2 1.1 PATHWORKS for DOS Version 4.1

Digital Equipment Corporation
Maynard, Massachusetts

First Published, 1988
Revised, May 1989, December 1989, January 1991, August 1991

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

The postpaid Reader's Comment form at the end of this document requests your critical evaluation to assist in preparing future documentation.

This document is available on CDROM.

This document was prepared using VAX DOCUMENT, Version 1.2

HOW TO ORDER ADDITIONAL DOCUMENTATION
DIRECT MAIL ORDERS

USA*

Digital Equipment Corporation
P.O. Box CS2008
Nashua, New Hampshire 03061

CANADA

Digital Equipment
of Canada Ltd.
100 Herzberg Road
Kanata, Ontario K2K 2A6
Attn: Direct Order Desk

INTERNATIONAL

Digital Equipment Corporation
PSG Business Manager
c/o Digital's local subsidiary
or approved distributor

In Continental USA, Alaska, and Hawaii call 800–DIGITAL.

In Canada call 800-267-6215.

*Any order from Puerto Rico must be placed with the local Digital subsidiary (809-754-7575).

Internal orders should be placed through the Software Distribution Center (SDC), Digital Equipment Corporation, Westminster, Massachusetts 01473.

Contents

2 Isolating DECnet Problems

3 DECnet Messages

Part 2 Transmission Control Program and Internet Protocol (TCP/IP)

4 TCP/IP Tools

5 Isolating TCP/IP Problems

6 TCP/IP Messages

Part 3 Local Area Transport (LAT)

7 Local Area Transport (LAT) Tools

8 Isolating Local Area Transport (LAT) Problems

9 LAT Messages

Part 4 Local Area System Transport (LAST)

10 Local Area System Transport (LAST) Tools

11 Isolating Local Area System Transport (LAST) Problems

12 LAST Messages

Part 5 Appendixes

A Routing Layer Events

B Tuning the DOS Client

C Ethernet Configuration Guidelines

D Token Ring Concepts and Terms

Glossary

Index

Examples

Figures

Tables

Preface

Purpose

This guide explains how to troubleshoot PATHWORKS networks using the tools supplied with each transport.

Audience

This guide is written for the network administrator who has experience in any one transport, but who may not be familiar with other transports used on the network.

Organization

This guide is divided into separate parts for each transport. The following transports are covered:

- DECnet
- TCP/IP
- LAT
- LAST

Within each part there are three chapters describing transport operation and troubleshooting procedures. Each part contains the following chapters:

- Tools
- Isolating Problems
- Messages

This guide also contains four appendices and a glossary.

Related Documents

Topic	Document
Overview of DECnet Architecture	DECnet Digital Network Architecture General Description
Using NCP	VMS Network Control Program Manual
Using DECnet-ULTRIX	DECnet-ULTRIX User's and Programmer's Guide
Managing DECnet-ULTRIX	DECnet-ULTRIX Guide to Network Management
Using VMS LAT	VMS LAT Control Program (LATCP) Manual
IBM Token-Ring Troubleshooting	IBM Token-Ring Network Problem Determination Guide
IBM Token-Ring Operations	IBM Token-Ring Network Administrator's Guide
IBM Token-Ring Architecture	IBM Token-Ring Network Architecture Reference
IBM Token-Ring Installation	IBM Token-Ring Installation Guide

Conventions

This manual uses the following conventions:

Convention	Meaning
Ctrl/*x*	While you hold down the Ctrl key, press another key or a pointing device button.
Ctrl/Alt/Del	While you hold down the Ctrl and Alt keys, press the Del key.
Esc *x*	Press the Esc key, release it, and then press another key or a pointing device button.
Return	Press the key that executes commands or terminates a sequence. This key is labeled Return, Enter, or ↵, depending on your keyboard.
MB1, MB2, MB3	MB1 indicates the left mouse button, MB2 indicates the middle mouse button, and MB3 indicates the right mouse button. (The buttons can be redefined by the user.)
UPPERCASE	In VMS, DOS, and OS/2 syntax, uppercase letters indicate commands and qualifiers. You can enter commands and qualifiers in any combination of uppercase or lowercase, unless otherwise noted. ULTRIX commands are case-sensitive. You must enter commands in the correct case, as printed in the text.
lowercase	Lowercase letters in VMS, DOS, and OS/2 syntax indicate parameters. You must substitute a word or value, unless the parameter is optional.
teal blue type	In examples of dialog between you and the system, teal blue type indicates information that you enter. In online (Bookreader) files, this information appears in boldface.
boldface	Boldface type indicates a new term that appears in the glossary. In online (Bookreader) files, boldface indicates information you enter.
two-line commands	In VMS commands, a hyphen (-) at the end of a command line indicates that the command continues to the next line. If you type the hyphen and press Return, the system displays the _$ prompt at the beginning of the next line. Continue entering the command. If you do not type the hyphen, VMS automatically wraps text to the next line. In ULTRIX commands, a backslash (\ ) performs the same function.

Convention	Meaning
	In DOS and OS/2 commands, no character is used at the end of the first line; DOS automatically wraps text. Enter the complete command, then press Return at the end of the command.
[ ]	Square brackets in command descriptions enclose the optional command qualifiers. Do not type the brackets when entering information enclosed in the brackets.
/	A forward slash in command descriptions indicates that a command qualifier follows.
|	A vertical bar in command descriptions indicates that you have a choice between two or more entries. Select one entry unless the entries are optional.
...	A horizontal ellipsis following an entry in a command line indicates that the entry or a similar entry can be repeated any number of times. An ellipsis following a file name indicates that additional parameters, values, or information can be entered.
. . .	A vertical ellipsis in an example indicates that not all the data is shown.
NOTE	Notes provide information of special importance.
CAUTION	Cautions provide information to prevent damage to equipment or software.
WARNING	Warnings provide information to prevent personal injury.

Terminology

The terms "personal computer" (PC) and "PC workstation" refer to standalone systems. The term "client" refers to a PC, connected to the network by PATHWORKS software, that can access resources on a server. A server is a system that offers services to clients.

The term "PATHWORKS" refers to PATHWORKS software. PATHWORKS is a trademark of Digital Equipment Corporation.

Part 1

DECnet Transport

1

DECnet Tools

The **Network Control Program** (NCP) is a utility program used to configure and control DECnet networks. You can use NCP for building the network configuration database, modifying its contents, monitoring network resources, and testing network components.

This chapter includes the following sections:

- Invoking NCP on VMS
- Invoking NCP on PCs
- NCP Command Syntax
- Using NCP on the Configuration Database
- Using NCP for Troubleshooting
- Token Ring Diagnostics

Invoking NCP on VMS

You can start NCP on a VMS system by entering the following at the DCL prompt:

```
$  RUN SYS$SYSTEM:NCP
```

If NCP starts up correctly, you see the NCP> prompt and can begin to execute NCP commands.

Invoking NCP on PCs

This section describes how to troubleshoot your network by using the PATHWORKS troubleshooting diskettes with your PC.

You need to perform the following steps:

1. Verify that the two troubleshooting diskettes have the correct files on them.

   - Place the first diskette into the A drive and display its contents by entering the following:

     ```
     A:dir
     ```

     The diskette should contain the following files:

     - NCP.EXE
     - NCPHELP.BIN
     - DNNETH.EXE
     - NCPTELL.EXE
     - MEMMAN.EXE

   - Place the second diskette into the A drive and display its contents by entering the following:

     ```
     A:dir
     ```

     The diskette should contain the following files:

     - NCP.EXE
     - NCPDEFO.EXE
     - NCPDEFOP.EXE
     - NCPEVENT.EXE
     - NCPHELP.BIN
     - NCPLOOP.EXE
     - NCPSHOW.EXE

2. Copy the files from both diskettes to the subdirectory containing the DECnet files (typically C:\DECNET) on your hard disk.

   - Copy the files from the first diskette in drive A by entering the following:

     ```
     C:\ > COPY  A:*.* C:\DECNET\*.*
     ```

   - Repeat the copy command for the second diskette.

3. Start NCP by entering the following:

```
C:\>  CD DECNET
C:\DECNET>  NCP
NCP>
```

If NCP starts up correctly, you see the NCP> prompt and can begin to execute NCP commands.

NCP Command Syntax

NCP command syntax has four parts: a command verb, a component, one or more parameters, and, optionally, one or more qualifiers.

NCP prompts you for selected parameters if you do not supply them. Unless otherwise indicated, you can specify parameters in any order. Table 1–1 shows an example of NCP syntax.

Table 1–1 Example of NCP Command Syntax

Command Verb	Component	Parameter	Qualifier
SHOW	ACTIVE LINES	CHARACTERISTICS	TO filespec
	KNOWN LINES	COUNTERS	
	LINE line-id	STATUS	
		SUMMARY	

Identifying Nodes and Objects

In an NCP command, a node can be identified by either a node name with a maximum of six alphanumeric characters, or a node address in the form *area-number.node-number*. The area number is any number from 1 to 63, inclusive, and the node number is any number from 1 to 1023, inclusive. If no area number is specified, the area number of the executor node is used. The **executor** is the local node executing the NCP commands. The default area number for the executor is 1. You can specify an **object** on the executor by using an object-name up to 12 characters in length. An object is a process that receives logical link requests.

Circuit and Line Values

The **circuit-id** and **line-id** values are in the form dev-c[-u], as defined in Table 1–2. NCP device names for VAX systems are shown in Table 1–3. NCP device names for PCs are shown in Table 1–4.

For example, the circuit and line identification for a VAX Ethernet UNA device is in the form UNA-c (such as UNA-0); identification for a Token Ring device is TRN-0. An example of a synchronous DDCMP device identifier is DMC-2, and an example of an asynchronous device identifier is TT-1-0. Examples for a PC are ETHER-1 for the Ethernet device, TOKEN-1 for Token Ring, and ASYNC-1 for the asynchronous device.

Table 1–2 Definition of Circuit and Line ID

dev	A device name (see Table 1–3 and Table 1–4)
c	A decimal number (0 or a positive integer) designating a device's hardware controller
u	The unit number of the device name (0 or a positive integer); included if more than one unit is associated with the controller

Table 1–3 DECnet-VAX Device Names

Circuit or Line Device	Device Names
Ethernet	UNA, QNA, SVA, BNA
Token Ring	TRN
Synchronous DDCMP	DMB, DMC, DMF, DMP
Asynchronous DDCMP	TT, TX

Table 1–4 DECnet-PC Device Names

Circuit or Line Device	Device Names
Ethernet	ETHER-1
Token Ring	TOKEN-1
Asynchronous	ASYNC-1

Logging Events

You can use NCP to log a series of specified events on a selected node. The specified events can include circuits and lines for the selected node. The selected node can be the local executor node or a node-id within the network. The following example causes all events for local node line DMC-1 to be logged on the console.

```
NCP>  SET LOGGING MONITOR LINE DMC-1 KNOWN EVENTS
```

NCP Help

NCP provides a Help facility with information about each command. You can access Help with the following command:

```
$  RUN SYS$SYSTEM:NCP
NCP>  HELP [topic...]
```

Using NCP on the Configuration Database

The **configuration database** consists of two databases:

- A permanent database that establishes the default parameter values for node startup
- A volatile (memory resident) database that contains the current parameter values in a functional network

On VMS nodes, the permanent database information is supplied to the volatile database when the network is started by running the STARTNET.COM command procedure. On PC nodes, the database is read during DECnet initialization.

The basic NCP commands required to define the network components in the permanent configuration database are shown in the following example:

```
$  RUN SYS$SYSTEM:NCP
NCP>  DEFINE EXECUTOR
NCP>  DEFINE NODE node-id
NCP>  DEFINE NODE NAME node-name
NCP>  DEFINE CIRCUIT circuit-id
NCP>  DEFINE LINE line-id
NCP>  DEFINE OBJECT object-name
NCP>  DEFINE LOGGING MONITOR STATE ON
NCP>  DEFINE LOGGING MONITOR EVENTS event-list
NCP>  EXIT
```

Note

If you are configuring the VMS node for the first time, you can use the automatic configuration command procedure NETCONFIG.COM to establish the parameters needed to get DECnet running. DOS and OS/2 nodes are configured using the NETSETUP procedure.

DEFINE Command

The DEFINE command establishes the contents of the permanent database. You must have SYSPRV privilege to change the DECnet permanent database on VMS.

For example, to define the permanent name of a node, enter the following commands:

```
$  RUN SYS$SYSTEM:NCP
NCP>  DEFINE NODE NAME node-name
NCP>  EXIT
```

SET Command

The SET command establishes the contents of the volatile database. You must have OPER privilege to change the DECnet volatile database on VMS. You can use the SET command with the ALL parameter to cause all DECnet permanent database entries for a network component to be loaded into the DECnet volatile database on VMS.

Use the SET commands to modify the current configuration on your node for any network component. For example, to add circuit and line entries for an Ethernet UNA device, enter the following commands:

```
$  RUN SYS$SYSTEM:NCP
NCP>  SET LINE UNA-0 STATE ON
NCP>  SET CIRCUIT UNA-0 STATE ON
NCP>  EXIT
```

LIST and SHOW Commands

Examine the contents of your network configuration database with the NCP commands LIST and SHOW. Use the LIST command to display information in the permanent database. Use the SHOW command to display volatile database entries.

For example, to display the permanent name and address of a node, enter the following commands:

```
$  RUN SYS$SYSTEM:NCP
NCP>  LIST NODE node-id
NCP>  EXIT
```

PURGE and CLEAR Commands

Delete entries from the configuration database with the PURGE and CLEAR commands. Use the PURGE command to delete permanent database entries. Use the CLEAR command to delete or reset volatile database entries.

For example, to delete a node from the permanent database, enter the following commands:

```
$  RUN SYS$SYSTEM:NCP
NCP>  PURGE NODE node-id ALL
NCP>  EXIT
```

You can also delete an individual parameter for a node. For example, to purge the RECEIVE PASSWORD parameter for node PURPLE, enter the following commands:

```
$  RUN SYS$SYSTEM:NCP
NCP>  PURGE NODE PURPLE RECEIVE PASSWORD
NCP>  EXIT
```

Note

On a VMS node, the PURGE command does not affect the volatile (memory-resident) copy of the DECnet database. Therefore, you can still access a node deleted with the PURGE command until DECnet is started again. If you use the CLEAR command to delete a node entry, the node entry reappears in the volatile database after DECnet is started again.

Using NCP for Troubleshooting

You can troubleshoot your network by issuing NCP loop tests from your node and allowing other nodes to send loop tests to your node. These tests check the operation of your local node, the connection to the remote node, and the communication hardware between them.

The loop tests give you the following information:

- Length of the test message
- Number of times to send the test message
- Type of format for the test message
- Node that receives the test message and returns it

Note

The NCP Loop commands should be used only with Ethernet networks. Token Ring network connections should be tested using the diagnostics supplied by your Token Ring vendors.

Start with your local node and progress outward to each of the components in your network to determine which specific component is not operating properly. If all components appear to be working properly, contact your network manager or the manager of the node you are trying to reach to determine the network problem.

You do not need special technical knowledge to use NCP for troubleshooting. However, it is helpful to know which nodes are in the network, where they are located, and how they are connected.

You can display network information and use other nodes to send loop tests to your node with the following NCP commands:

- LOOP checks the operation of your local node, the connection to the remote node, and the communication hardware that connects them. This hardware includes local and remote modems.
- MONITOR LOGGING continuously displays event-logging information on the terminal screen.
- READ LOG displays the contents of the event-logging buffer.
- SHOW displays statistics about node, line, counter, and circuit characteristics.
- TELL instructs a remote DECnet node to display information about its lines, or circuits.
- ZERO resets line, circuit, or executor counters.

When you run a loop test, network counters record events that occur while the test is running. The counters record the error and traffic information on the network, including events for your local node, line, or circuit. You can zero these counters prior to running the loop test by using the ZERO CIRCUIT, ZERO LINE, and ZERO EXECUTOR commands. When you run the loop test, the errors and traffic that are recorded reflect the most recent network activity. To display the counters after you run the loop test, use one of the following commands:

- SHOW CIRCUIT COUNTERS
- SHOW LINE COUNTERS
- SHOW EXECUTOR COUNTERS

Loop tests require that the line and circuit states are ON before you run them. Therefore, NCP turns lines and circuits ON before running the loop test. When you start the test, NCP displays a message indicating that the line or circuit is turned ON.

Some of the loop tests use a device called a **loopback connector** to check the operation of the various components. The loopback connector is a hardware device that you attach to each component to isolate it from the others while you test it. Loop test data is sent to the connector or network and then echoed back to the local node. If the loop test data does not return, or if it does not match the original data, the problem is probably with the component you are currently testing.

LOOP Commands

The following section describes the LOOP commands you can use to test your DECnet network.

MIRROR Command

Use the MIRROR command on the local PC node when you perform a loop test from a remote node to the local PC node. MIRROR allows test messages from the remote node to be echoed by the local node back to the remote node. VMS nodes automatically mirror back to the remote node.

LOOP EXECUTOR Command

You can test the network software on your PC using the LOOP EXECUTOR command. You send the loop messages through the network and routing software back to yourself. Your network software receives the messages and reports their receipt. If this test is not successful, you need to reinstall the network software.

LOOP LINE CONTROLLER Command

You can test the network controller board on your PC by using the LOOP LINE CONTROLLER command.

You must attach the loopback connector, included in your DECnet-DOS software kit, to run this test. The message is sent out through the network controller and is turned around at the loopback connector. If this test is not successful, check the hardware controller on your PC.

LOOP NODE Command

You can check the connection to a node on your network by issuing the LOOP NODE command.

Using this command, you can send test data through the network software, through the network controller, and over the line to a remote node. A mirror must be running on the remote node to echo the test message back to your local node. If this test does not complete successfully, it indicates a problem with the connection to the remote node.

LOOP CIRCUIT Command

You can check the logical link connection to an adjacent node by using the LOOP CIRCUIT command.

This command sends test data to a remote node through the network and routing software, through the network controller, and over the circuit to an adjacent node. The mirror on the adjacent node echoes the test data back to your local node using the same logical link. If this test is not successful, it indicates a problem along the link to the adjacent node.

Token Ring Diagnostics

This section describes the diagnostic software you can use to test the DEC TRNcontroller 100 (DEQRA) hardware and software on a Token Ring network. PC clients on the Token Ring should be tested using the diagnostics supplied by your vendor. For detailed information about Token Ring networks, refer to the IBM documents listed in Related Documents at the beginning of this guide. See also Appendix D, Token Ring Concepts and Terms.

The DEC TRNcontroller 100 is an interface card that enables Digital Q-bus VAX VMS 3XXX and 4000 series computers to connect to Token Ring networks. The DEC TRNcontroller 100 includes the software necessary for interfacing with a Token Ring network.

The DEC TRNcontroller 100/DEC Token Ring Network Device Driver for VMS kit includes the diagnostic program DEQRA$DIAGS.EXE. You can use the diagnostic program to test the following parts of the DEC TRNcontroller 100:

- Board status
- Lobe loop test
- Ring loop test

Note

Running the diagnostic program causes a hardware reset of the DEC TRNcontroller 100 board. Therefore, verify that the board is not in use before you run the diagnostic program.

Running DEQRA$DIAGS

You can run the diagnostic program as a foreign command by entering the following:

```
$   TR_DIAG :==$SYS$TEST:DEQRA$DIAGS.EXE
$   TR_DIAG/DEVICE=TRA0/SPEED=16
```

Note

The speed value in the previous command must match your Token Ring network transmission speed and the speed value in the DEC TRNcontroller 100 TRDRIVER.INI configuration file. Therefore, the speed value must be 4 or 16.

The diagnostic program displays the following menu. The menu options are described later in this section.

```
DEQRA Diagnostics

1 = Board Status
2 = Lobe Loopback Test
3 = Ring Loopback Test
q = Quit

Enter Option:
```

Board Status Test

This test verifies that the DEC TRNcontroller 100 board is performing correctly. The test sends a data packet from the diagnostic program to the device driver, which forwards the packet to the board. The board returns the packet to the device driver, which then returns it to the diagnostic program. This verifies operation of the following components:

- Program to driver interface
- Driver to board interface
- DEC TRNcontroller 100 software

Lobe Loopback Test

This test verifies that the DEC TRNcontroller 100 lobe is performing correctly. The DEC TRNcontroller 100 should be connected to a lobe that is **not** connected to a MAU.

The test has the host send 10 frames to the board, which transmits the frames onto the lobe cable. The disconnected lobe cable forms an internal loopback path so the frames are received back by the board and returned to the host. This verifies operation of the following components:

- DEC TRNcontroller 100 software
- Token Ring interface circuitry
- Lobe cable

Ring Loopback Test

This test verifies that the DEC TRNcontroller 100 network connection is performing correctly. The DEC TRNcontroller 100 lobe must be connected to the MAU for this test.

The test has the host send 10 frames to the board, which transmits the frames onto the ring network. The frames circulate once around the ring and are received by the board, which returns them to the host. This verifies operation of the following components:

- DEC TRNcontroller 100 software
- Token Ring interface circuitry
- Lobe cable
- Network connection

2 Isolating DECnet Problems

This chapter consists of the DECnet problem-isolation flowcharts and a series of troubleshooting procedures. The flowcharts help you isolate a network problem. When you isolate the problem, a decision point leads you to a specific procedure or set of procedures to fix the problem. You can locate the starting page for each procedure in the Contents or in the Index.

This chapter provides the following master procedures:

- VMS Server Master Procedure (DECnet)
- ULTRIX Server Master Procedure (DECnet)
- OS/2 Server Master Procedure (DECnet)
- DOS Client Master Procedure (DECnet)
- OS/2 Client Master Procedure (DECnet)
- Troubleshooting Hardware and Configuration (DECnet)

DECnet Problem-Isolation Flowcharts

You must consider several key questions to isolate a network problem. The answer to each question determines which procedures you should perform. This section contains a table and a series of flowcharts that guide you through the procedures.

The first key question asks if the network has ever carried traffic. If the answer is no, perform the appropriate master procedure. This master procedure combines three procedures into one. You may not have to perform all of the subprocedures in the master procedure.

The remaining flowcharts ask questions specific to your network. The procedure you use depends on your answer to the questions. You may have to perform client, file server, or printer server procedures.

Note

You should address each question in order. The answers to each question help you rule out unlikely problems.

Table 2–1 lists the key questions in order and indicates the path you should take. For example, if your answer to key question 1 is No, go to Figure 2–1. If your answer is Yes, go to key question 2.

Table 2–1 Key Questions for DECnet

	Key Question	If ...	Go to ...
1.	Has the network ever carried traffic?	No	Figure 2–1, Problem with Untried Network (DECnet Flowchart 1)
		Yes	Key Question 2
2.	Has hardware been added or changed?	Yes	Figure 2–2, When Hardware Has Changed (DECnet Flowchart 2)
		No	Key Question 3
3.	Has software been modified?	No	Figure 2–3, When Software Is Unmodified (DECnet Flowchart 3)
		Yes	Key Question 4
4.	Is there an error message? If not, is there a transport problem?	Yes	Figure 2–4, Transport Problem (DECnet Flowchart 4)
		No	Key Question 5
5.	Is there a problem with the file server?	Yes	Figure 2–5, File Server Problem (DECnet Flowchart 5)
		No	Key Question 6
6.	Is there a problem with remote printing?	Yes	Figure 2–6, Remote Printing Problem (DECnet Flowchart 6)

Figure 2–1 Problem with Untried Network (DECnet Flowchart 1)

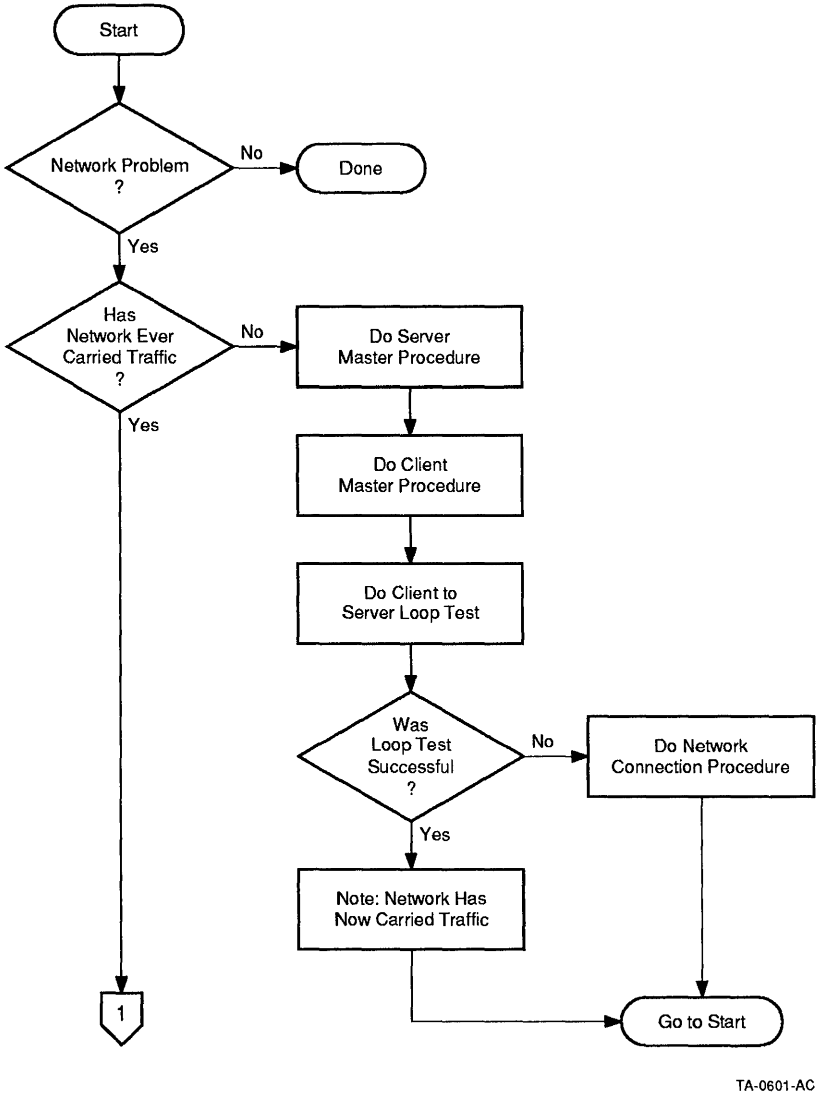
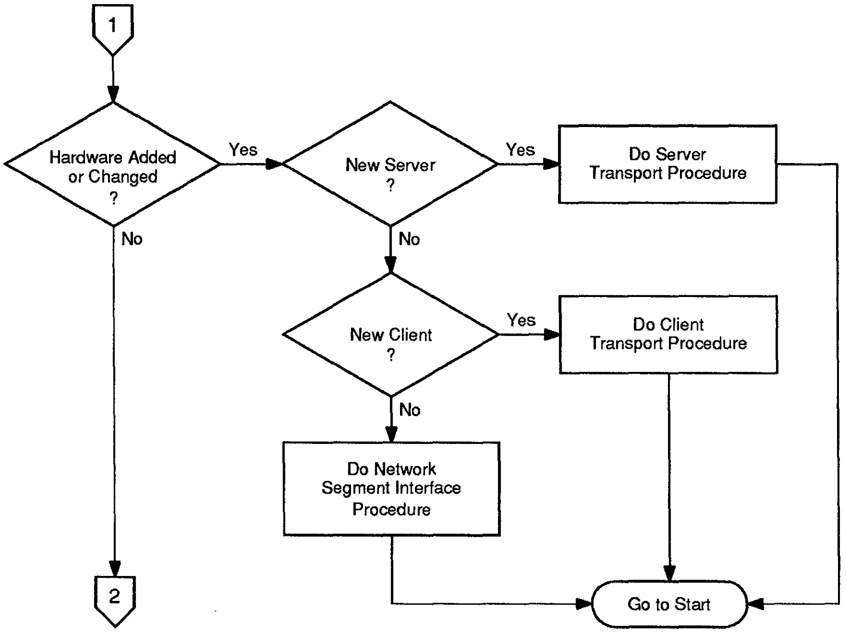

Start
Network Problem ?
No
Done
Yes
Has Network Ever Carried Traffic ?
No
Do Server Master Procedure
Yes
Do Client Master Procedure
Do Client to Server Loop Test
Was Loop Test Successful ?
No
Do Network Connection Procedure
Yes
Note: Network Has Now Carried Traffic
1
Go to Start
TA-0601-AC

Figure 2–2 When Hardware Has Changed (DECnet Flowchart 2)


1
Hardware Added or Changed ?
Yes
New Server ?
Yes
Do Server Transport Procedure
No
No
New Client ?
Yes
Do Client Transport Procedure
No
Do Network Segment Interface Procedure
2
Go to Start

TA-0602-AC

Figure 2–3 When Software Is Unmodified (DECnet Flowchart 3)

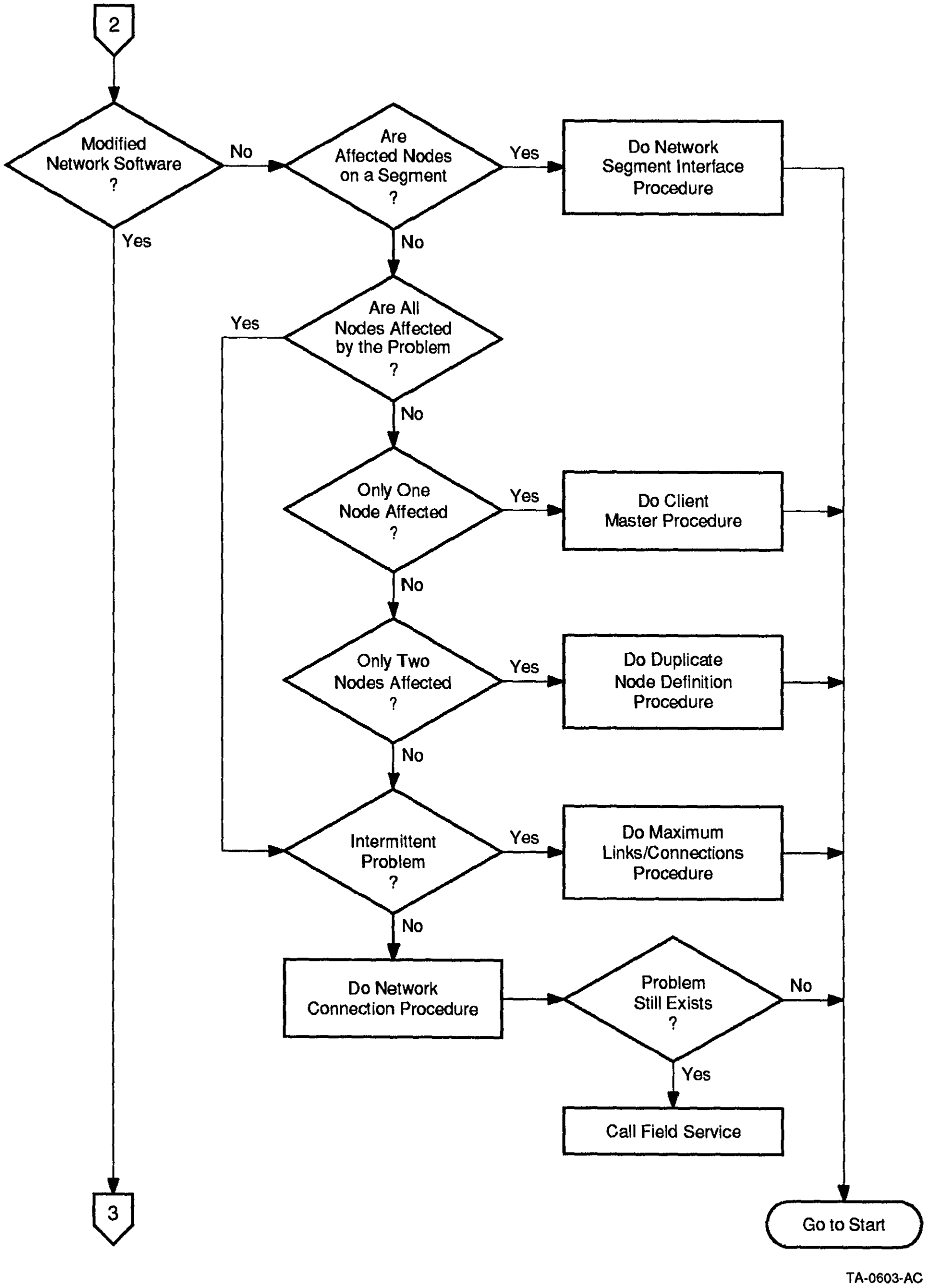

2
Modified Network Software ?
No
Are Affected Nodes on a Segment ?
Yes
Do Network Segment Interface Procedure
Yes
No
Are All Nodes Affected by the Problem ?
Yes
No
Only One Node Affected ?
Yes
Do Client Master Procedure
No
Only Two Nodes Affected ?
Yes
Do Duplicate Node Definition Procedure
No
Intermittent Problem ?
Yes
Do Maximum Links/Connections Procedure
No
Do Network Connection Procedure
Problem Still Exists ?
No
Yes
Call Field Service
3
Go to Start
TA-0603-AC

Figure 2–4 Transport Problem (DECnet Flowchart 4)

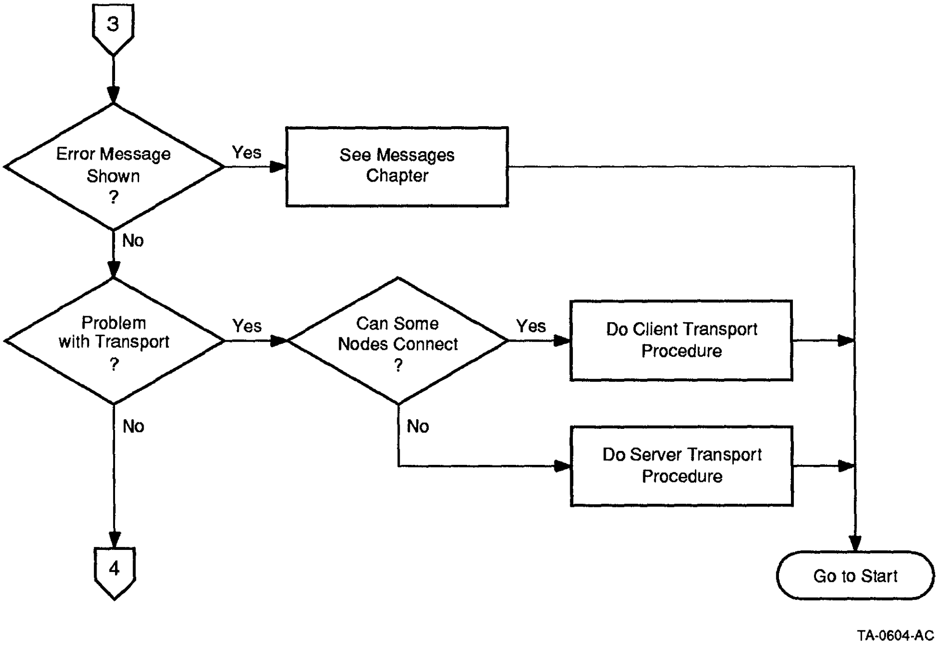


Figure 2–5 File Server Problem (DECnet Flowchart 5)

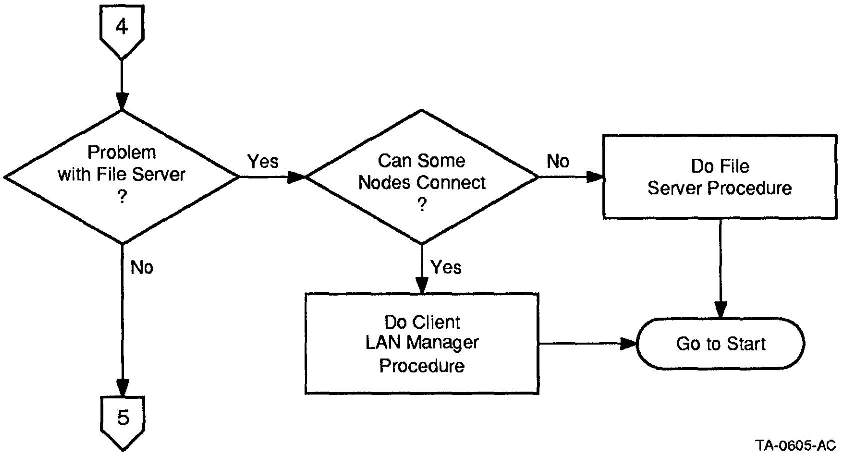
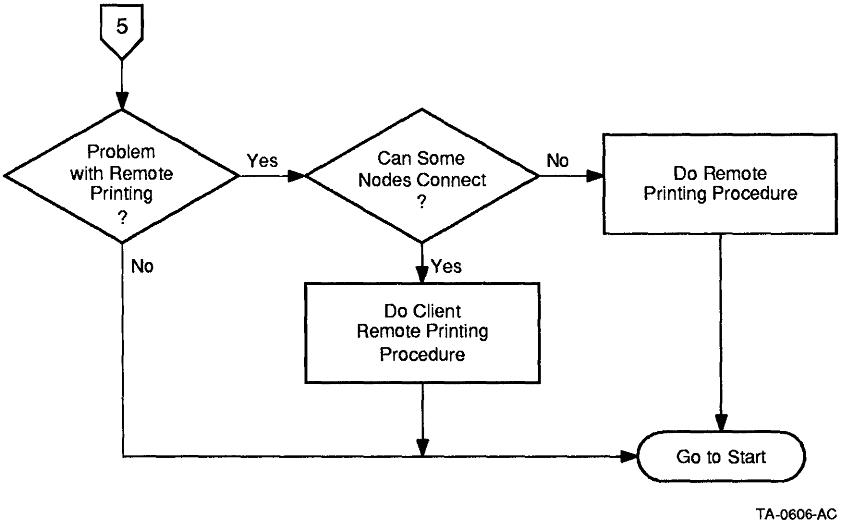


Figure 2–6 Remote Printing Problem (DECnet Flowchart 6)


5
Problem with Remote Printing ?
Yes
Can Some Nodes Connect ?
No
Do Remote Printing Procedure
No
Yes
Do Client Remote Printing Procedure
Go to Start
TA-0606-AC

VMS Server Master Procedure (DECnet)

The VMS Server Master Procedure consists of a set of subsidiary procedures, which together compose the VMS server master procedure. Use these procedures in conjunction with the DECnet Problem-Isolation Flowcharts.

The VMS Server Master Procedure is composed of the following:

- VMS Server Transport Procedure (DECnet)
- VMS File Server Procedure (DECnet)
- VMS Remote Printing Procedure (DECnet)

Use all the VMS Server Procedures to verify that your VMS server is operational. First, verify that DECnet is operational. Then, verify that the appropriate services are operational.

VMS Server Transport Procedure (DECnet)

This procedure verifies that DECnet is operating correctly on a VMS server.

1. Log in to the system manager's account and determine the version of VMS by entering the following:

   ```
   $  SHOW SYSTEM
   ```

   The first line of the response contains the version number of the VMS operating system. If the version of the VMS operating system is less than 5.1, you must upgrade your VMS operating system.

2. Ensure that DECnet is running by checking that the DECnet executor state is on by entering the following:

   ```
   $  RUN SYS$SYSTEM:NCP
   NCP>  SHOW EXECUTOR
   ```

   - If the response indicates that the executor state is on, DECnet is running. Ensure that the response contains the correct node name and address. Record the node name and address for future reference. Proceed to the next numbered step.
   - If the response indicates that the executor state is off, DECnet is not running. Set the executor to on in the volatile database and define it as on in the permanent database, using the following commands:

     ```
     NCP>  SET EXECUTOR STATE ON
     NCP>  DEFINE EXECUTOR STATE ON
     ```

   - If the command returns an error message, DECnet is not running. Restart DECnet using the following commands:

     ```
     NCP>  EXIT
     $  @SYS$STARTUP:STARTNET
     ```

   - If you receive the following system error message, your DECnet license is not installed.

     ```
     %SYSTEM-F-NOLICENSE, Operation requires software license
     ```

     If you do not own a license, you must purchase one. Otherwise, install your DECnet license according to the instructions that you received with it. If DECnet starts successfully once you have installed your license, go back to step 1. Otherwise, see the installation instructions that you received with the DECnet software.

3. Ensure that the executor is operating correctly by entering the following command.

   ```
   NCP> LOOP EXECUTOR
   ```

   - If the executor is operating correctly, proceed to the next numbered step.

   - If the response is an error message, ensure that the executor state is on. (Refer to the previous numbered step for details.)

4. Ensure that the appropriate lines are on and running by entering the following command:

   ```
   NCP> SHOW KNOWN LINES
   ```

   - If the lines are on and running, proceed to the next numbered step.

   - If the command returns the message “No information in database” enter the following commands:

     ```
     NCP> SET LINE device STATE ON
     NCP> DEFINE LINE device STATE ON
     NCP> SHOW LINE device STATUS
     ```

     In these commands:

     device — Indicates the type of controller.

     For an 8xxx series VAX computer, the first Ethernet device is BNA-0 or BNI-0, and the second is BNA-1 or BNI-1.

     For a 7xx series VAX computer, the first Ethernet device is UNA-0 and the second is UNA-1.

     For a MicroVAX I or MicroVAX II computer, the first Ethernet device is QNA-0 and the second is QNA-1.

     For a MicroVAX 2000 computer, the first Ethernet device is SVA-0 and the second is SVA-1.

     For Q-bus VAX VMS systems 3XXX and 4000 series the Token Ring device is TRN-0.

     For asynchronous devices, TXA0 through TXA3 are referred to as TX-0-0 through TX-0-3; TXB0 through TXB3 are referred to as TX-1-0 through TX-1-3; TTA0 through TTA3 are referred to as TT-0-0 through TT-0-3; TTB0 through TTB3 are referred to as TT-1-0 through TT-1-3.

   - If the response indicates that the line is an unknown component and the indicated device is BNA-x or BNI-x, UNA-x, QNA-x, or SVA-x, ensure that the physical device is installed.

- If the response indicates that the line is an unknown component and the indicated device is TX-x-x or TT-x-x, the device may not be defined as a DDCMP line. A DDCMP line can be either static or dynamic.
- If you have an asynchronous device, set it as a DDCMP line. A static DDCMP line always carries a DECnet protocol. A line configured as a static DDCMP line cannot be used as a terminal port. To set device TTA0 as a static DDCMP line, enter the following:

  ```
  NCP> EXIT
  $ RUN SYS$SYSTEM:SYSGEN
  SYSGEN> CONNECT NOA0/NOADAPTER
  SYSGEN> EXIT
  $ SET TERMINAL TTA0: /SPEED=9600 /MODEM /PROTOCOL=DDCMP /PERM
  $ RUN SYS$SYSTEM:NCP
  NCP> SET LINE TT-0-0 LINE SPEED 9600 RECEIVE BUFFER 4
  NCP> SET LINE TT-0-0 PROTOCOL DDCMP POINT STATE ON
  NCP> SET CIRCUIT TT-0-0 STATE ON
  NCP> SHOW LINE TT-0-0 STATUS
  ```

  A dynamic DDCMP line can be switched between DECnet and terminal protocols. However, both protocols must use the same device characteristics, such as baud rate and parity. To set device TTA0 as a dynamic DDCMP line, enter the following:

  ```
  NCP> EXIT
  $ RUN SYS$SYSTEM:SYSGEN
  SYSGEN> CONNECT NOA0/NOADAPTER
  SYSGEN> EXIT
  $ INSTALL CREATE SYS$LIBRARY:DYNSWITCH/SHARE/PROTECT/HEADER/OPEN
  $ RUN SYS$SYSTEM:SYSGEN
  SYSGEN> CONNECT VTA0:/NOADAPTER/DRIVER=TTDRIVER
  $ SET TERMINAL TTA0:/EIGHT_BIT/PARITY=NONE/DISCONNECT/PERM
  $ SET TERMINAL TTA0:/NOTYPEAHEAD/SPEED=1200/MODEM/PERM
  $ SET TERMINAL TTA0:/NOHANGUP/PROTOCOL=DDCMP/SWITCH=DECNET/MANUAL
  $ RUN SYS$SYSTEM:NCP
  NCP> SET LINE TT-0-0 LINE SPEED 1200 RECEIVE BUFFER 4
  NCP> SET LINE TT-0-0 PROTOCOL DDCMP POINT
  NCP> SET CIRCUIT TT-0-0 STATE ON
  NCP> SET NODE node_address INBOUND inbound
  NCP> SET NODE node_address RECEIVE PASSWORD password
  ```

  In the last two commands:

  inbound — Is either ENDNODE or ROUTER.

  password — Is the same as the remote nodes' EXECUTOR TRANSMIT PASSWORD (for example, DECnet).

  In the previous example, the use of 1200 bps baud rate assumes a remote connection through a modem. It is acceptable to use a 9600 baud, dynamic, direct line. After entering the last command, exit from the terminal emulator and set the client line state to on.

Your hardware configuration can contain multiple physical ports, such as the following:

- Two Ethernet controllers

Note

DECnet cannot operate two Ethernet controllers connected to the same Ethernet segment.

- Two or more asynchronous ports
- A combination of one or more Ethernet controllers and one or more asynchronous ports
- An Ethernet controller and a Token Ring controller

If you wish to make simultaneous connections to these devices using the DECnet protocol, DECnet must be configured as a router. (You may have to upgrade your DECnet license.) To configure DECnet as a router, enter the following:

```
NCP> DEFINE EXECUTOR TYPE ROUTING IV
NCP> SET EXECUTOR STATE OFF
NCP> EXIT
$ @SYS$STARTUP:STARTNET
```

Note

If the line state is on for only one device, DECnet does not have to be configured as a router. For example, on a MicroVAX that has two Ethernet controllers, the line state for QNA-0 is on and the line state for QNA-1 is off. Thus, DECnet is not required to be a router, but can operate on QNA-0. Additionally, the LASTDRIVER could be operating on QNA-1 or QNA-0 and QNA-1.

---

5. Verify that the appropriate circuits are on and running by entering the following command:

   ```
   NCP> SHOW KNOWN CIRCUITS
   ```

   - If the circuits are on and running, proceed to the next numbered step.
   - If the circuit state is off, set the circuit state on by entering the following:

     ```
     NCP> SET CIRCUIT device STATE ON
     NCP> DEFINE CIRCUIT device STATE ON
     ```

- If the circuit state is on, but the substate is synchronizing or starting, check the physical connections for this circuit. If the connection is an asynchronous connection, check the executor, line, and circuit states at the client.

- Check that the VMS server network interface hardware is operating correctly. Follow the procedure listed below for the type of network interface hardware (Ethernet, Asynchronous, Token Ring) you are using.

  ### Ethernet

  Disconnect the Ethernet network cable and install the appropriate loopback connector. Then enter the following command:

  ```
  $ RUN SYS$SYSTEM:DTSEND
  ```

  If there is no error message, disconnect the loopback connector and reconnect the network cable. Proceed to the next numbered step. If a device timeout or other error message is displayed there may be a hardware problem. Contact your authorized service representative.

  ### Asynchronous

  Disconnect the asynchronous network cable and install the appropriate loopback connector. Then enter the following command:

  ```
  NCP> SHOW CIRCUIT device
  ```

  When the line state is on, the SHOW CIRCUIT command response should indicate that the adjacent node is the VMS server node being tested. If it does, the line is operating correctly. Proceed to the next numbered step.

  If the state is starting, repeat the SHOW CIRCUIT command. Within 30 seconds, the state should change to on. If, in 30 seconds, the state does not change to on, check the following:

  - Line is configured as a static DDCMP line
  - Loopback plug is in place
  - Line state is on
  - Circuit state is on

  ### Token Ring

  Run the DEC TRNcontroller 100 (DEQRA) diagnostic program included in the DEC TRNcontroller 100/DEC Token Ring Network Device Driver for VMS kit. Run the diagnostic as a foreign command by entering the following:

```
$   TR_DIAG :==$SYS$TEST:DEQRA$DIAGS.EXE
$   TR_DIAG/DEVICE=TRA0/SPEED=16
```

Note

The speed value in the previous command must match your Token Ring network transmission speed and the speed value in the DEQRA's TRDRIVER.INI configuration file. Therefore, the speed value must be 4 or 16.

The diagnostic program displays the following menu:

```
DEQRA Diagnostics

1 = Board Status
2 = Lobe Loopback Test
3 = Ring Loopback Test
q = Quit

Enter Option:
```

Choose test number one (Board Status). This test verifies the DEQRA board is performing correctly by checking the following components:

- Program to DRIver interface
- Driver to board interface
- DEC TRNcontroller 100 software

If there is no error message, proceed to the next numbered step.

Note

For detailed information about Token Ring networks, refer to the IBM documents listed in Related Documents at the beginning of this guide.

---

6. Ensure that the client is registered in the server's network database by entering (at the server node) the following:

```
NCP> LIST NODE client_node_name
```

- If the NCP response contains the correct client node name and address, then the client is registered. Proceed to the next numbered step.
- If the NCP response is an error message stating that the node is an unrecognized component, then the client is not registered. To register the node, use the PCSA Manager Menu.

Alternatively, if the node is not a remote boot node, you can use NCP to define the node as follows:

```
NCP> DEFINE NODE client_node_address NAME client_node_name
```

7. This step verifies correct operation for networks with routers and without routers. Proceed to either the Without Routers or With Routers procedure that matches your network.

   - Without Routers

     If there is no DECnet router on the network, verify that the server DECnet node address has the same area number as the client DECnet node address by performing the following steps:

     a. Check the server area number by entering the following at the server:

        ```
        $ RUN SYS$SYSTEM:NCP
        NCP> SHOW EXECUTOR
        ```

     b. Check the client area number by entering the following at the client:

        ```
        C:\> NCP SHOW EXECUTOR
        ```

        In both cases, the area number is displayed before the period (.) in the node address. If the area numbers are the same, proceed to the next numbered step. If the area numbers are not the same, redefine the area number for either the server or the client.

   - With Routers

     If there is a DECnet router on the network, ensure that the router maximum area and node values in the DECnet router node database are greater than or equal to the values for all the server nodes and clients on the network. To check the values, perform the following steps:

     a. Restart the client that malfunctioned. At the client, enter the following:

        ```
        C:\> NCP READ LOG

               Events Logged as of  9-AUG-1990  10:10:32

               Event type  6.6  Line state on
               Occurred   9-AUG-1990  8:00:29
               Reason:  Operator command

               Event type  4.15  Adjacency up
               Occurred   9-AUG-1990  8:01:37
               Designated router:  8.999

               End of log
        ```

        The NCP response in the previous example is a normal response. In this case, the designated router is node 8.999.

b. Go to the node that is the designated router and determine the router characteristics by entering the following:

```
$ RUN SYS$SYSTEM:NCP
NCP> SHOW EXECUTOR CHARACTERISTICS
```

The maximum area number and maximum address are listed on the lines beginning with:

Maximum area = The area number is displayed before the period in the node address. The number listed here should be greater than, or equal to, the area numbers for all server nodes and clients.

Maximum address = The value listed here should be greater than or equal to the node address for all server nodes and clients.

c. If any server or client node address or area number exceeds the maximum value listed by the routing node, increase the maximum value at the router by entering the following commands at the router node:

```
$ RUN SYS$SYSTEM:NCP
NCP> DEFINE EXECUTOR MAXIMUM ADDRESS max_address
NCP> SET EXECUTOR MAXIMUM ADDRESS max_address
NCP> DEFINE EXECUTOR MAXIMUM AREA max_area
NCP> SET EXECUTOR MAXIMUM AREA max_area
```

Use the following table parameters for the previous commands:

Parameter	Description
max_address	Is the highest address (that part of the node_address to the right of the period) in the network.
max_area	Is the highest area (that part of the node_address to the left of the period) in the network.

Note

These procedures are only valid for VMS routers. Other routers are similar but you must refer to the appropriate router documentation.

8. Verify that the node name and node address are consistent for all nodes on the network. Figure 2–7 shows examples of node databases for the nodes in a simple network.

Figure 2–7 Examples of Node Databases

	VMS Server		Workstation 1		Workstation 2	
	Name	Addr	Name	Addr	Name	Addr
Executor	VVSVR	8.200	WKSONE	8.101	WKSTWO	8.102
Known Nodes	WKSONE	8.101	VVSVR	8.200	VVSVR	8.200
	WKSTWO	8.102	WKSTWO	8.102	WKSONE	8.101

TA-0591-AD

VMS Server Transport Procedure Completion (DECnet)

The VMS Server Transport Procedure is complete. Successfully completing this procedure indicates that DECnet is set up correctly on the VMS server.

VMS File Server Procedure (DECnet)

This procedure verifies that the file server is operating correctly on a VMS server. Before using this procedure, ensure that DECnet is operating properly. If DECnet is not operating properly, the file server will not operate properly.

1. Verify the VMS file server object type is correctly defined by entering the following:

   ```
   $ RUN SYS$SYSTEM:NCP
   NCP> SHOW OBJECT PCFS
   ```

   - If the NCP response indicates that object name PCFS is known and that it is defined as number 64, the VMS file server object type is defined correctly. Proceed to the next numbered step.
   - If the File/PID field is blank, the PCFS image is not running. How to start the file server is described later in this procedure.
   - If the File/PID field is not blank, one of the following conditions can exist:
     - The NCP response is an error message that the object is an unrecognized component. In this case, the object type PCFS is undefined. The file server may or may not be running, with the default object name OBJ_64 and the number 64.
     - The object type PCFS is defined with a number other than 64. The file server may or may not be running, with the default object name OBJ_64 and the number 64.

     In either of these conditions, determine all object types that are defined by entering the following:

     ```
     NCP> SHOW KNOWN OBJECTS
     ```

     If the NCP response indicates that PCFS is a defined object type with a number other than 64, the VMS file server object type is defined incorrectly. To remove the incorrect definition, enter the following:

     ```
     NCP> CLEAR OBJECT PCFS ALL
     NCP> PURGE OBJECT PCFS ALL
     ```

     If the NCP response indicates that an object type OBJ_64 is defined with a number 64, the VMS file server object type is defined incorrectly. If the File/PID is not blank, the file server is running. To stop the file server, enter the following:

```
NCP> EXIT
$ ADMINISTER /PCSA
PCSA_MANAGER>  STOP FILE_SERVER CONNECTIONS /ALL_SERVICES
%PCSA-I-FSVRSTOPPED, all connections stopped, File Server process
terminated
PCSA_MANAGER> EXIT
$ RUN SYS$SYSTEM:NCP
```

Define the object type PCFS and start the file server by entering the following:

```
NCP> SET OBJECT PCFS NUMBER 64 PROXY NONE
NCP> DEFINE OBJECT PCFS NUMBER 64 PROXY NONE
NCP> EXIT
$ SET DEFAULT SYS$STARTUP
$ @PCFS_STARTUP
```

2. Verify that the object type PCSA$RMI is correctly defined by entering the following:

```
NCP> SHOW OBJECT PCSA$RMI

Object Volatile Summary as of  9-AUG-1990 11:00:44

   Object   Number  File/PID          User Id          Password

  PCSA$RMI       0  SYS$SYSTEM:PCSA_RMI.COM
```

- If the object type PCSA$RMI is correctly defined, proceed to the next numbered step.
- If the object is not defined, define it by entering the following:

```
NCP> PURGE OBJECT PCSA$RMI ALL
NCP> CLEAR OBJECT PCSA$RMI ALL
NCP> SET OBJECT PCSA$RMI NUMBER 0 FILE SYS$SYSTEM:PCSA_RMI.COM
NCP> DEFINE OBJECT PCSA$RMI NUMBER 0 FILE SYS$SYSTEM:PCSA_RMI.COM
```

3. Verify that the VMS file server is running and accepting connections by entering the following:

```
$ ADMINISTER /PCSA
PCSA_MANAGER>  SHOW FILE_SERVER STATUS
```

- If the PCSA Manager response indicates that the file server is accepting connections, the server is running. Proceed to the next numbered step.
- If the file server is running, but not accepting connections, allow only registered connections by entering the following PCSA Manager command:

```
$ ADMINISTER /PCSA
PCSA_MANAGER>  START FILE_SERVER CONNECTIONS /REGISTERED
```

- If the file server is set to refuse unregistered connections, use PCSA Manager to register nodes. Alternatively, if the node is not a remote boot node, you can use NCP to register the node as follows:

  ```
  $ RUN SYS$SYSTEM:NCP
  NCP> DEFINE NODE unregistered_node_address NAME unregistered_node_name
  ```

- If the file server is not running, the response is the following error message:

  ```
  %PCSA-E-NOFSVRLINK, unable to establish link to File Server
  %PCSA-E-FILESRVNOTRUN, File Server not running
  ```

  Start the file server by entering the following:

  ```
  $ @SYS$STARTUP:PCFS_STARTUP
  ```

4. Verify that the service you are attempting to connect to exists by entering the following:

   ```
   $ ADMINISTER /PCSA
   PCSA_MANAGER> SHOW FILE_SERVER SERVICES /AUTHORIZED
   ```

   - If the service is correctly listed, proceed to the next numbered step.
   - If the service you are trying to connect to is not listed, use PCSA Manager to register the service.

     It is not necessary to register the default directory or subdirectories of an authorized VMS user's account. It is only necessary that the VMS directory exist and that the VMS account name and password provide access to the directory at the desired RMS protection level.

     On a properly registered client node:

     server_node — Indicates a valid VMS server node on which the client operator is an authorized VMS user.

     alias — Indicates the account name as defined in the VMS User Authorization File (UAF).

     user_name — Is a valid VMS user name.

     password — Is a valid password for the user name.

     Therefore, the following command can connect to the default login directory:

     ```
     C:\> USE \\server_node\alias%user_name password
     ```

   - If the service is not a PUBLIC service, ensure that the user is authorized to use the service by entering the following:

     ```
     $ ADMINISTER /PCSA
     PCSA_MANAGER> SHOW FILE_SERVER SERVICES /AUTHORIZED /USERNAME=user_name
     ```

- If the user is not authorized to connect to the desired service, use the GRANT command to authorize the connection by entering the following:

  ```
  PCSA_MANAGER> GRANT user_name service_name alias_name /ACCESS=(READ,WRITE,CREATE)
  ```

5. Verify that the VMS file server has not reached its limit for the number of sessions or connections. Determine the file server limits by entering the following:

   ```
   PCSA_MANAGER> SHOW FILE_SERVER CHARACTERISTICS
   ```

   - List the current sessions or connections established with the server by entering the following commands:

     ```
     PCSA_MANAGER> SHOW FILE_SERVER SESSIONS
     PCSA_MANAGER> SHOW FILE_SERVER CONNECTIONS
     ```

     The server limit is reached if the number of sessions or connections displayed by the previous commands is equal to the number of session or connection limits, as displayed by the PCSA Manager SHOW FILE_SERVER CHARACTERISTICS command.

     If the server session or connection limit has been reached, new sessions or connections cannot be established until enough of the existing sessions or connections are closed to reduce the number(s) to less than the limit(s).

   - Ensure that the value “Total server wide sessions” is at least two less than the DECnet executor parameter “maximum links.”

VMS File Server Procedure Completion (DECnet)

The VMS File Server Procedure is complete. Successfully completing this procedure indicates that the file server is set up correctly on the VMS server.

VMS Remote Printing Procedure (DECnet)

This procedure verifies that remote printing is operating correctly on a VMS server. For remote printing to operate properly, the file server must be operating properly.

1. Verify the following to ensure that the printer is ready to print:
   - The printer is connected to a power source.
   - The printer is connected to the VAX computer.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is online.
2. Verify that the printer queue is defined and running. Log in to the system manager's account on the server node and enter the following:

   ```
   $ SHOW QUEUE server_print_queuename
   ```

   - If the response indicates that the queue is a generic printer queue, proceed to the next numbered step.
   - If the response is "No Such Queue", use the PCSA Manager to set up the printer queue.
   - If the response indicates that the queue is stopped, the queue should be started by entering the following:

     ```
     $ START/QUEUE printer_device_queuename
     ```

3. Verify that you can print with the VMS PRINT command, specifying a queue that the VMS server uses. For example, to print a file and specify the queue LN03_DPORT, enter the following:

   ```
   $ PRINT/QUEUE=LN03_DPORT filename.ext
   ```

4. Verify that the VMS file server is running and accepting connections by entering the following:

   ```
   $ ADMINISTER /PCSA
   PCSA_MANAGER> SHOW FILE_SERVER STATUS
   ```

   - If the PCSA Manager response indicates that the file server is accepting connections, the server is running. Proceed to the next numbered step.
   - If the file server is not accepting connections, allow only registered connections by using the following PCSA Manager commands:

     ```
     $ SET DEFAULT SYS$SYSTEM
     $ ADMINISTER /PCSA
     PCSA_MANAGER> START FILE_SERVER CONNECTIONS /REGISTERED
     ```

- If the response contains the following error message, the file server is not running. For help on starting the file server and ensuring that it is operating properly, see File Server Procedure in the previous section.

  ```
  PCSA_MANAGER>  SHOW FILE_SERVER STATUS
  %PCSA-E-NOSVRLINK, unable to establish link to File Server
  %PCSA-E-FILESRVNOTRUN, File Server is not running
  ```

5. Verify that the service you are attempting to connect to exists and that the alias is correct by entering the following:

   ```
   $  SET DEFAULT SYS$SYSTEM
   $  ADMINISTER /PCSA
   PCSA_MANAGER>  SHOW FILE_SERVER SERVICES /AUTHORIZED /ALIAS=alias
   ```

VMS Remote Printing Procedure Completion (DECnet)

The VMS Remote Printing Procedure is complete. Successfully completing this procedure indicates that the printer services are set up correctly on the VMS server.

VMS Server Master Procedure Completion (DECnet)

The VMS Server Master Procedure is complete.

ULTRIX Server Master Procedure (DECnet)

This section contains a set of subsidiary procedures, which together compose the ULTRIX Server Master Procedure. Use these procedures with the DECnet Problem-Isolation Flowcharts.

The ULTRIX Server Master Procedure is composed of the following:

- ULTRIX Server Transport Procedure
- ULTRIX File Server Procedure
- ULTRIX Printer Services Procedure

Use all the ULTRIX server procedures to verify that your ULTRIX server is operational. First, verify that DECnet is operational. Then, verify that the appropriate services are operational.

ULTRIX Server Transport Procedure (DECnet)

This procedure verifies that DECnet is operating correctly on an ULTRIX server.

1. Log in to the system manager's account. After logging in, determine the version of ULTRIX by entering the following:

   ```
   $ setld -i
   ```

   The response contains the version numbers of the ULTRIX operating system. If the version of the ULTRIX operating system is less than 300 (3.0) you may have to upgrade your ULTRIX operating system.

2. Verify that DECnet is running by checking that the DECnet executor state is on by entering the following:

   ```
   # ncp
   ncp> show executor
   ```

   - If the response indicates that the executor state is on, DECnet is running. Check that the response contains the correct node name and address. Record the node name and address for future reference. Proceed to the next numbered step.
   - If the response indicates that the executor state is off, DECnet is not running. Set the executor to on in the volatile database and define it as on in the permanent database, using the following commands:

     ```
     ncp> set executor state on
     ```

   - If the show executor command returns an error message, DECnet is not running. Restart DECnet with your network startnet command.
   - If you receive the following system error message, your DECnet license is not installed.

     ```
     %SYSTEM-F-NOLICENSE, Operation requires software license
     ```

     If you do not own a license, you must purchase one. Otherwise, install your DECnet license according to the instructions that you received with it. If DECnet is started successfully once you have installed your license, go back to step 1. Otherwise, see the installation instructions that you received with the DECnet software.

3. Verify that the executor is operating correctly by entering the following:

   ```
   ncp> loop executor
   ```

   - If the executor is operating correctly, proceed to the next numbered step.
   - If the response is an error message, check that the executor state is on.

4. Check that the appropriate lines are ON and running by entering the following:

   ```
   ncp> show known lines
   ```

   - If the lines are ON and running, proceed to the next numbered step.
   - If the command returns the message “No information in database”, enter the following commands. The device indicates the type of controller you are using.

     ```
     ncp> set line (device) state on
     ncp> define line (device) state on
     ncp> show line (device) status
     ```

   - If the response indicates that the line is an unknown component and the indicated device is BNT-x, UNA-x, QNA-x, or SVA-x, check that the physical device is installed.

5. Verify that the appropriate circuits are ON and running by entering the following:

   ```
   ncp> show known circuits
   ```

   - If the line state is on, the show circuit command response should indicate that the adjacent node is an ULTRIX server node being tested. If so, the line is operating correctly. Proceed to the next numbered step.
   - If the circuit state is off, set the circuit state ON by entering the following:

     ```
     ncp> set circuit device state on
     ncp> define circuit device state on
     ```

   - If the circuit state is on, but the substate is synchronizing or starting, check the physical connections for this circuit.

     Disconnect the network cable, and install the appropriate loopback connector. For example, on a MicroVAX with a DESTA, disconnect the BNC connector from the DESTA and install a ThinWire loopback connector. A ThinWire loopback connector includes a T-connector and two terminators, as shown in Figure 2–11.

   - If a device timeout or other error message is displayed, there may be a hardware problem. Contact your authorized service representative.
   - If the state is starting, repeat the SHOW CIRCUIT command. Within 30 seconds, the state should change to on. If, in 30 seconds, the state does not change to on, check the following:
     - The line is configured as static DDCMP line
     - The loopback plug is in place
     - The line state is on

  - The circuit state is on

6. Verify that the client is registered in the server's network database by entering (at the server node) the following:

   ```
   ncp>  list node client_node_name
   ```

   - If the response contains the correct client node name and address, then the client is registered. Record the client name and address for future reference. Proceed to the next numbered step.
   - If the response is an error message stating that the node is an "unrecognized component," then the client is not registered. To register the node, use the SET/DEFINE NODE commands.

     If the node is not a remote boot node, you can define the node as follows:

     ```
     ncp>  DEFINE NODE client_node_address NAME client_node_name
     ```

7. This step verifies correct operation for networks with routers and without routers. Proceed to either the Without Routers or With Routers procedure that matches your network.

   - Without Routers

     If there is no DECnet router on the network, check that the server DECnet node address has the same area number as the client DECnet node address by entering the following at the server:

     ```
     %  ncp
     ncp>  show executor
     ```

     Check the client area number by entering the following at the client:

     ```
     % ncp>  show executor
     ```

     In both cases, the area number is displayed before the period (.) in the node address.

     If the area numbers are not the same, redefine the area number for either the server or the client.

   - With Routers

     If there is a DECnet router on the network, ensure that the router maximum area and node values in the DECnet router node database are greater than or equal to the values for all the server nodes and clients on the network. Check the values using the following procedures.

Restart the client that malfunctioned. At the client, enter the following:

```
ncp> show logging console

Logging Volatile Summary as of Wed Sep 12 16:02:34 EDT 1990

Logging = console

State                              = On
Name                               = /dev/console
Sink node                          = 9.587 (AMOK), events =
                                 0.0-9
                                 2.0-1
                                 3.0-7
                                 4.0-19
                                 288.0-31
```

The response in the previous example is a normal response. In this case, the designated router is node 9.587.

Go to the node that is the designated router and determine the router characteristics by entering the following:

```
# ncp
ncp> show executor characteristics
```

Among the characteristics shown are the maximum area number and maximum address. Check them for the following:

Maximum area = The area number is displayed before the period (.) in the node address. The number listed here should be greater than or equal to the area numbers for all server nodes and clients.

Maximum address = The value listed here should be greater than or equal to the node address for all server nodes and clients.

If any server or client node address or area number exceeds the maximum value listed by the routing node, increase the router's maximum value by entering the following commands at the router node:

```
# ncp
ncp> define executor maximum address max_address
ncp> set executor maximum address max_address
ncp> define executor maximum area max_area
ncp> set executor maximum area max_area
```

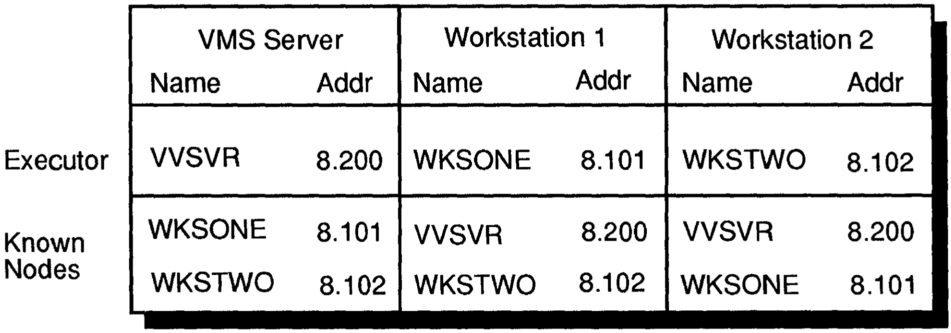
In the previous commands:

max_address Is the highest address (that part of the node_address to the right of the period) in the network.

max_area Is the highest area (that part of the node_address to the left of the period) in the network.

8. Verify that the node names and node address are consistent at all nodes on the network. Figure 2–8 shows example node databases for the nodes in a simple network.

Figure 2–8 Examples of Node Databases



	VMS Server		Workstation 1		Workstation 2	
	Name	Addr	Name	Addr	Name	Addr
Executor	VVSVR	8.200	WKSONE	8.101	WKSTWO	8.102
Known Nodes	WKSONE	8.101	VVSVR	8.200	VVSVR	8.200
	WKSTWO	8.102	WKSTWO	8.102	WKSONE	8.101

TA-0591-AD

ULTRIX Server Transport Procedure Completion (DECnet)

This completes the ULTRIX Server Transport Procedure. Completing the procedure indicates that the DECnet transport is running correctly on the ULTRIX server.

ULTRIX File Server Procedure (DECnet)

This procedure verifies that the file server is operating correctly on an ULTRIX server. Before using this procedure, verify that DECnet is running on the server. Otherwise, the file server will not operate correctly.

1. Display general DECnet information with the following command:

   ```
   # ncp show exec
   ```

2. Ensure that the ULTRIX file server is running and accepting connections by entering the following:

   ```
   # pcsamgr
   ```

   Select the CONFIG menu item, then select the Start Server submenu item. The correct response is the message "ERROR: File Server is Active", indicating the file server is running. If the file server is not active, this selection starts the server.

   Alternately, you can enter the following command line:

   ```
   # ps -aux|grep pcsa
   ```

   The correct response shows that "pcsanbud" and "pcsaadmd" are running. If they are not running, enter the **pcsamgr** command and use the CONFIG and Start Server menu to start them.

3. Enter a SHOW SYSTEM command to verify that the following processes exist:

   - pcsanbud
   - pcsaadmd

4. Ensure the service you are attempting to connect to exists by entering the following:

   ```
   # pcsamgr
   ```

   Select the VIEW menu item and the File Services submenu item. If the service you are trying to connect to is not listed, use the PCSA Manager to register the service.

   It is not necessary to register the default directory or subdirectories of an authorized ULTRIX user's account. It is only necessary that the ULTRIX directory exists and that the account name and password provide access to the directory at the desired protection level.

   At a client node, use the following command to connect to the default login directory:

   ```
   A:\> USE ?: \\internet_hostname\account password
   ```

In this command:

DECnet nodename	Is the ULTRIX server running DECnet
account	Is a valid account name as defined in the ULTRIX /etc/passwd file.
password	Is a valid password for the user name.

5. If the service is not a PUBLIC service, ensure that the user has access to the directory.

   - Enter the following command:

     ```
     # ls -lgd service_directory
     ```

   - Examine the directory protection

     If the user does not have access via the ULTRIX protection mask the user cannot connect to the service. Add the user to the group the service is in and verify the group has, at minimum, the "r" and "x" set.

6. Ensure that the ULTRIX file server has not reached its limit for the number of sessions or connections.

   Enter the following command:

   ```
   # pcsamgr
   ```

   Choose the CONFIG menu item and the Server Setup submenu item. Verify that the Max Sessions and Max Connections values are correct.

   List the current sessions or connections established with the server by viewing the File Services and Zooming on each File Service.

   The server limit is reached if the number of sessions or connections displayed are equal to the number of session or connection limits, as displayed by the PCSA Manager SHOW FILE_SERVER CHARACTERISTICS command.

   If the server session or connection limit has been reached, new sessions or connections cannot be established until enough of the existing sessions or connections are closed to reduce the number(s) to less than the limit(s). Or, you can increase the limits and restart the server.

ULTRIX File Server Procedure Completion (DECnet)

The ULTRIX File Server Procedure is complete. Successfully completing this procedure indicates that the file server is set up correctly on the ULTRIX server.

ULTRIX Remote Printing Procedure (DECnet)

This procedure verifies that remote printing is operating correctly on an ULTRIX server. For remote printing to operate properly, the file server must be operating properly.

1. To ensure that the printer is ready to print, verify the following:
   - The printer is connected to a power source.
   - The printer is connected to the VAX/RISC computer.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is online.
2. Log in to the system manager account on the server node.
3. Ensure that the printer queue is defined and running by entering:

   ```
   # lpstat -z(queue_name)
   ```

   - If the response indicates that queuing is enabled, proceed to the next numbered step.
   - If the response from the command is "unknown printer", the print queue must be set up. Use **pcsamgr** to set up the printer queue.
   - If the response indicates that queuing is disabled, the queue should be started with the following command:

     ```
     # lpc enable queue_name
     ```
4. Verify that you can print with the ULTRIX lpr command, specifying a queue that the ULTRIX server uses. For example, to print a file and specify a queue, enter the following command:

   ```
   # lpr -p queue_name filename
   ```
5. Ensure that the ULTRIX file server is running and accepting connections by entering the following:

   ```
   # pcsamgr
   ```

   Select the CONFIG menu item, then select the Start Server submenu item. The correct response is the message "ERROR: File Server is Active", indicating the file server is running. If the file server is not active, this selection starts the server.

   Alternately, you can enter the following command line:

   ```
   # ps -aux|grep pcsa
   ```

The correct response shows that "pcsanbud" and "pcsaadmd" are running. If they are not running, enter the **pcsamgr** command and use the CONFIG and Start Server menu items to start them.

For help on starting the file server and ensuring that it is operating properly, refer to the ULTRIX File Server Procedure in this chapter.

If the server is not accepting connections, allow only registered connections by using the **pcsamgr** command and use the CONFIG and Start Server menu.

Choose the View menu to examine the Printer submenu Services and Queues items to verify correct operation.

ULTRIX Remote Printing Procedure Completion (DECnet)

The ULTRIX Remote Printing Procedure is complete. Successfully completing this procedure indicates that the printer services are set up correctly on the ULTRIX server.

ULTRIX Master Server Procedure Completion (DECnet)

The ULTRIX Master Server Procedure is complete. If successful, you know that the ULTRIX server on your network is set up correctly.

OS/2 Server Master Procedure (DECnet)

This section contains a set of subsidiary procedures, which together make up the OS/2 Server Master Procedure. Use these procedures in conjunction with DECnet Problem-Isolation Flowcharts to verify that the OS/2 Server is operating correctly. The OS/2 Server Master Procedure is composed of the following:

- OS/2 Server Procedure (DECnet)
- OS/2 LAN Manager Procedure (DECnet)

OS/2 Server Procedure (DECnet)

1. Ensure that the hardware is set up correctly.

   - Check for sufficient memory
   - Check for sufficient disk space

   The main hardware problems that you may encounter are related to insufficient memory or insufficient disk storage. If the PC functions well as a client, and if it has operated in the past as a server, you should first suspect that disk or memory space is too low.

   Insufficient memory can appear as thrashing: that is, the PC spends too much time swapping memory to disk. Insufficient memory also causes client problems, such as long-term lock errors. The only solution to this problem is to add memory to the server.

   Insufficient disk space is a serious problem as client users may not be able to save data they are working on. First, ensure that client users delete old or duplicate files. If the disk is partitioned, open a new service on another partition. Add another disk drive or add a new service on another partition.

2. Ensure that you select BASIC services during installation.

   You must select BASIC services during the installation of PATHWORKS for OS/2. If it is not selected, the required files are not copied onto the PC's disk. As a result, you cannot use Netsetup to configure the PC as a server. (Netsetup will not allow you to select BASIC). At this point, you must repeat the installation procedure and select BASIC.

   Basic services enable multiple users to simultaneously access the server. Peer services enable only one user to access the server.

3. Check for an Internal Consistency error.

   If OS/2 reports an Internal Consistency error during startup, it is most likely that either the PATHWORKS for OS/2 installation was not completed properly or that CONFIG.SYS has been modified incorrectly. In particular, check that the LIBPATH, PATH and DPATH variables for PATHWORKS LANMAN subdirectories precede the OS/2 subdirectories.

4. Check the services.

   If the OS/2 server appears to be installed and configured correctly, you may want to produce a list of the services available to the server. To do this, enter the following:

   ```
   C:\  NET VIEW \\SERVER
   ```

   If the error message "Server not started" appears, it is usually the result of insufficient memory or disk space.

OS/2 Server Procedure Completion (DECnet)

Completing this procedure indicates that the OS/2 server is operating correctly.

OS/2 LAN Manager Procedure (DECnet)

This procedure shows you how to set up a File Server using the LAN Manager. This will allow other clients on the LAN access to a directory on your PC. This procedure is composed of the following:

A. Setting up a Shared Directory

B. Setting up the Service using the LAN Manager

C. Testing the Server

The prerequisites for performing this are:

- OS/2 Version 1.2 or later must be installed and running.
- PATHWORKS for OS/2 Version 1.2 or later must be installed and running.
- PATHWORKS for OS/2 Version 1.2 or later must have been installed with the LAN Manager BASIC or 386 services selected in the NETSETUP Configuration Network Setup screen. If this is not done, the required files are not available for providing services to DOS and OS/2 clients.

A. The first step is creating a shared directory that clients can access. It is necessary to separate the shared directory from your own directories and files. Create the shared directory called USERFILE. Enter the following:

```
C:\  MD USERFILE
```

B. The next step is to set up the service using the LAN Manager. You must log in as the Network Administrator to create and manage services offered to clients on your server. In the following example, the node name WSTN16 and the service USERFILE are used.

1. Log in to the network as the Network Administrator. Enter the following:

   ```
   C:\  NET LOGON ADMIN PASSWORD
   ```

   The LAN Manager prompts you that you are presently logged on (for example, logged on as standalone) and asks you if you want to log off. Answer yes (default). Use the literal PASSWORD shown; it is the default password. (At some later time, be sure to change this password).

   If you are on a network with OS/2 servers operating under user level security, and the primary Domain Controller is active, you may need to perform the following:

   a. Place a T-connector on your Ethernet card, or use the LOOP command with Token Ring.

   b. Enter the following:

      ```
      C:\  NET LOGON ADMIN PASSWORD
      ```

c. Change the password for the domain account to match the password on the primary domain controller.

d. Enter the following:

```
C:\  NET LOGON ADMIN NEWPASSWORD
```

e. Reconnect to the network.

2. Start the Administrator version of the LAN Manager's screen. Enter the following:

```
C:\  NET ADMIN
```

   LAN Manager responds with the message:

```
C:\You have administrator's privileges at WSTN16
```

3. Press Return and the Administrator's screen appears.
4. Select VIEW by pressing Alt, followed by Return.
5. On the menu that appears, press S to select shared resources. The Shared Resources dialog appears.
6. Add a shared resource by pressing A.
7. LAN Manager displays a box called "What would you like to share?" The default answer is Disk directory. Select the default by pressing Return.
8. LAN Manager displays the "Shared a Directory with the Network?" dialog box.

   a. Enter the share name. When you press Return, you may see the message "Incorrectly formed pathname of file." Ignore the message and continue by pressing Return.

   b. Enter the correct path for the shared resource directory. Enter the following:

```
C:\  USERFILE
```

   c. Click on the Done box.

9. Save the server configuration.

   a. Press Alt.

   b. Press the right arrow twice. The cursor (reverse video area) is on Config.

   c. Press Return. The configuration menu appears.

   d. Press S. The Save Configuration dialog box appears.

e. Accept the default values by choosing OK in the lower-right portion of the display. The following message appears:

```
This file exists. Do you wish to replace it?
```

f. Press Return. This accepts Yes as the answer for the message. A message appears telling you that the file was saved. The LAN Manager Administrator's screen appears.

10. Press F3 to exit the LAN Manager and return to the OS/2 prompt.
11. Check that the server is present by entering:

```
C:\  NET VIEW
```

The system responds with a list of servers, including the one you just added.

C. Test the server.

Test the service using another PC on the network.

1. Enter the USE command for your server node and service:

```
C:\  USE ?: \\yournode\USERFILE
```

2. The system displays which virtual device is connected to the service: For example:

```
C:\  USE ?: \\WSTH16\USERFILE
Device N: connected to \\WSTN16\USERFILE
C:\
```

3. Create a test file on the server. For example, if device N: is connected to the service, create the file by entering and pressing the keys exactly as shown:

```
C:\  N: Return
N:\  COPY CON TEST TEST.TXT Return
This is a test file Ctrl-Z
Return
```

4. Check that the file exists. Enter the following:

```
N:\  TYPE TEST.TXT
This is a test file.
N:\
```

5. Disconnect from the service. Enter:

```
N:\  C:
C:\  USE N: /DISCONNECT
```

OS/2 LAN Manager Procedure Completion (DECnet)

This completes the OS/2 Server LAN Manager Procedure. Completing this procedure indicates the Lan Manager is operating correctly.

OS/2 Server Master Procedure Completion (DECnet)

The completes the OS/2 Server Master Procedure. Completing this procedure indicates the server is operating correctly.

DOS Client Master Procedure (DECnet)

This section contains a set of subsidiary procedures, which together make up the DOS Client Master Procedure. Use these procedures with DECnet Problem-Isolation Flowcharts. In addition, at the end of this section there is a client loopback test, which explains how to test a client's Ethernet network controller. The Client Master Procedure is composed of the following:

- DOS Client Transport Procedure (DECnet)
- DOS Client LAN Manager Procedure (DECnet)
- DOS Client Remote Printing Procedure (DECnet)

Use these procedures to verify that your DOS client is operating correctly. First, verify that DECnet is installed and running correctly. Then, use the LAN Manager Procedure to verify that the LAN Manager is operating correctly on the DOS client. Then, use the DOS Client Remote Printing Procedure to verify that your printing service is set up and working correctly. If you are having problems with the DOS client, you may have to perform one or more of the following tests:

- Client-to-server loop test
- Client-to-client loop test
- Daisy-chain segment test
- DEMPR configuration segment test
- Client loopback test

To perform these tests, boot the client with the key diskette. Then perform the indicated test.

DOS Client Transport Procedure (DECnet)

This procedure verifies that DECnet is operating correctly on a DOS client.

> **Note**
>
> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Verify that DECnet is operational at the DOS client by entering the following:

   ```
   C:\> NCP
   NCP> SHOW EXECUTOR
   ```

   - If the response shows the executor state ON, DECnet is operational at the client. Proceed to the next numbered step.
   - If the response is the error message "Network error: Network is unreachable", then DECnet is not operational. To start DECnet, enter the following commands:

     ```
     NCP> EXIT
     C:\> STARTNET
     ```

2. Verify that the correct driver is installed by entering the following:

   ```
   C:\> NCP
   NCP> SHOW LINE
   ```

   - If the Ethernet driver is installed, the response indicates that the line name is ETHER-1.
   - If the asynchronous driver is installed, the response indicates that the line name is ASYNC-1.
   - If the Token Ring driver is installed, the response indicates that the line name is TOKEN-1.
   - If the DOS client is configured with the wrong driver, you can reconfigure the client.

     When reconfiguring the client, you cannot use the same DECPARM.DAT parameter file with both drivers. You might want to save the current DECPARM.DAT. If the current driver is the Ethernet or Token ring driver, rename DECPARM.DAT to DECPARM.ETH. If the current driver is the asynchronous driver, rename DECPARM.DAT to DECPARM.DCP.

If you are configuring the client to use the asynchronous driver and the client STARTNET.BAT file contains commands to load LAT, LAST, or LAD, remove those commands or put remark (REM) statements in front of them.

Ethernet Driver

To configure the DOS client to use the Ethernet driver, enter the following:

```
C:\>  RENAME AUTOEXEC.BAT AUTOEXEC.SAV
C:\>  CD DECNET
C:\DECNET>  COPY MSNET.ETH MSNET.INI
C:\DECNET>  DEL DECPARM.DAT
```

Press Ctrl/Alt/Del to reboot. After the PC reboots, enter the following:

```
A>  CD DECNET
A>  NET INSTALL node_name node_address
A>  CD ..
A>  RENAME AUTOEXEC.SAV AUTOEXEC.BAT
A>  AUTOEXEC
```

Use the following parameters for the previous commands:

node_name — Is the DECnet node name of the client executor.

node_address — Is the DECnet node address of the client executor.

Token Ring Driver

To configure the DOS client to use the Token Ring driver, enter the following:

```
C:\>  RENAME AUTOEXEC.BAT AUTOEXEC.SAV
C:\>  CD DECNET
C:\DECNET>  COPY MSNET.ETH MSNET.INI
C:\DECNET>  DEL DECPARM.DAT
```

Press Ctrl/Alt/Del to reboot. After the PC reboots, enter the following:

```
A>  CD DECNET
A>  NET INSTALL node_name node_address
A>  CD ..
A>  RENAME AUTOEXEC.SAV AUTOEXEC.BAT
A>  AUTOEXEC
```

Use the following parameters for the previous commands:

node_name — Is the DECnet node name of the client executor.

node_address — Is the DECnet node address of the client executor.

Asynchronous Driver

To configure the DOS client to use the asynchronous driver, enter the following:

```
C:\> RENAME AUTOEXEC.BAT AUTOEXEC.SAV
C:\> CD DECNET
C:\DECNET> COPY MSNET.DCP MSNET.INI
C:\DECNET> DEL DECPARM.DAT
```

Press Ctrl/Alt/Del to reboot. After the PC reboots, enter the following:

```
C:  CD DECNET
C:  NET INSTALL node_name node_address baud modem ON
C:  CD ..
C:  RENAME AUTOEXEC.SAV AUTOEXEC.BAT
C:  AUTOEXEC
```

Use the following parameters for the previous commands:

node_name — Is the DECnet node name of the client executor.

node_address — Is the DECnet node address of the client executor.

baud — Is the baud rate to use when communicating over the asynchronous line.

modem — Is either FULL or NULL.

3. Verify that the line state is on by entering the following:

```
C:\> NCP
NCP> SHOW LINE
```

4. Verify that the circuit state is on by entering the following:

```
C:\> NCP
NCP> SHOW CIRCUIT
```

5. If the DOS client is configured with an asynchronous driver, verify that the line and circuit characteristics are set correctly by entering the following:

```
NCP> SHOW LINE CHARACTERISTICS

Line Characteristics as of 11-Sep-1990 14:27:21

Line =  ASYNC-1

Line state                          = On
Line substate                       = Running
Device Id                           = 3COM-1
Duplex                              = Full Duplex
Protocol type                       = DDCMP
Line speed                          = 9600
Communication mode                  = 0
Stop bits                           = 1
Modem type                          = Null

NCP> SHOW CIRCUIT CHARACTERISTICS

Circuit Characteristics as of 11-Sep-1990 14:27:21
Circuit =  ASYNC-1

Circuit state                    = On
Circuit substate                 = Running
Service                          = Enabled
Adjacent node                    = 62.1023 (    )
Block size                       = 576
Hello timer                      = 30
Listen timer                     = 33
Verification                     = 0
User                             = DECnet
Owner                            = DECnet
Line Id                          = ASYNC-1
Protocol type                    = DDCMP
```

6. Verify that the client node name and address match the client node name and address as known to the server by entering the SHOW EXECUTOR command.

   If the node name and number are not the same at the client and at the server, reregister the client with the server or redefine the node name and address of the client executor using the following:

   ```
   C:\> NCP
   NCP> DEFINE EXECUTOR ADDRESS node_address NAME node_name STATE ON
   ```

   Use the following parameters for the previous command:

   node_address — Is the DECnet node address of the client executor (for example, 62.10).

   node_name — Is the DECnet node name of the client executor (for example, PCGURU).

   For the redefined executor node name and node address to take effect, the DOS client must be rebooted.

7. Ensure the server node name and address are correctly defined at the client. At the client, enter the following:

   ```
   NCP> LIST NODE node_name
   ```

   Use the following parameters for the previous command:

   node_name — Is the node name of the server node (for example, VVSRV).

   Check the following:

   - The node name and address listed match the values listed at the server node.
   - The DOS client recognizes the server as a LAN Manager node; that is, in the column labeled MS-NET, there is an M for the given node.

If the node name and address are incorrect at the DOS client or if the server node is not recognized as a LAN Manager node (in the column labeled MS-NET, there is no M for the given node), clear the DOS client definition of the server node by entering the following:

```
C:\>  NCP
NCP>  CLEAR NODE node_name
NCP>  PURGE NODE node_name
NCP>  DEFINE NODE node_address NAME node_name MS-NET
```

Use the following parameters for the previous commands:

node_address   Is the DECnet node address of the server (for example, 8.200).

node_name   Is the DECnet node name of the server (for example, VVSRV).

8. Ensure that the client network interface hardware is operating correctly by performing one of the following:

   - Token Ring

     Perform the diagnostics supplied by your vendor to verify the correct operation of the client Token Ring interface hardware.

Note

For detailed information about Token Ring networks, refer to the IBM documents listed in Related Documents at the beginning of this guide. See also Appendix D, Token Ring Concepts and Terms in this guide.

   - Ethernet

     Enter the following:

     ```
     NCP>  LOOP LINE CONTROLLER
     ```

     If the loopback test is unsuccessful, a hardware problem exists. For repair, contact your authorized service representative. For additional information about loopback tests on a client, see Client Loopback Test (DECnet) in this chapter.

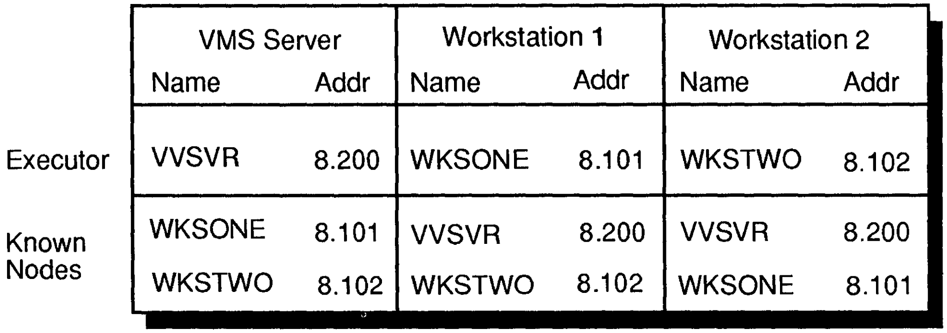
9. If there is no DECnet router on the network, verify that the server DECnet node address has the same area number as the client DECnet node address by entering the following:

   ```
   NCP>  SHOW EXECUTOR
   ```

   In both cases, the area number is displayed before the period in the node address. If the area numbers are not the same, redefine the area number for either the server or the client.

10. Verify that the node names and node address are consistent at all nodes on the network. Figure 2–9 shows example node databases for the nodes in a simple network.

Figure 2–9 Examples of Node Databases



	VMS Server		Workstation 1		Workstation 2	
	Name	Addr	Name	Addr	Name	Addr
Executor	VVSVR	8.200	WKSONE	8.101	WKSTWO	8.102
Known Nodes	WKSONE	8.101	VVSVR	8.200	VVSVR	8.200
	WKSTWO	8.102	WKSTWO	8.102	WKSONE	8.101

TA-0591-AD

11. Verify that the DOS client is operating correctly. Perform the Loop Circuit and Loop Node tests for Ethernet clients. See Client Loopback Test (DECnet) in this chapter.

DOS Client Transport Procedure Completion (DECnet)

This completes the DOS Client Transport Procedure. Completing this procedure indicates that DECnet is operating correctly on the DOS client.

DOS Client LAN Manager Procedure (DECnet)

This procedure verifies that the basic LAN Manager is operating correctly on the DOS client. To use the basic LAN Manager, DECnet must be operating correctly.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Ensure that the basic LAN Manager is running by entering:

   ```
   C:\> USE /STATUS
   ```

   The basic LAN Manager is running if the response includes the following:

   - DECnet is installed
   - Session is installed
   - Redirector is installed

   If the response indicates that the basic LAN Manager is running, proceed to the next numbered step.

   The basic LAN Manager is not running if the response includes the following:

   - DECnet is not installed
   - Session is not installed
   - Redirector is not installed

   If the response indicates that the basic LAN Manager is not running, load DECnet/PCSA components by entering the following:

   ```
   C:\> STARTNET
   ```

   The system displays a series of messages indicating that network components are loaded. The display ends with a suggestion that you enter the LOGIN command. At this point, enter the USE/STATUS command again to check whether all components are installed.

2. Verify that the DOS client node name and address match the DOS client node name and address known to the server by entering the following:

   ```
   C:\> NCP
   NCP> SHOW EXECUTOR
   ```

If the node name and address are not the same at the client and at the server, reregister the client with the server, or redefine the node name and address of the client executor by entering the following:

```
NCP> DEFINE EXECUTOR ADDRESS node_address NAME node_name STATE ON
```

Use the following parameters for the previous command:

node_address — Is the DECnet node address of the client (for example, 8.101).

node_name — Is the DECnet node name of the client (for example, WKSONE).

For the redefined executor node name and node address to take effect, the client must be rebooted.

3. Ensure the server node name and address are correctly entered at the client. At the client, enter the following:

```
NCP> LIST NODE node_name
```

Use the following parameters for the previous command:

node_name — Is the node name of the server node (for example, VVSRV).

Check the following:

- The node name and address listed match the values listed at the server node.
- The DOS client recognizes the server as a basic LAN Manager node, that is, in the column labeled MS-NET, there is an M for the given node.

If the node name and address are incorrect at the DOS client or if the server node is not recognized as a basic LAN Manager node (in the column labeled MS-NET, there is no M for the given node), clear the DOS client definition of the server node by entering the following:

```
NCP> CLEAR NODE node_name
NCP> PURGE NODE node_name
NCP> DEFINE NODE node_address NAME node_name MS-NET
```

Use the following parameters for the previous commands:

node_address — Is the DECnet node address of the server (for example, 8.200).

node_name — Is the DECnet node name of the server (for example, VVSRV).

4. Verify that the service you are attempting to connect to is offered by the server node. If the server is a VMS server, at the DOS client enter the following:

```
C:\> NET FILE \\server_node%user_name password
```

Use the following parameters for the previous command:

server_node	Is the DECnet node name of a valid server node.
user_name	Is a valid user name.
password	Is a valid password for the user name.

5. Verify that the system file, CONFIG.SYS, contains commands for increasing the number of available I/O buffers, file descriptors, and logical drive names by entering the following:

```
C:\> TYPE CONFIG.SYS
files=20
buffers=25
device=c:\cache.exe 256 on /ext
device=\decnet\laddrv.sys /D:4
device=\command.com /P /e:256
device=\decnet\ELNKII.SYS
lastdrive=z
```

Note

Ensure that the LADDRV.SYS qualifier /D: is correctly entered.

6. Verify that the machine name has been set using the SET NAME command.

Note

If the client will be connecting to the OS/2 User-Level Security System, make sure that SET LOGON has been run for the client.

DOS Client LAN Manager Procedure Completion (DECnet)

The DOS Client LAN Manager Procedure is complete. Successfully completing this procedure indicates that the basic LAN Manager is set up correctly on the DOS client.

DOS Client Remote Printing Procedure (DECnet)

This procedure verifies that remote printing is operating correctly on a DOS client. To use remote printing, the basic LAN Manager must be operating correctly.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. To ensure that the printer is ready to print, verify the following:
   - The printer is connected to a power source.
   - The printer is connected to the server.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is online.
2. Verify that the service you are attempting to connect to is offered by the server node. If the server is a VMS server, at the DOS client enter the following:

   ```
   C:\> NET FILE \\server_node%user_name password
   ```

   Use the following parameters for the previous command:

   server_node — Is the DECnet node name of a valid server node.

   user_name — Is a valid user name.

   password — Is a valid password for the user name.

3. At the DOS client, enter the following:

   ```
   C:\ > USE print_device \\server_node
   \print_service%user_name password
   C:\> NET PRINT /D:print_device
   ```

   Use the following parameters for the previous commands:

   print_device — Is one of the valid DOS print devices (for example, LPT1, LPT2, LPT3, PRN).

   server_node — Is the DECnet node name of a valid server node.

   print_service — Is the name of the remote printing service on the indicated server node. The name must end with a colon.

   user_name — Is a valid user name.

   password — Is a valid password for the user name.

   You can use the DOS COPY command to copy a file to the remote printing service.

   In Microsoft Windows, use Control Panel to select the redirected print device and printer type.

   Use the USE command to determine the print devices that are redirected and the remote printing services to which they are redirected.

DOS Client Remote Printing Procedure Completion (DECnet)

The DOS Client Remote Printing Procedure is complete. Completion of this procedure indicates that remote printing is set up correctly on the DOS client.

DOS Client Master Procedure Completion (DECnet)

The DOS Client Master Procedure is complete. If successful, you know that the DOS client on your network is set up correctly.

OS/2 Client Master Procedure (DECnet)

This section contains a set of subsidiary procedures, which together make up the OS/2 Client Master Procedure. Use these procedures in conjunction with the DECnet Problem-Isolation Flowcharts. The OS/2 Client Master Procedure is composed of the following:

- OS/2 Client Transport Procedure (DECnet)
- OS/2 Client LAN Manager Procedure (DECnet)
- OS/2 Client Remote Printing Procedure (DECnet)

Use these procedures to verify that your OS/2 client is operating correctly. First, verify that DECnet is installed and running correctly. You can then use the LAN Manager Procedure to verify that the LAN Manager is operating correctly on the OS/2 client. You can then use the OS/2 client remote printing procedure to verify that your printing services are set up and working correctly.

OS/2 Client Transport Procedure (DECnet)

This procedure verifies that DECnet is operating correctly on an OS/2 client.

1. Verify that DECnet is operational at the OS/2 client by entering the following:

   ```
   C:\> NCP
   NCP> SHOW EXECUTOR
   ```

   - If the executor state is on, then DECnet is operational on the client. Proceed to the next numbered step.
   - If the response is an error message, DECnet is not installed. To start DECnet, run Netsetup and make sure that DECnet is started.

2. Verify that the correct driver, Ethernet, Token Ring, or asynchronous, is installed by entering the following:

   ```
   C:\> NCP
   NCP> SHOW LINE
   ```

   - If the Ethernet driver is installed, the response indicates that the line name is ETHER-1.
   - If the asynchronous driver is installed, the response indicates that the line name is ASYNC-1.
   - If the Token Ring driver is installed, the response indicates that the line name is TOKEN-1.
   - If the client is configured with the wrong DECnet driver, you can reconfigure the client. OS/2 can use both the Ethernet and asynch driver at the same time. Use the following steps to configure the appropriate driver.

     ### Ethernet Driver

     To configure the OS/2 client to use the Ethernet driver, run Netsetup in the configure mode and select Ethernet for DECnet. Press Ctrl/Alt/Del to reboot.

     ### Token Ring Driver

     To configure the OS/2 client to use the Token Ring driver, run Netsetup in the configure mode and select Token Ring for DECnet. Press Ctrl/Alt/Del to reboot.

Asynchronous Driver

To configure the OS/2 client to use the asynchronous driver, run Netsetup in the configure mode and select asynch for DECnet. Pressing Ctrl/Alt/Del to reboot will restart the client. However, this kind of reboot is NOT recommended for systems running HPFS. For HPFS systems, turn off the PC, and then reboot.

3. Verify that the line state is on by entering the following:

```
C:\> NCP
NCP> SHOW LINE
```

4. Verify that the circuit state is on by entering the following:

```
C:\  >NCP
NCP> SHOW CIRCUIT
```

5. If the OS/2 client is configured with an asynchronous driver, ensure that the line and circuit characteristics are set correctly by entering the following:

```
NCP> SHOW LINE CHARACTERISTICS

Line Characteristics as of  10-Sep-1990 15:07:09

Line =  ASYNC-1

Line state                          = On
Line substate                       = Running
Device Id                           = COM-1
Duplex                              = Full-Duplex
Protocol type                       = DDCMP
Line speed                          = 9600
Communication mode                  = 0
Stop bits                           = 1
Modem type                          = Null

NCP>  SHOW CIRCUIT CHARACTERISTICS

Circuit Characteristics as of  10-Sep-1990 15:16:45
Circuit =  ASYNC-1
Circuit state                       = On
Circuit substate                    = Running
Service                             = Enabled
Adjacent node                       =  ()
Block size                          = 0
Hello timer                         = 30
Listen timer                        = 0
Verification                        = 0
User                                = DECnet
Owner                               = DECnet
Line Id                             = ASYNC-1
Protocol type                       = DDCMP
```

6. Ensure that the client node name and address match the client node name and address known to the server by entering the SHOW EXECUTOR command.

   If the node name and number are not the same at the client and at the server, reregister the client with the server, or redefine the node name and address of the client executor using Netsetup as follows:

   ```
   C:\>  NETSETUP
   ```

   For the redefined executor node name and node address to take effect, the OS/2 client must be rebooted.

7. Verify that the server node name and address are correctly defined at the client. At the client, enter the following:

   ```
   NCP>  LIST NODE node_name
   ```

   Use the following parameters for the previous command:

node_name	Is the node name of the server node (for example, CUPPCO).

   Check the following:

   - The node name and address match the values listed at the server node.
   - The OS/2 client recognizes the server as a LAN Manager node, that is, in the column labeled MS-NET, there is an M for the given node.

   If the node name and address are incorrect at the OS/2 client or if the server node is not recognized as a LAN Manager node (in the column labeled MS-NET, there is no M for the given node), clear the OS/2 client definition of the server node by entering the following:

   ```
   C:\>  NCP
   NCP>  CLEAR NODE node_name
   NCP>  PURGE NODE node_name
   NCP>  DEFINE NODE node_address NAME node_name MS-NET
   ```

   Use the following parameters for the previous commands:

node_address	Is the DECnet node address of the server (for example, 62.20).
node_name	Is the DECnet node name of the server (for example, CUPPCO).

8. Verify that the client Ethernet network interface hardware is operating correctly by entering the following:

```
NCP>  LOOP LINE CONTROLLER
```

Note

You cannot do this with the 3C503 Ethernet controller. This controller does not support LOOP LINE CONTROLLER.

If the loopback test is unsuccessful, a hardware problem exists. For repair, contact your authorized service representative. For additional information about loopback tests on a client, see Client Loopback Test in this chapter.

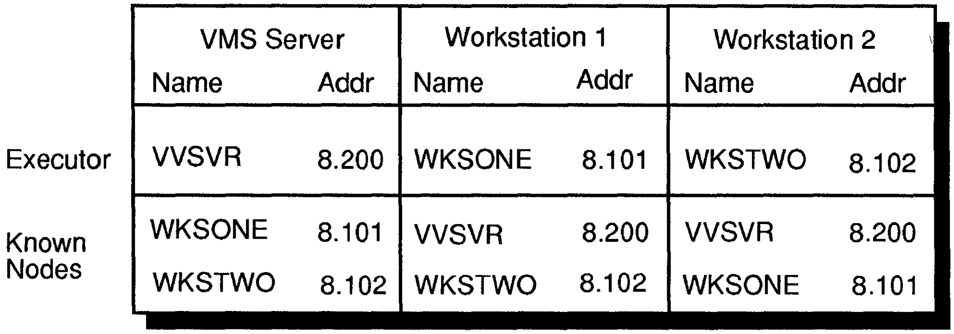
9. If there is no DECnet router on the network, ensure that the server DECnet node address has the same area number as the client DECnet node address. To check the client or the server area number, enter the following:

```
NCP>  SHOW EXECUTOR
```

In both cases, the area number is displayed before the period (.) in the node address. If the area numbers are not the same, redefine the area number for either the server or the client.

10. Ensure that the node name and node address are consistent at all nodes on the network. Figure 2–10 shows example node databases for the nodes in a simple network.

Figure 2–10 Examples of Node Databases



	VMS Server		Workstation 1		Workstation 2	
	Name	Addr	Name	Addr	Name	Addr
Executor	VVSVR	8.200	WKSONE	8.101	WKSTWO	8.102
Known Nodes	WKSONE	8.101	VVSVR	8.200	VVSVR	8.200
	WKSTWO	8.102	WKSTWO	8.102	WKSONE	8.101

TA-0591-AD

OS/2 Client Transport Procedure Completion (DECnet)

The OS/2 Client Transport Procedure is complete. Successfully completing this procedure indicates that DECnet is set up correctly on the OS/2 client.

OS/2 Client LAN Manager Procedure (DECnet)

This procedure verifies that the basic LAN Manager is operating correctly on the OS/2 client. To use the basic LAN Manager, DECnet must be operating correctly.

1. Ensure that the basic LAN Manager is running by entering:

   ```
   C:\>  USE \STATUS
   USE Version X1.1.02 PCSA Connection Manager
   Copyright (c) 1989, 1990 by Digital Equipment Corporation

   Component Information

       Datalink version 1.1.21 is installed
       LAST version 0.05 is installed
       LAD version 0.04 is installed
       DECnet version 1.01.00 is installed
       Workstation version 2.2 is installed

   Workstation Information

       Workstation is installed and active
       Messenger is installed and active
       Recvr is installed and active
       Netpopup is installed and active

   Client Information

       DECnet node name:  CUPPCO (62.20)
       Station address:   AA-00-04-00-14-F8
       Hardware address:  02-60-8C-0B-AD-62
       Ethernet hardware: unknown

       Physical drives:    8 (A:-H:)
       Logical drives:    26 (A:-Z:)
       Virtual drives:     4 (E:-H:)

   C:\>
   ```

   The response in the previous example indicates that the basic LAN Manager is running.

2. If the response indicates that the basic LAN Manager is not running, run Netsetup to make sure the LAN Manager is started by entering the following:

   ```
   C:\>  NETSETUP
   ```

   The system displays a series of messages indicating that network components are loaded. The display ends with a suggestion that you enter the LOGIN command. At this point, enter the USE/STATUS command again to check whether all components are installed.

3. Ensure that the OS/2 client node name and address match the OS/2 client node name and address known to the server by entering:

   ```
   C:\>  NCP
   NCP>  SHOW EXECUTOR
   ```

   If the node name and number are not the same at the client and at the server, reregister the client with the server, or redefine the node name and address of the client executor.

4. If the client executor node name and address are incorrect or undefined, enter:

   ```
   NCP>  DEFINE EXECUTOR ADDRESS node_address NAME node_name STATE ON
   ```

   where:

node_address	Is the DECnet node address of the client (for example, 62.20).
node_name	Is the DECnet node name of the client (for example, CUPPCO).

   For the redefined executor node name and node address to take effect, the client must be rebooted.

5. Ensure the server node name and address are correctly entered at the client. At the client, enter:

   ```
   NCP>  LIST NODE node_name
   ```

   where:

node_name	Is the node name of the server node (for example, CUPPCO).

   Make sure that:

   - The node name and address listed match the values listed at the server node.
   - The OS/2 client recognizes the server as a basic LAN Manager node; that is, in the column labeled MS-NET, there is an M for the given node.

   If the node name and address are incorrect at the OS/2 client, or if the server node is not recognized as a basic LAN Manager node (in the column labeled MS-NET, there is no M for the given node), clear the OS/2 client definition of the server node by entering:

   ```
   NCP>  CLEAR NODE node_name
   NCP>  PURGE NODE node_name
   NCP>  DEFINE NODE node_address NAME node_name MS-NET
   ```

   where:

node_address	Is the DECnet node address of the server (for example, 62.20).
node_name	Is the DECnet node name of the server (for example, CUPPCO).

6. Ensure that the service you are attempting to connect to is offered by the server node. If the server is a VMS server, at the OS/2 client enter the following:

   ```
   C:\>  USE \\server_node_name
   ```

where:

server_node_name Is the DECnet node name of a valid server node

7. Ensure that the system file, CONFIG.SYS, contains commands for increasing the number of available I/O buffers, file descriptors, and logical drive names by entering:

```
C:\>  TYPE CONFIG.SYS
PROTSHELL=C:\OS/2\PMSHELL.EXE_
 C:\OS/2\OS/2.INI
 C:\OS/2\OS/2SYS.INI C:\OS/2\CMD.EXE
SET COMSPEC=C:\OS/2\CMD.EXE
LIBPATH=C:\OS/2\DLL;C:\;
SET PATH=C:\OS/2;C:\OS/2\SYSTEM;_
 C:\OS/2\INSTALL;C:\;
SET DPATH=C:\OS/2;C:\OS/2\SYSTEM;_
 C:\OS/2\INSTALL;C:\;
SET PROMPT=$i[$p]
SET HELP=C:\OS/2\HELP
BUFFERS=30
IOPL=YES
DISKCACHE=64
MAXWAIT=3
MEMMAN=SWAP,MOVE,NOSWAPDOS
PROTECTONLY=NO
SWAPPATH=C:\OS/2\SYSTEM 512
THREADS=128
SHELL=C:\OS/2\COMMAND.COM /P
BREAK=OFF
FCBS=16,8
RMSIZE=640
DEVICE=C:\OS/2\DOS.SYS
COUNTRY=001,C:\OS/2\SYSTEM\COUNTRY.SYS
DEVINFO=SCR,VGA,C:\OS/2\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_VGA
SET VIO_VGA=DEVICE(BVHVGA)
DEVICE=C:\OS/2\POINTDD.SYS
DEVICE=C:\OS/2\PDIMOU01.SYS
DEVICE=C:\OS/2\MOUSE.SYS TYPE=PDIMOU$
DEVICE=C:\OS/2\PMDD.SYS
DEVICE=C:\OS/2\EGA.SYS
SET KEYS=ON
DEVICE=C:\OS/2\COM01.SYS
```

Note

Ensure that the LADDRV.SYS qualifier /D: is correctly entered.

OS/2 Client LAN Manager Procedure Completion (DECnet)

The OS/2 Client LAN Manager Procedure is complete. Successfully completing this procedure indicates that the basic LAN Manager is set up correctly on the OS/2 client.

OS/2 Client Remote Printing Procedure (DECnet)

This procedure verifies that remote printing is operating correctly on an OS/2 client. To use remote printing, the basic LAN Manager must be operating correctly.

To ensure that the printer is ready to print, check the following:

- The printer is connected to a power source.
- The printer is connected to the server.
- The printer has an adequate supply of paper.
- The paper passes through the printer correctly.
- The printer is on line.

1. Verify that the service you are attempting to connect to is offered by the server node. If the server is a VMS server, at the OS/2 client enter the following:

   ```
   C:\> USE \\server_node_name
   ```

   where:

   server_node_name   Is the DECnet node name of a valid server node

   At the system prompt, enter the following:

   ```
   C:\> USE print_device \\server_node\print_service%user_name password
   C:\> PRINT \D:print_device
   ```

   where:

   print_device   Is one of the valid OS/2 print devices (for example, LPT1, LPT2, LPT3, PRN).

   server_node   Is the DECnet node name of a valid server node.

   print_service   Is the name of the remote printing service on the indicated server node. (The name must end with a colon.)

   user_name   Is a valid user name.

   password   Is a valid password for the user name.

   You can use the OS/2 COPY command to copy a file to the remote printing service. Use the USE command to determine the print devices that are redirected and the remote printing services to which they are redirected.

OS/2 Client Remote Printing Procedure Completion (DECnet)

The OS/2 Client Remote Printing Procedure is complete. Successfully completing this procedure indicates that remote printing is set up correctly on the OS/2 client.

OS/2 Client Master Procedure Completion (DECnet)

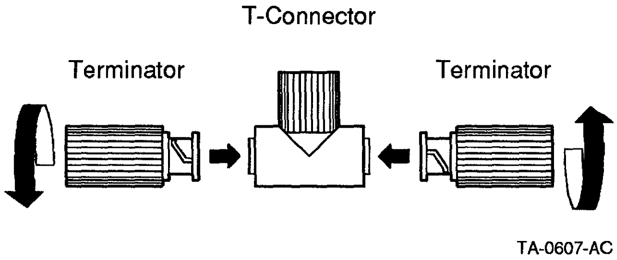
The OS/2 Client Master Procedure is complete. If successful, the OS/2 client on your network is set up correctly.

Client Loopback Test (DECnet)

The client loopback test for Ethernet requires a ThinWire loopback connector, which includes one T-connector and two terminators. These are provided with your server.

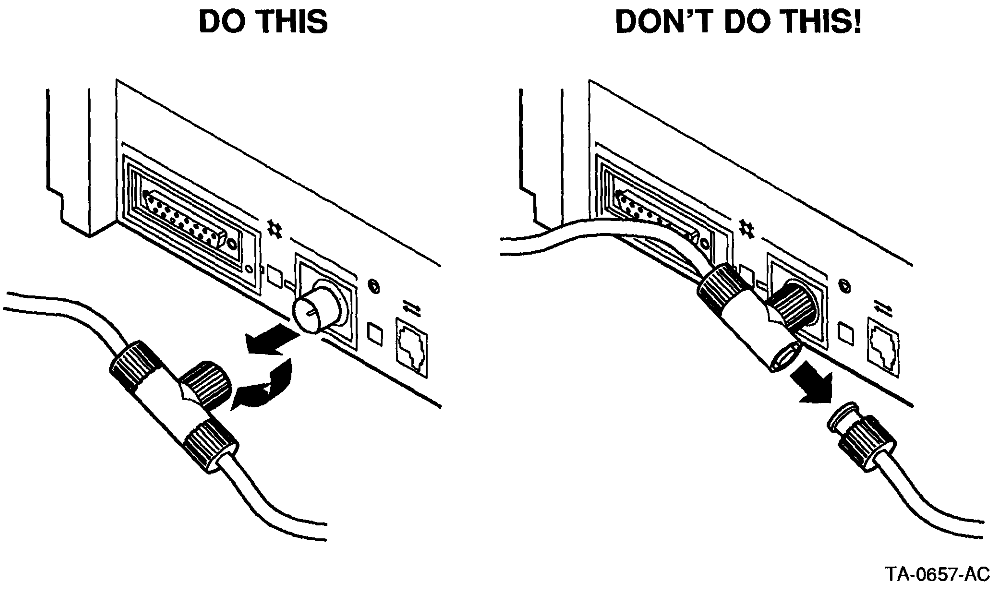
1. Assemble the loopback connector. Attach the two terminators to the opposite ends of the T-connector (Figure 2–11).

Figure 2–11 Loopback Connector Assembly



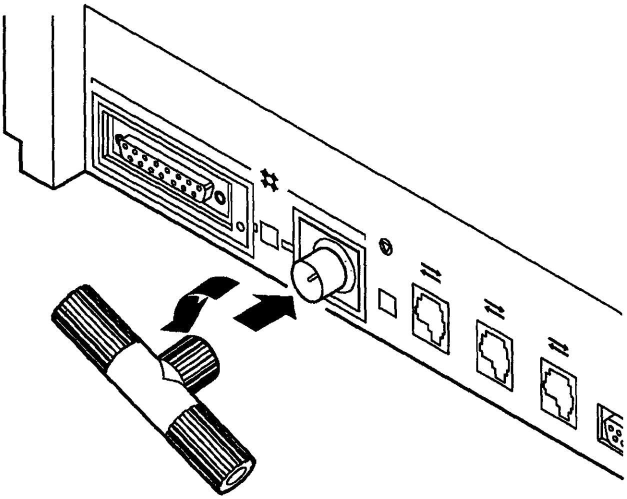
2. Disconnect the client from the network (Figure 2–12).

Figure 2–12 Disconnecting ThinWire Cabling From Client



3. Plug the loopback connector into the client (Figure 2–13).

Figure 2–13 Loopback Connector Installation



4. To test a client, ensure that the key diskette is in drive A and run the Extended Self-Test. The configuration screen is displayed when the Extended Self-Test is complete. Press any key to continue. If the Extended Self-Test fails, there is a hardware problem; contact your authorized service representative.

   To test a PC client, turn off the system unit and turn it on again to run the power-up test. If the power-up test fails, there is a hardware problem; refer to the client documentation.

   With the loopback connector on your client, the network connection will fail, displaying a network error code, and you will be at the operating system prompt. Go to step 5.

   If you cannot start the operating system, turn off the client, reinsert the key diskette, turn on the client, and try to reboot the system. If the operating system still fails to start, then the diskette is probably bad; create a new key diskette.

5. Using an OS/2 system diskette, reboot the client. When the operating system prompt appears, remove the system diskette and insert the PCSA diskette. At the operating system prompt, enter:

   ```
   C:\> NCP
   NCP> LOOP LINE CONTROLLER
   ```

   - If the client loopback test is successful, a network cabling problem may exist. The following is an example of a successful loopback test:

     ```
     LOOP LINE CONTROLLER (Ethernet)

        1.  Unplug network cable from Controller on back of PC.
        2.  Place the loopback plug on the Controller.  Test will
            fail if loopback plug is not in place.
        3.  Press any key to begin test.
        4.  At the end of the test, reconnect the Controller to
            the network.


     LOOP LINE CONTROLLER test started at 10-SEPT-1990 15:22:47

     LOOP LINE CONTROLLER test finished successfully at 10-SEPT-1990 15:22:47

     Please remove loopback plug and reconnect your node to the network.
     Press any key to continue.
     ```

   - If the client loopback test is unsuccessful, a hardware problem exists. For repair, contact your authorized service representative. The following is an example of an unsuccessful loopback test:

     ```
     LOOP LINE CONTROLLER (Ethernet)

     1.  Unplug network cable from Controller on back of PC.
     2.  Place the loopback plug on the Controller.  Test will
         fail if loopback plug is not in place.
     3.  Press any key to begin test.
     4.  At the end of the test, reconnect the Controller to
         the network.

     LOOP LINE CONTROLLER test started at 10-SEPT-1990 15:22:54

     LOOP LINE CONTROLLER test failed at 10-SEPT-1990 15:22:54

     Please remove loopback plug and reconnect your node to the network.
     Press and key to continue.
     ```

6. Remove the loopback connector from the back of the client.

7. Reconnect the ThinWire Ethernet cable to your client.

The client loopback test is complete. If the loopback test was successful, you know the client is operational.

Troubleshooting Hardware and Configuration (DECnet)

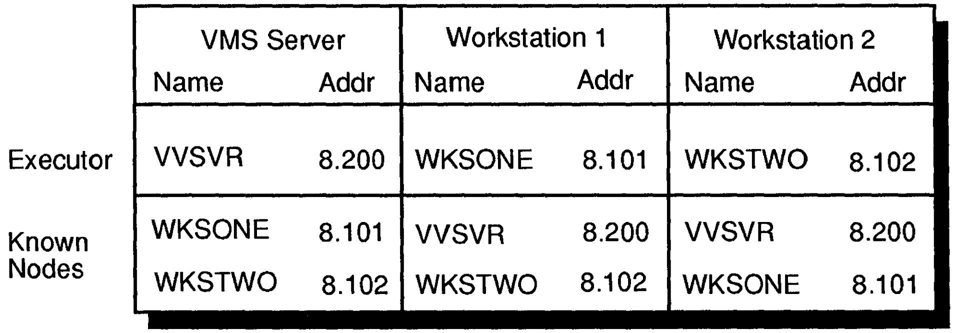
This section contains a set of procedures to use for isolating problems with the configuration of your network or with network hardware. Use the procedures in conjunction with DECnet Problem-Isolation Flowcharts. The following procedures and tests are included:

- Duplicate Node Definition Procedure (DECnet)
- Maximum Links/Connections Procedure (DECnet)
- Loop Tests (DECnet)
- Network Connection Procedure (DECnet)
- Network Segment Interface Procedure (DECnet)

Duplicate Node Definition Procedure (DECnet)

Use this procedure to confirm that two Ethernet nodes do not have the same node names or node addresses. Figure 2–14 shows example node databases for the nodes in a simple network.

Figure 2–14 Examples of Node Databases



	VMS Server		Workstation 1		Workstation 2	
	Name	Addr	Name	Addr	Name	Addr
Executor	VVSVR	8.200	WKSONE	8.101	WKSTWO	8.102
Known Nodes	WKSONE	8.101	VVSVR	8.200	VVSVR	8.200
	WKSTWO	8.102	WKSTWO	8.102	WKSONE	8.101

TA-0591-AD

To ensure that the node names and node addresses are consistent for all nodes on the network, do the following:

1. Verify that the same key diskette was not used to boot two clients. Also, check that a copy of a key diskette was not used to boot a client while the original key diskette was used to boot another client.

   This applies to network key diskettes as well as physical key diskettes.

2. On each node, use the NCP SHOW EXECUTOR command to display the node's name and address. Enter the data you collect in a table similar to that in Figure 2–14. Use this table to verify that node names and addresses are set up as expected.

Duplicate Node Definition Procedure Completion (DECnet)

The Duplicate Node Definition Procedure is complete.

Maximum Links/Connections Procedure (DECnet)

This procedure verifies that the number of allowed links, connections, or sessions on Ethernet or Token Ring networks has not been exceeded.

VMS File Servers

1. Use the NCP command SHOW EXECUTOR CHARACTERISTICS to determine the maximum number of DECnet links.
2. Use the PCSA Manager command SHOW FILE_SERVER CHARACTERISTICS to determine the maximum limit for total server-wide sessions.

   The number of links that the server must support is three times the number of PC clients on the network plus the number of nodes in the cluster plus the number of additional links required by individual applications. Ensure that the maximum limit for total server-wide sessions is larger than this number, and ensure that the number of file server total server-wide sessions is at least two less than the DECnet maximum links.

Maximum Links/Connections Procedure Completion (DECnet)

The Maximum Links/Connections Procedure is complete.

Loop Tests (DECnet)

The loop tests are composed of the following specific loop tests:

- Server-to-Server Loop Test
- Client-to-Server Loop Test
- Client-to-Client Loop Test

If the loop test fails, do the appropriate DECnet server or client procedure for each node. If no problem is found, see the section on the Network Connection Procedure in this chapter.

Server-to-Server Loop Test (DECnet)

To execute a loop test between two servers, at one server enter:

```
NCP>  LOOP NODE node_id
```

where node_id is the DECnet node address of the other server

Client-to-Server Loop Test (DECnet)

To execute a loop test between a client and a server, at the client enter:

```
NCP>  LOOP NODE node_id
```

where node_id is the DECnet node address of the server.

Client-to-Client Loop Test (DECnet)

To execute a loop test between two clients, at one client enter:

```
NCP>  MIRROR
```

At the other client, enter:

```
NCP>  LOOP NODE node_id
```

where node_id is the node address of the mirror client.

Loop Tests Completion (DECnet)

The loop tests procedure is complete.

Network Connection Procedure (DECnet)

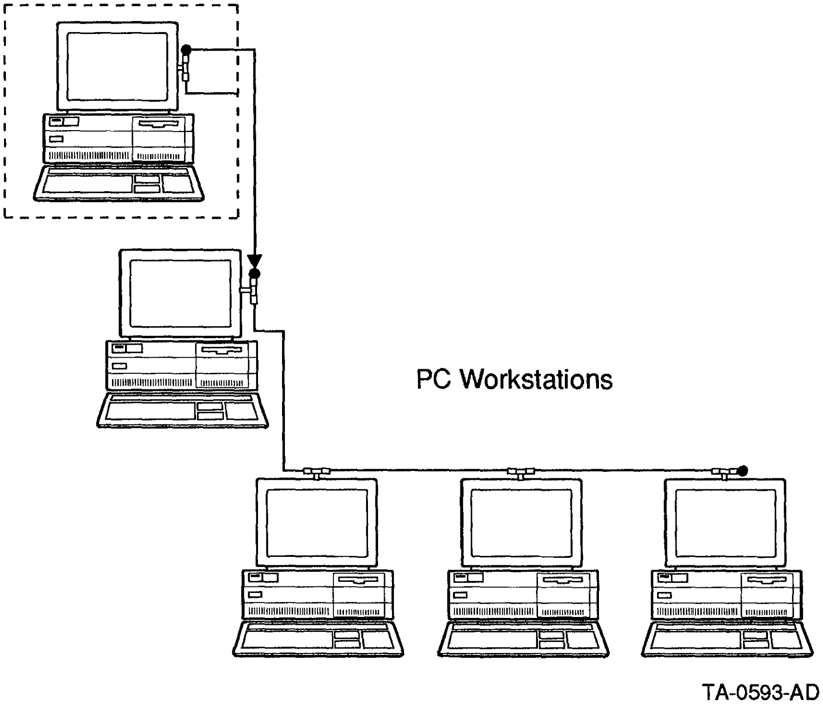
To troubleshoot a problem on an Ethernet cable, follow the instructions for either the Daisy Chain or the Digital ThinWire Ethernet Multiport Repeater (DEMPR) configuration segment tests. Before doing either test, make sure that the server is cabled to the network correctly.

Daisy Chain Segment Test (DECnet)

Starting at the end of an Ethernet segment:

1. Remove the terminator from the end of the chain.
2. Insert the terminator at the next T-connector (Figure 2–15).
3. Run the Client Loopback Test on the last node in the chain.
4. Run the appropriate server troubleshooting test from the server node to the last node.
   - If successful, the segment removed was bad. Replace that segment and retest. (A bad T-connector or terminator can cause a problem.)
   - If failure still occurs, return to step 1 above. Repeat these steps until you find the bad segment or network component.

Figure 2–15 Checking Daisy Chain Configuration Segments



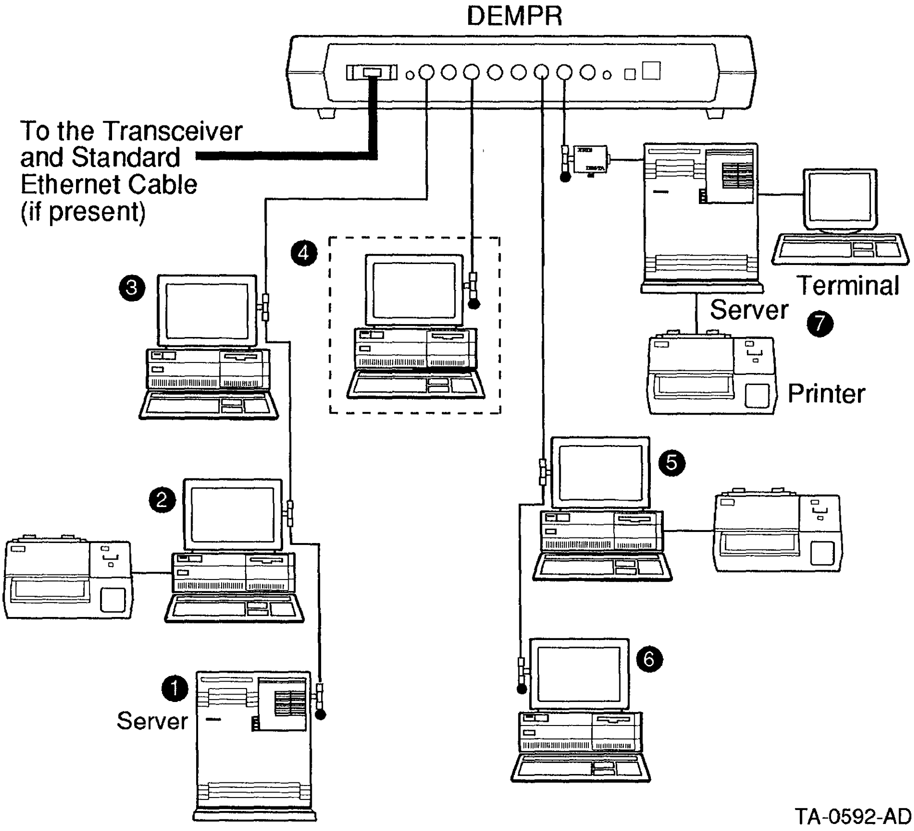
Daisy Chain Segment Test Completion (DECnet)

The Daisy Chain Segment Test is complete.

DEMPR Configuration Segment Test (DECnet)

Refer to the Ethernet example shown in Figure 2–16 to perform the test.

Figure 2–16 Checking DEMPR Configuration Segments



From the point of failure (node 4) to node 1:

1. Reset the DEMPR if any lights are on or blinking.
2. Follow the daisy chain segment test for nodes 1, 2, and 3.
3. Use the following DEMPR segment test:
   - Remove the connection from the DEMPR port for the failing segment (in this example, node 4).
   - Connect the failing segment to another DEMPR port.
   - Run the Client Loopback Test and the Client Remote Boot Procedure on this node (node 4).

- Reset the DEMPR to make sure that the segment is not disconnected. If the light remains on or blinking after the reset, the segment is not properly connected.
- Run the appropriate server troubleshooting test from node 1 to node 4, which is now connected to a new port.
  - If successful, reconnect the segment to the original port and retest. If this is successful, resetting the cable connections and the DEMPR may have fixed the problem. If this fails, the original port is faulty. Replace the bad component.
  - If the new port fails, replace the cable between the client and the DEMPR and retest. If successful, then the original cable was faulty. If the test fails, the DEMPR has a hardware failure. You can test other DEMPR ports or contact your authorized service representative.

DEMPR Configuration Segment Test Completion (DECnet)

The DEMPR Configuration Segment Test is complete.

Network Connection Procedure Completion (DECnet)

The Network Connection Procedure is complete.

Network Segment Interface Procedure (DECnet)

This procedure verifies that the nodes on an Ethernet network segment can communicate on the network segment and that the network segment interface is suspect.

If two or more nodes are daisy chained on a network segment, disconnect the end of the ThinWire nearest the network segment interface and install a terminator. Using the appropriate loop test (server to server, client to client, or client to server), do a loop test between the two nodes at either end of the segment.

If the loop test is successful, the network segment interface, H4000, DEMPR, or DEREP, is probably faulty. If you have a similar component elsewhere in the network, try temporarily substituting the similar component for the suspect unit.

If the loop test fails, check the terminators at both ends of the network segment. If no problem is observed, disconnect one of the tested nodes and move the terminator to the new end of the segment. Repeat the loop test between the two nodes at either end of the segment. Continue this process until the loop test is successful or until only two nodes remain.

If, after removing a node, the loop test is successful, the removed node is probably faulty.

If the loop test failed and you are down to two nodes, try connecting and testing, in turn, each of the two remaining nodes with a third node. If one loop test completes successfully, the remaining node is probably faulty.

Network Segment Interface Procedure Completion (DECnet)

The Network Segment Interface Procedure is complete.

3

DECnet Messages

This chapter discusses common network problems. It presents the problems according to the symptom each problem displays. A symptom can be a displayed message (such as the DECnet event message, "Aborted Service Request"), or a description of the problem situation (such as, "LAN Bridge Cannot Downline Load").

Following each symptom is an explanation of why the problem occurs, a brief description of the troubleshooting strategy for the problem, a troubleshooting procedure that gives step-by-step instructions for solving the problem, and general recommendations.

The step-by-step procedures do not present a complete methodology for solving the problems. Instead, they provide the *most likely* solutions for the problems—the solutions to try first.

Organization

The network problems discussed in this chapter are organized alphabetically according to the symptom message or problem description. PC-based messages are listed at the end of this chapter in alphabetical order.

The explanation section for each problem gives the reasons for the problem and describes the extent of the problem. Table 3–1 categorizes the problems according to the extent of their disturbance on the network, as follows:

- ULTRIX host problems
- VMS node problems
- LAN problems
- WAN problems
- Cross-category problems (two or more of the preceding problems)

Table 3–1 also includes the protocol involved in each problem.

Table 3–1 Network Problems and Extent of Disturbance on the Network

Extent of Problem	Protocol	Symptom or Problem Description
ULTRIX Host	DECnet	Connect Failed, Access Control Rejected
ULTRIX Host	DECnet	Connect Failed, Unrecognized Object
VMS Node	DECnet	Device Not Mounted
VMS Node	DECnet	Insufficient Resources at Remote Node
VMS Node	DECnet	Invalid Parameter Value
VMS Node	DECnet	Line Synchronization Lost
VMS Node	DECnet	Login Information Invalid
VMS Node	DECnet	Network Object Unknown
VMS Node	DECnet	Network Partner Exited
VMS Node	DECnet	Node Out of Range Packet Loss
VMS Node	DECnet	Partial Routing Update Loss
VMS Node	DECnet	Verification Reject
LAN	DECnet/MOP	Aborted Service Request
LAN	DECnet	Adjacency Rejected, Adjacency Up
LAN	Generic	Babbling Device
LAN	Generic	Broadcast Storm
LAN	DECnet/MOP	LAN Bridge Cannot Downline Load
LAN	Generic	LAN Segment Communication Problem
WAN	DECnet	Asynchronous DECnet Problems
WAN	DECnet	Partitioned Area
Cross-category	DECnet	Circuit State Problems
Cross-category	Generic	Dialup Problems
Cross-category	DECnet	Remote Node Is Not Currently Reachable

Troubleshooting Notes

Keep the following in mind as you begin troubleshooting network problems:

For VMS Systems

- Using privileged accounts

  Many of the procedures in this chapter require the use of an account with system management level privileges. Many procedures also assume that you have access to accounts with these privileges on all nodes in your network. For procedures requiring use of a privileged account on a node to which you do not have access, ask the system manager of that node to perform the action.

- Using the SET and DEFINE commands in NCP

  Many procedures call for setting NCP parameters with the SET command, which modifies only the volatile database. After you verify that the solution for a problem works, be sure to use the DEFINE command to modify the permanent database.

- Modifying passwords

  Some procedures call for correcting mismatches between passwords specified in the SYSUAF file and NCP databases. Before you make any changes, be sure that you have the authority to make the modifications. If you do not have the authority to do so, refer the required change to the appropriate system or network manager.

For ULTRIX Systems

- Modifying passwords

  Some procedures call for correcting mismatches between passwords specified in the /etc/passwd file and NCP object databases. Before you make any changes, be sure that you have the authority to make the modifications. If you do not have the authority to do so, refer the required change to the appropriate system or network manager.

Aborted Service Request

Symptoms

With the local Ethernet circuit service state enabled, the system displays one of the following DECnet event messages:

```
%%%%%%%%%%%   OPCOM  5-OCT-1990 13:48:07.73   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 0.7, aborted service request
From node x.xxx (NODE1), 5-OCT-1990 13:48:07.73
Circuit UNA-1, Line open error,  . . .

%%%%%%%%%%%   OPCOM  5-OCT-1990 13:48:07.73   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 0.7, aborted service request
From node x.xxx (NODE1), 5-OCT-1990 13:48:07.73
Circuit UNA-1, Receive timeout,  . . .
```

Explanation

These messages indicate a LAN problem involving DECnet and the Maintenance Operation Protocol (MOP). The problem can affect any load host system. A load host system is any system that provides downline loading and upline dumping for other systems.

Generally, this symptom results from a node requesting a service from an adjacent node. However, a problem prevents the request from being processed at the adjacent node.

A. In the case of the *line open error* message, the Network Management Listener (NML) on the adjacent node receives a MOP message, but is unable to acquire control of the line. NML on the adjacent node scans the node database, but is unable to locate a matching hardware address for the requesting node.

   A load host system can be set up to allow loading for some systems and not for others. If a node is receiving requests when it is not set up to load other systems (for example, when it does not have the appropriate files), you can disable loading or just ignore any inappropriate load requests.

   Finally, if the adjacent node is not intended to receive MOP requests but is still receiving requests, the adjacent node may be set up improperly to prevent these requests. You can disable loading or ignore the aborted service request messages.

Note

Before you take any action on this problem, determine the intended use of the adjacent node.

If the adjacent node is intended to load other nodes, the line open error message can be caused by any of the following:

- Incorrect information in the adjacent node's volatile node database regarding the node that is requesting the operation

  Some devices, such as the DECserver 100s and DECserver 200s do not have to be defined in the NCP database on the load host. However, other devices, such as DECserver 500s, DECSAs, DECrouters, and MicroVAX systems must be defined.

  Some of the information that is commonly missing from or incorrect in the volatile node database includes the following:

  - Hardware address
  - Ethernet address
  - Load file
- Improper protection on the load file, or a nonexistent load file
- Problems with the load image

  For example, the load image may not exist or it may not be readable. Also, if secondary and tertiary files are required, they may not exist or be readable.

B. In the case of the *receive timeout* message, one of the following is occurring:

- The line message receive timer expires before the request can be received from the adjacent node.
- If another node is set up as a load host system for the same server, and the other node services the request first, the remaining load host system receives the receive timeout message. This may not be a problem.

Aborted Service Request

These situations can be caused by any of the following:

- The service timer on the local node is too short.
- The line error level on the load host is too high for any message to get through.
- A hardware problem exists with the node being loaded.

  For example, there might be a problem with a QNA.
- A problem exists with the path to the node being loaded.

Troubleshooting Strategy

A. To resolve the line open error message problem, you may need to perform some or all of the following steps:

- If the node receiving the load requests is not intended to load other nodes, disable loading on the node receiving the requests.
- Check the local node's node definitions for the requesting node, and update them, if necessary.
- Check the load file's existence, file protections, and logical name definitions.
- If secondary and tertiary load files are required, check their existence, file protections, and NCP definitions.

B. To resolve the receive timeout message problem, you may need to perform some or all of the following steps:

- Perform hardware tests on the node being loaded.
- Check for problems on the path.
- Check the service timer and increase it, if necessary.
- Check the line error level on the load host.

Troubleshooting Procedure

A. To resolve the line open error message problem, do the following:

Note

Step 1 turns the circuit off and causes users to lose connections.

1. If the local node is *not* intended to load other nodes, use the following commands to disable loading on the local node:

```
NCP>  DEFINE CIRCUIT circuit-id SERVICE DISABLED
NCP>  SET CIRCUIT circuit-id STATE OFF
NCP>  SET CIRCUIT circuit-id ALL
```

2. Use the following NCP command on the node receiving the request to make sure that its volatile node database contains correct information for the requesting node:

```
NCP>  SHOW NODE remote-node-id CHARACTERISTICS
```

3. If the requesting node is not defined in the receiving node's volatile node database, or if it is incorrectly defined, use the following command to define it:

```
NCP>  SET NODE nodename ADDRESS address SERVICE-
_NCP>  CIRCUIT ethernet-device HARDWARE ADDRESS-
_NCP>  ethernet-address LOAD FILE file specification
```

4. Use the following DCL command to check whether the load file exists and, if so, whether it has WORLD:READ access specified:

```
$  DIRECTORY/PROTECTION filename.ext
```

5. If the file protection on the load file does not include world read privilege, use the following command to set W:R protection on the file:

```
$  SET PROTECTION filename.ext/PROTECTION=(W:R)
```

6. If the requesting node is a DECserver, make sure the logical name definition, MOM$LOAD, is defined to point to the directory where the load file is located:

```
$  DEFINE/SYSTEM/EXECUTOR MOM$LOAD directory_specification
```

7. If the requesting node requires secondary or tertiary load files, run NCP and use the following command to check whether the files are defined in the node database:

```
NCP>  SHOW NODE node-id CHARACTERISTICS
```

8. If the files are not defined in the node database, use the following command to define them:

   ```
   NCP> SET NODE node name SECONDARY LOADER file -
   _NCP> specification, TERTIARY LOADER file specification
   ```

9. If secondary or tertiary load files are required, make sure the file protection on these files includes WORLD:READ access.

B. **To resolve the receive timeout message problem, do the following:**

1. Use appropriate hardware tests to determine if a problem exists with the node being loaded.

2. If a problem exists with the path to the node being loaded, see resources routine procedures for information on resolving path problems.

   The problem may be a LAN segment problem such as one caused by a bridge or repeater. You may need to refer to other LAN problems described in this chapter, such as "LAN Segment Communication Problem" and "Babbling Device."

3. Check the current value of the service timer on the line using the following NCP command:

   ```
   NCP> SHOW LINE line-id CHARACTERISTICS
   ```

4. If the value for the service timer is too low, increase it using the following NCP command:

   ```
   NCP> SET LINE line-id SERVICE TIMER milliseconds
   ```

5. Use the following commands to display the load host's line error level:

   ```
   NCP> SHOW LINE line-id COUNTERS
   NCP> SHOW CIRCUIT circuit-id COUNTERS
   ```

   High error rates can indicate that the load host is unable to load devices. Perform loopback tests on the devices to see if the devices have a problem.

Adjacency Rejected/Adjacency Up

Symptoms

A node repeatedly displays the following DECnet event messages:

```
%%%%%%%%%%%   OPCOM  27-JUN-1990 09:32:32.98   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.16, adjacency rejected
From node x.xxx (NODE1), 27-JUN-1990 09:32:32.82
Circuit BNT-0, Adjacent node = y.yyy (NODE2)

%%%%%%%%%%%   OPCOM  27-JUN-1990 09:32:32.93   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.15, adjacency up
From node x.xxx (NODE1), 27-JUN-1990 09:32:32.83
Circuit BNT-0, Adjacent node = z.zzz (NODE3)
```

This symptom can be accompanied by application error messages such as "Path to network node lost." This problem is also known as a bouncing circuit.

Explanation

These messages indicate a LAN problem involving the DECnet routing layer. The problem results from conflicts between the designated routing node on the LAN and another routing node on the LAN.

A LAN can consist of multiple DECnet areas, and each DECnet area on a LAN has a designated routing node. Each routing node broadcasts its designated router status across the LAN. However, one of the routing nodes (usually the one that is not the designated routing node) has a hardware problem that causes it to have inaccurate routing information.

This problem tends to occur on QNA systems used as routing nodes. With these systems, a receiver lockup can occur, causing the QNA system to send but not receive routing information. As a result, the QNA system does not get the correct routing information.

Troubleshooting Strategy

To solve this problem, determine the routing node or nodes that are causing the problem, check that the cables are secure, and check for hardware problems on the routing nodes.

Adjacency Rejected/Adjacency Up

Troubleshooting Procedure

1. **Look at the OPCOM messages on a system console on one of the end nodes in the LAN. The alternating messages "Adjacency rejected" and "Adjacency up" include the name of the routing nodes causing the problem.**
2. **Make sure that the cable connections for the problem routing node are secure.**
3. **Run NCP on the problem routing node, and use the following command to check whether the problem routing node has a hardware problem:**

   ```
   NCP>  SHOW KNOWN CIRCUITS
   ```

   If NCP does not list adjacencies, then the board in this system is probably faulty. In this case, shut down the network on this system using the following command:

   ```
   NCP>  SET EXECUTOR STATE OFF
   ```

4. **Run diagnostics on the Ethernet interface board to determine the cause of the hardware failure.**

Recommendations

Be sure that you define a designated routing node for your LAN. If possible, the routing node should only process routing requests. This is because routing can create a high traffic load on the designated routing node. If the designated routing node is also used for other user activities, response time may suffer.

Some additional guidelines for routing node setup include the following:

- Define the designated routing node's routing priority as 127, and all others lower.
- Define a backup designated router for each LAN.
- Define the backup routing node's routing priority as 126.
- Give the designated routing node the highest DECnet address in its DECnet area.

  You do this because designated router status in a LAN defaults to the node with the highest DECnet address in the LAN if two nodes have the same routing priority.

Asynchronous DECnet Problems

Symptoms

An asynchronous DECnet connection cannot be created. The circuit is either never established or it is established, but is in an on-starting or on-synchronizing state.

Explanation

This symptom indicates a WAN problem because it involves a point-to-point circuit. Both static and dynamic asynchronous DECnet can be used in a dedicated circuit, hardwired, or dialup environment. This example assumes that the circuit is a dialup circuit.

Two types of asynchronous DECnet exist: static and dynamic. Static asynchronous DECnet is a connection that allows only DECnet traffic. Dynamic asynchronous DECnet allows both DECnet or simple asynchronous connectivity to occur as needed.

Troubleshooting Strategy

Most asynchronous DECnet problems are the result of improper setup or installation of various devices. Solving this problem requires that you address three potential problem areas:

A. The system software, which may require that you install additional software and set up system parameters properly:

   For example, for both dynamic and static asynchronous DECnet, the following need to be properly set up on a VMS system:

   - The asynchronous DDCMP driver needs to be loaded into memory.
   - The terminal characteristics need to be properly set.

B. The DECnet software, which may require that you adjust certain network definitions.

C. The communications link, which may require that you address dialup problems.

In troubleshooting this problem, use dynamic asynchronous DECnet if possible. Dynamic asynchronous DECnet allows you to establish a connection to a remote node, which shows that data can flow between the two points. This proves that the communication link is operating properly and the system setup is correct.

Asynchronous DECnet Problems

If you use hardwired or dedicated circuits, use static asynchronous DECnet, and treat this as a circuit problem, solving the problem with loopback tests at the appropriate location. See NCP LOOPBACK and "Circuit State Problems," in this chapter for more information.

Troubleshooting Procedure

A. **Check the system software, using the following steps:**

1. For both dynamic and static asynchronous DECnet, do the following to install the asynchronous DDCMP driver into memory:

   a. Enable privileges on your process using the following command:

   ```
   $ SET PROCESS/PRIVILEGES=ALL
   ```

   b. Use the following command to check whether the driver is installed:

   - For static asynchronous DECnet, check the system response for the NOA0 device ❶ as shown in Example 3–1.
   - For dynamic asynchronous DECnet, check the system response for the VTA0 device ❷ as shown in Example 3–1.

   ```
   $ MCR SYSGEN
   SYSGEN> SHOW/DEVICE
   ```

   c. If SYSGEN does not display the NOA0 device, use the following command to install it:

   ```
   SYSGEN> CONNECT NOA0/NOADAPTER
   ```

2. Perform the following step for dynamic asynchronous DECnet only. Otherwise, go to step 3.

   Use the following commands to install DYNSWITCH and VIRTUAL terminals:

   a. Do the following on both nodes:

   ```
   $ INSTALL:=$SYS$SYSTEM:INSTALL
   $ INSTALL/COMMAND
   INSTALL> CREATE SYS$LIBRARY:DYNSWITCH/SHARE-
    INSTALL> /PROTECT/HEADER/OPEN
   INSTALL> EXIT
   $
   ```

Example 3–1 SYSGEN SHOW/DEVICE Display

```
__Driver_____Start____End___Dev___DDB______CRB______IDB_____Unit__UCB____
NODRIVER    80271680 80274E60
                            NOA❶ 803D5C40 803BF1C0 803DF480
                                                              0 8026E930
LTDRIVER   80269600 8026DA60
                            LTA 803DBFA0 803C0710 803BFCC0
                                                              0 80265050
                                                              1 80265320
                                                              4 8026FBE0
CTDRIVER   80262C90 80264A50
                            RTB 803D1C20 803BBB70 803D1E60
                                                              0 80243F00
RTTDRIVER  80262150 80262C90
                            EIGHT 803D2F40 803BD0C0 803CFEE0
                                                              0 80243230
                                                              0 8026E930
   .
   .
   .
RTTDRIVER  80255860 8025B739
                            VTA❷ 803D0EA0 803C16E0 803CF520
                                                              0 80227C00
   .
   .
   .
SYSGEN>
```

b. To install virtual terminals do the following on both nodes:

```
$ MCR SYSGEN
SYSGEN> CONNECT VTA0/NOADAPTER/DRIVER=TTDRIVER
SYSGEN> EXIT
$
```

3. Set the terminal port characteristics correctly.

Note

This example assumes a dialup connection.

a. For nondialup connections, remove the MODEM and NOHANGUP parameters.

b. For static asynchronous DECnet, execute the following command to insure the terminal characteristics are set up properly.

```
$ SET TERMINAL/PERMANENT/PROTOCOL=DDCMP/NOTYPE_AHEAD/MODEM-
_$ /NOHANGUP/EIGHT_BIT/NOAUTOBAUD/SPEED=xxx TTA0:
```

c. For dynamic asynchronous DECnet, execute the following command to insure the terminal characteristics are set up properly.

```
$ SET TERMINAL/PERMANENT/NOTYPE_AHEAD/MODEM/DISCONNECT-
_$ /EIGHT_BIT/NOAUTOBAUD/SPEED=xxx tta0:
```

B. **Check the DECnet software to make sure that the circuit is set up properly in NCP.**

1. For *static asynchronous DECnet* only, run NCP and display the characteristics with the following command:

```
NCP> LIST LINE tt-0-0 CHARACTERISTICS
NCP> LIST CIRCUIT tt-0-0 CHARACTERISTICS
```

2. Use the following command to set the line state, receive buffers (4 is the recommended default), and line speed:

```
NCP> DEFINE LINE tt-0-0 STATE on RECEIVE BUFFERS 4-
_NCP> LINE SPEED 2400
```

3. Set the circuit state on using the following command:

```
NCP> DEFINE CIRCUIT tt-0-0 STATE ON
```

C. **Make sure the communications link is functioning properly.**

1. For dialup problems, see "Dialup Problems" in this chapter.

Note

Modems that perform automatic error correcting often do not work with asynchronous DDCMP lines. If a line works without DECnet but fails when you start DECnet, check to see if the modem error correcting is enabled, and turn this option off if possible.

2. For systems that are hardwired, or directly cabled, or both, set the circuit state on, and perform loopback tests as follows:

- For static asynchronous DECnet, execute the following commands:

```
NCP> SET CIRCUIT tt-0-0 all
NCP> LOOP CIRCUIT tt-0-0
```

  The loopback test shows if a bad cable, modem, circuit, or device exists.

- For dynamic asynchronous DECnet, first, use the following command to temporarily make the line a static asynchronous DECnet line for the loopback testing:

```
$ SET TERMINAL/PERMANENT/PROTOCOL=DDCMP/NOTYPE_AHEAD-
_$ /MODEM/NOHANGUP/EIGHT_BIT/NOAUTOBAUD/SPEED=xxxx TTA0:
```

Then, run NCP and use the following commands to set the line and circuit characteristics and perform loopback testing:

```
NCP>  SET LINE tt-0-0 STATE on RECEIVE BUFFERS 4 LINE SPEED 2400
NCP>  SET CIRCUIT tt-0-0 STATE on
NCP>  LOOP CIRCUIT tt-0-0
```

For more information, also see Circuit State Problems in this chapter.

Babbling Device

Symptoms

Users perceive very slow response time for network operations.

Explanation

This symptom indicates a LAN problem. A device on the network has a hardware problem, causing it to send out large amounts of data to the local area network. Such a device is called a **babbler** or **babbling device.**

Troubleshooting Strategy

To solve this problem, determine the LAN segment on which the babbling device exists, and the physical location of the babbling device on that segment. After you determine the location of the device, use hardware diagnostic techniques to determine the cause of the problem.

Troubleshooting Procedure

A. **Determine the physical location of the babbling device using LTM or DECelms. If LTM or DECelms are not available at your site, go to step C.**

1. If your site uses LTM, use the menus to determine the physical address of the babbling device.

   Under the heading Top Ten Talkers, LTM displays the addresses of the devices it recognizes that are generating the most traffic. After you have the physical address of the babbling device, you can use DECelms to determine the physical location of the babbling device.

Note

LTM displays only the addresses of devices it recognizes. If the babbling device is generating corrupt information (such as a long stream of preamble) for its own name and address, you may have trouble determining the physical address or location. In this case, you can use LTM to capture bad packets. Using the information on bad packets, you may be able to deduce the address of the problem device.

If you cannot determine the address of the babbling device using LTM, go to step 3.

---

2. If your site uses DECelms, and you know the physical address of the babbling device, do the following to locate the physical location of the babbling device:

   1. Run DECelms and examine the node's address in the bridge's forwarding database using the following commands:

      ```
      ELMS> USE bridge-id
      ELMS> SHOW ADDRESS node-address
      ```

      DECelms displays the last line to recognize communication from the physical address specified.

   2. To further isolate the location of the babbling device, use the following command on the next bridge to display the line on that bridge that last saw the physical address.

      ```
      ELMS> USE bridge-id
      ELMS> SHOW ADDRESS node-address
      ```

   3. Continue querying the bridges in this way until you isolate the babbling device to a specific LAN on the network.

B. **After you determine the LAN segment on which the problem device is located, do the following:**

   1. Ask users on that segment if there have been any new devices added to the LAN, or if they have been having any problems with devices on the LAN.

   2. Check these devices for correct operation.

   3. Ask the system manager of the system causing the problem to disconnect the faulty device.

C. **If you do not have LTM or DECelms at your site, or if you cannot determine the physical address of the babbling device, trace the problem to the babbling device by using the following steps:**

1. Collect information on the amount of data transferred from and received by each node in the network for a given time.
2. Compare the data for all the systems.
3. Use an Ethernet scope or LAN analyzer to determine the source of the problem, or disconnect each individual node until you find the babbling device.

   Start disconnecting nodes that are losing connections and having significant performance problems across all protocols.

Broadcast Storm

Symptoms

Only the host computers having the highest performance CPUs and Ethernet controllers can gain access to the network. Host response time becomes slow and utilization percentage becomes very high. In the DECelms Line Counters display, the Transmit Multiple Collisions and Collision Limit Exceeded values become very high. The LAN utilization percentage values displayed by the LAN Bridge 200 Line Monitor and LAN Traffic Monitor (LTM) rise toward 100 percent.

Explanation

This symptom indicates a LAN problem. Hosts may be using protocols that overuse the Ethernet broadcast address. By default, the bridges are required to pass these messages to every segment in the network, even to segments where there is no possible recipient. Every host in the network must read all the frames sent to the broadcast address.

Causes of broadcast storms include:

- Protocol problems — Certain protocols rely on the use of the Ethernet broadcast address instead of using multicast addresses, for example, ARP broadcasts.
- Configuration problems — Many different versions of both 4.2BSD and 4.3BSD UNIX, and many vendor's operating systems based on these different versions exist. Some operating systems perform differently from other operating systems when they receive broadcast packets they do not recognize as broadcasts. The different ways operating systems handle broadcast packets can cause problems.

  For example, when hosts using 4.3BSD UNIX are placed in a network of 4.2BSD UNIX hosts, a major "ARP storm" often occurs. The 4.2BSD hosts have gateway software enabled by default and consider any IP broadcast address other than zeros as an unknown address. When a 4.3BSD host using the new broadcast address of ones is added to the network, the 4.2BSD hosts simultaneously broadcast an ARP lookup request whenever the new 4.3BSD host uses the IP broadcast address of ones. The resulting broadcast storm can have a crippling effect on network performance.

Broadcast Storm

Troubleshooting Strategy

Follow this strategy to troubleshoot a broadcast storm:

1. Determine the protocol that is causing the storm.
2. Contain the problem by adding filters for the protocol in all the LAN Bridge 200 models.
3. Identify the segment where the storm originated and resolve the problem.

Troubleshooting Procedure

To troubleshoot a broadcast storm, follow these steps:

A. **Use LAN Traffic Monitor (LTM) to determine the protocol that is causing the broadcast storm.**

   1. From the LTM Main Menu, select #2, Node, Type and Multicast Traffic Displays.
   2. From the Node, Type and Multicast Traffic Displays Menu, select #4, Multicast Traffic by Type Display. LTM prompts you for a multicast address.
   3. Enter the broadcast address, FF-FF-FF-FF-FF-FF. LTM displays the following:

```
MC Address : FF-FF-FF-FF-FF-FF  Broadcast    Type Count : 3

Type Field 06-00 Xrx_NSIDP   Frame Count  2820      7.51%
Type Field 08-00 DOD_TCPIP   Frame Count 10272     14.09%
Type Field 08-06 TCPIP_ARP   Frame Count 10272  ❶ 67.41%
```

   In this case, the broadcast storm is caused by TCP/IP, which has the Protocol Type 08-00, and by the Address Resolution Protocol (ARP), which is used by TCP/IP for locating addresses. ARP has the Protocol Type value 08-06. According to the display, ARP is generating 67.41% ❶ of the broadcast traffic on the network.

B. **Contain the problem by adding filters for the Protocol Types 08-00 and 08-06 to the protocol databases of the LAN Bridge 200 models using DECelms. These filters instruct the bridges to filter (discard) frames that contain TCP/IP or ARP protocol information. The effect is to isolate the broadcast storm as much as possible, perhaps even to a single segment, if a LAN Bridge 200 connects the segment where the broadcast storm originated.**

   1. If the LAN Bridge 200 models do not have a password set, enter the following commands:

```
ELMS> USE KNOWN BRIDGES
ELMS> ADD PROTOCOL 08-00 DISPOSITION FILTER
ELMS> ADD PROTOCOL 08-06 DISPOSITION FILTER
```

2. If the LAN Bridge 200 models have the same password, enter the following commands, where *password* is the password:

   ```
   ELMS> USE KNOWN BRIDGES
   ELMS> ADD PROTOCOL 08-00 DISPOSITION FILTER PASSWORD password
   ELMS> ADD PROTOCOL 08-06 DISPOSITION FILTER PASSWORD password
   ```

3. If the LAN Bridge 200 models have different passwords, repeat the following commands for each bridge, where *bridge-name* is the name of the bridge and *password* is its password:

   ```
   ELMS> USE bridge-name
   ELMS> ADD PROTOCOL 08-00 DISPOSITION FILTER PASSWORD password
   ELMS> ADD PROTOCOL 08-06 DISPOSITION FILTER PASSWORD password
   ```

4. Because LAN Bridge 100 and LAN Bridge 150 models do not support protocol filtering, you must instruct these bridges to filter frames sent to the broadcast address by entering the following commands, where *bridge-id* is the name of the target bridge. If the target bridge is a LAN Bridge 150 that has a password set, you must include PASSWORD and the bridge's password.

   ```
   ELMS> USE bridge-id
   ELMS> ADD ADDRESS FF-FF-FF-FF-FF-FF DISPOSITION FILTER-
   _ELMS> PASSWORD password
   ```

C. **Locate the segment where the storm originated and resolve the problem.**

1. From the LTM Main Menu, select #2, Node, Type and Multicast Traffic Displays.

2. From the Node, Type, and Multicast Traffic Displays Menu, select #6, List of Nodes Using Protocol Type. LTM prompts you for a Protocol Type value.

3. Enter 08-00 or 08-06 to display a list of the hosts using TCP/IP or ARP. LTM displays the addresses of the hosts using the protocol.

4. Follow the procedure described in the Babbling Device example to find the segment where the broadcast storm originated.

5. Resolve the problem, or at least ensure that it is isolated to a single segment. If the bridge connecting the segment is a LAN Bridge 200, enter the following commands to ensure that it has the appropriate protocol entries in its protocol database.

   ```
   ELMS> USE bridge-id
   ELMS> SHOW PROTOCOL 08-00
   ELMS> SHOW PROTOCOL 08-06
   ```

If the bridge connecting the problem segment is a LAN Bridge 100 or LAN Bridge 150 model, ensure that the bridge has an entry for the broadcast address in its forwarding database:

```
ELMS>  USE bridge-id
ELMS>  SHOW MULTICAST ADDRESS FF-FF-FF-FF-FF-FF
```

D. **Finally, remove any unnecessary protocol or address entries that you added when you were first trying to contain the problem.**

The following commands remove a protocol entry from the protocol database of a LAN Bridge 200:

```
ELMS>  USE bridge-name
ELMS>  REMOVE PROTOCOL 08-00 PASSWORD password
```

The following commands remove an address entry from the forwarding database of a bridge. (You do not need to include the password if the target bridge is a LAN Bridge 100 model or if it does not have a password set.)

```
ELMS>  USE bridge-id
ELMS>  REMOVE ADDRESS FF-FF-FF-FF-FF-FF PASSWORD password
```

Recommendations

- You can minimize broadcast storms by adding protocol filters to isolate protocols that misuse the broadcast address. Use LTM and DECelms to study the protocols used on each segment in your extended LAN and use filters to contain protocols to the LAN segment where they are used. (You can do the same for multicast addresses also.)

  For example, if one segment in an extended LAN supports a classroom of nodes using AppleTalk, you can add a protocol entry for AppleTalk with the disposition FILTER in the bridge connecting the segment. The filter prevents the AppleTalk broadcasts from entering the extended LAN, where there are no nodes using AppleTalk. This prevents the broadcasts from taking up valuable network bandwidth and host processing power.

- Because of the potential problems caused by the different ways operating systems handle broadcast packets, make sure that you install recent releases of the respective operating systems on your network. If you cannot upgrade a system, see an expert about possibly creating a patch to prevent potential broadcast storms.

Circuit State Problems

Symptoms

The system displays one of the following messages when you use the NCP command, SHOW CIRCUIT circuit-id:

```
NCP>  SHOW CIRCUIT circuit-id
Circuit on-starting
Circuit on-synchronizing
Circuit off-synchronizing
```

Explanation

This symptom indicates a DECnet-VAX node problem that sometimes manifests itself as a LAN or WAN problem initially.

A. Circuit on-starting is generally a normal condition indicating that the circuit is ready to begin a node initialization sequence. Circuit on-starting is only a problem if an adjacent node is connected, or should be connected to the circuit that is on-starting.

   When it is not a normal condition, circuit on-starting indicates a problem with point-to-point (non-Ethernet) links, including any of the following:

   - The remote node is not running.
   - The line is not connected, or there is a bad connection on the cables for the devices.
   - The modem is not running.
   - The circuit on the remote node is in the OFF state.

B. Circuit on-synchronizing means the node initialization sequence between two adjacencies is failing, and usually indicates a routing-related problem. Generally, circuit on-synchronizing can be caused by any of the following:

   - DECnet event 4.2, Node out-of-range packet loss
   - DECnet event 4.3, Oversized packet loss
   - DECnet event 4.6, Verification reject
   - The circuit is ON and the executor state is OFF
   - The circuit is ON and the line is OFF

C. Circuit off-synchronizing indicates a hardware problem.

Circuit State Problems

Troubleshooting Strategy

A. For circuit on-starting, do the following:

   1. Check the configuration.
   2. Check that the remote node is running, and its lines and circuits are on.
   3. Check that the local node's lines are on.
   4. Use loopback tests.

B. For circuit on-synchronizing, do the following:

   1. Enable event logging.
   2. Check for class 4 DECnet events, and correct as described in step B.
   3. Make sure that the executor state is on.
   4. Make sure that the lines and circuits are on.

C. For circuit off-synchronizing, check the device hardware manuals to resolve the hardware problem.

Troubleshooting Procedure

A. **For circuit on-starting problems, do the following:**

   1. Check the configuration that should exist.
   2. Check with the system manager of the remote node to see if the system is running, and if the circuits and lines are turned on.
   3. Run NCP and use the following command to make sure that the local lines are turned on:

      ```
      NCP>  SHOW KNOWN LINES
      ```

   4. If the local lines are not on, use the following NCP command to turn them on:

      ```
      NCP>  SET LINE line-id STATE ON
      ```

   5. Use loopback tests to determine where the physical problem exists.

      The problem could be at any one of many locations. Systematically work across the physical connection, looping back to test at successively more remote points, using the loopback tests described in resources routine procedures section.

- For controllers, use controller loopback tests.
- For distribution panels or cables, use a loopback connector.
- For modems, use modem local loopback tests.
- For communications lines, use modem remote loopback tests.

B. **For circuit on-synchronizing problems, do the following:**

1. Make sure that OPCOM is running, and use the following DCL command to enable event logging:

   ```
   $ REPLY/ENABLE=NETWORK
   ```

2. Check for class 4 DECnet events.

   - DECnet event 4.2, Node out-of-range packet loss, means that the remote node's address is greater than the local executor's MAXIMUM ADDRESS parameter. See "Node Out of Range Packet Loss" problem in this chapter, for more information on this problem.
   - DECnet event 4.3, Oversized packet loss, means that the routing layer discarded a packet because the packet was too large to forward to an adjacent node. The solution is to ensure that all nodes in the network have the same executor buffer size, then to stop and restart the network.

     ```
     NCP> DEFINE EXECUTOR BUFFER SIZE value
     NCP> SET EXECUTOR STATE OFF
     NCP> EXIT
     $ @STARTNET.COM
     ```

   - DECnet event 4.6, Verification reject, means that a problem exists with the transmit or receive passwords. The solution is to make sure that the transmit and receive passwords match. See "Verification Reject" in this chapter for more information on this problem.

3. If the circuit is on and the executor state is off, use the following NCP command to turn the executor state on:

   ```
   NCP> SET EXECUTOR STATE ON
   ```

4. Use the following command to restart DECnet, if necessary:

   ```
   $ @STARTNET.COM
   ```

5. If the circuit is on and the line is off, use the following NCP command to turn the line on:

   ```
   NCP> SET LINE line-id STATE ON
   ```

C. **If the circuit is off-synchronizing, the device has a hardware problem.**

Follow the procedures in the appropriate hardware manuals or refer the problem to Digital Services.

Connect Failed, Access Control Rejected

Symptoms

ULTRIX system users receive an error message such as the following when attempting any network operation:

```
connect failed, access control rejected
```

Explanation

This symptom indicates a DECnet-ULTRIX host problem involving the session layer. It can be caused by any of the following:

- Incorrect user-supplied access control information
- Incorrect proxy access set up
- Invalid account specified for the object
- Incorrect or nonexistent proxy database or proxy accounts
- Restricted proxy access on either the local or the remote host

Note

This message may not indicate a problem; the host may be restricting incoming network access for security reasons.

To troubleshoot this problem effectively, you need to understand the order of access control for DECnet-ULTRIX.

ULTRIX systems check first for explicit, user-supplied access control information. If user-supplied information does not exist, the ULTRIX system checks for proxy access information. If proxy access information does not exist, the ULTRIX system checks for default access information.

Note

NCP parameters determine the type of proxy access permitted, if any, for objects on a host or for the host itself. NCP information specified for an object always supersedes the executor information. This is true for proxy as well as default account information.

Connect Failed, Access Control Rejected

Proxy access for the executor is determined according to the parameters shown in Table 3–2.

Table 3–2 NCP Executor Proxy Access Parameters

Executor Parameter	Function
INCOMING PROXY DISABLED	Ignores all incoming proxy requests, and instead, relies exclusively on access control information supplied in the connect requests to validate the logical link.
INCOMING PROXY ENABLED	Invokes the appropriate proxy, based on the source user, source node, and supplied access control information, if any. This is the default.
OUTGOING PROXY DISABLED	Specifies that proxy login is not requested on any outgoing logical links.
OUTGOING PROXY ENABLED	Specifies that proxy login is requested on outgoing logical links. This is the default.

Troubleshooting Strategy

Before you attempt to solve this problem, do the following:

- Determine the type of access control the user specified when trying to access the remote host or node.
- Determine the objects the user tried to access.

A. For user-specified access control problems, do the following:

   1. Check the user-specified access control information.
   2. Make sure that the account the user wants to access exists on the remote host, and create one if appropriate.
   3. Modify the password information for the remote account.

B. For proxy access control problems, do the following on the source (local) and target (remote) hosts:

   1. On the source (local) host, make sure that PROXY OUTGOING is enabled.
   2. On the target (remote) host, do the following:
      a. Make sure that PROXY INCOMING is enabled.
      b. Make sure that the /etc/dnet_proxy file has the correct, case-sensitive entries.

c. Make sure that the local host is defined in the remote host's DECnet database.

C. For default access control problems, do the following:

1. If the requested object on the remote host has an account associated with it, check the /etc/passwd file to make sure that the account exists.
2. If the requested object on the remote host does not have an account associated with it, create an account for the object and modify the object to ensure that the object has an account associated with it.

Troubleshooting Procedure

A. **Before you try to solve this problem, do the following:**

Use the following list to help determine which step to use to solve the problem:

- If the user specified explicit access control information when trying to access the remote host, use step A to solve the problem.
- If the user tried to access the remote host using proxy access, use step B to solve the problem.
- If the user did not try to access the remote host using proxy access, use step C.
- If you do not know if the user tried to access the remote host using proxy access, use step B first, and continue with step C if necessary to solve the problem.

Note

To help solve this problem faster, you can try to connect to a different object on the remote host. If the connection succeeds when directed toward the new object, then the problem is probably object-specific and not related to proxy access. You can focus your efforts on ensuring that the object on the remote host is set up properly.

A. **For user-supplied, explicit access control problems, do the following:**

1. Try to log in to the remote host with the same access information the user tried. If you cannot log in to the host, the access information is probably incorrect.

2. Log in to an account on the remote host.
3. Log in to the superuser account.
4. Look at the password file, using the following command:

   ```
   # cat /etc/password
   ```

5. If the /etc/password file does not list the account the user tried to access, use the following command to add the account if a new account is appropriate:

   ```
   # adduser
   ```

   The adduser command prompts you for the following information about the new account for the new user:

   - Login name
   - Full name
   - Login group (default is [users])
   - Other groups
   - Parent directory (default is [/usr/users])
   - Password

   The adduser command adds the new user account to the /etc/password file, and sets up a home directory for the new user containing the files .cshrc, .login, and .profile.

Note

In ULTRIX versions prior to 4.0, the adduser command does not prompt for a password for the user, so be sure to use the passwd command to specify a password for the user if you want to prevent unauthorized access to the account.

6. If you are using an ULTRIX version prior to 4.0, use the following command to specify a password for the account, substituting the new user's password for newpassword:

   ```
   # passwd username
   New password:  newpassword
   Retype new password:  newpassword
   ```

   The characters you type for the new password are not dispıayed on the screen.

7. Try to log in to the user's account with the new password.

8. For proxy access control problems, do the following:
   a. On the source (local) host do the following:
      1. Log in to an account on the local host.
      2. Log in to the superuser account.
      3. Run ncp, and use the following command to display the executor characteristics and determine if proxy outgoing is enabled:

         ```
         ncp> show executor characteristics
         ```

      4. If proxy outgoing is not enabled, use the following ncp commands to enable it in both the volatile and permanent databases:

         ```
         ncp> set executor proxy outgoing enabled
         ncp> define executor proxy outgoing enabled
         ```

   b. On the target (remote) host, do the following:
      1. Run ncp, and use the following commands to display the executor characteristics and determine if proxy incoming is enabled:

         ```
         ncp> show executor characteristics
         ```

      2. If proxy incoming is not enabled, use the following ncp commands to enable it in the both volatile and permanent databases:

         ```
         ncp> set executor proxy incoming enabled
         ncp> define executor proxy incoming enabled
         ```

      3. Display or edit the /etc/dnet_proxy file to make sure that it has the correct, case-sensitive entries for the local host and user.
      4. If entries are missing from the /etc/dnet_proxy file or are incorrect, edit the /etc/dnet_proxy file, using the following format for the entries:

         ```
         source::user   local_user
         ```

      5. Run ncp and use the following commands to make sure that the source (local) host is defined in the volatile and permanent DECnet databases:

         ```
         ncp> set node hostname address aa.nnn
         ncp> define node hostname address aa.nnn
         ```

9. Do the following to resolve problems due to default access control information:
   a. Log in to an account on the remote host.

b. Run ncp, and use the following command to display the default user account:

```
ncp> show object object_name characteristics
```

c. If the object does not have an account associated with it, use the following command to create an account if a new account is appropriate:

```
# adduser
```

d. Run ncp, and modify the object using the following command:

```
ncp> set object object_name default user account_name
```

Connect Failed, Unrecognized Object

Symptoms

Users on an ULTRIX system receive the following message when trying to access a remote host:

```
connect failed, unrecognized object
```

Explanation

This is a DECnet-ULTRIX host problem involving the session layer on the remote host. The connect failed message occurs when the object requested is not defined in ncp, or if the requested object has file protection problems.

Troubleshooting Strategy

A. Check to see if the object is defined in ncp.

B. If the object is not defined, define it.

C. Check to see if the file specified for the object exists.

D. If the file for the requested object does not exist, create it.

E. Make sure that the protection specified for the file is correct.

Troubleshooting Procedure

A. **Run ncp and use the following command to see if the object is defined on the remote host.**

```
ncp> tell remote-node-id show known objects
```

B. **If the object is not defined, log in to the superuser account and run ncp to define the object using the following command and additional parameters as required:**

```
ncp> set object object-id
```

C. **If the object is defined, run ncp and use the following command on the remote host to see if the object has a file specified:**

```
ncp> tell remote-node-id show object object-id characteristics
```

D. **Use the following command to see if the file specified for the object exists.**

```
# ls -l
```

E. **If the file for the requested object does not exist, create the file.**

F. **Ensure that the protection on the specified file is correct. Generally, world execute access is required for most objects.**

1. Use the following commands to set the file protection:

   ```
   # chmod a+x /usr/etc/fal
   ```

2. Use the following commands to ensure that the directories above the file (including the root (/) directory) also have the correct file protection to allow access:

   ```
   # cd /usr
   # ls -ld etc
   # chmod a+x etc
   ```

Device Not Mounted

Symptoms

Users receive the following error message when attempting to perform any network operation:

```
Device not mounted.
```

Explanation

This is a DECnet-VAX problem related to the local node. When DECnet starts, SYSGEN loads the necessary drivers, and creates and mounts the NET0 device. However, this message shows that DECnet is not running, because a network application attempted to open the NET0 device to perform a DECnet operation, but the device is not mounted.

Troubleshooting Strategy

To resolve this problem, start DECnet. If starting DECnet does not resolve the problem, check to see if NETACP is running.

Troubleshooting Procedure

A. **Use the following command to determine if the NET devices are loaded:**

```
$ SHOW SYSTEM
```

If NETACP is one of the process names listed, the devices are loaded and DECnet is running.

B. **If the NET devices are not loaded, use the following command to start DECnet:**

```
$ @SYS$MANAGER:STARTNET
```

C. **If the previous command returns an error, it may be due to problems with the LOADNET.COM file. Do the following to resolve LOADNET.COM problems:**

1. Make sure that the LOADNET.COM file exists.

   The STARTNET.COM file calls the LOADNET.COM file, and, if the LOADNET.COM file does not exist, the STARTNET procedure fails.

2. Run NCP, and use the following command to stop the network:

   ```
   NCP>  SET EXECUTOR STATE OFF
   ```

3. Exit NCP, and use the following command to display command lines and data lines from the STARTNET procedure:

   ```
   $  SET VERIFY
   ```

   Resolve any problems indicated by the command and data lines from the STARTNET procedure.

4. Use the following command to restart the network:

   ```
   $  @SYS$MANAGER:STARTNET
   ```

D. **If starting DECnet does not resolve the problem, something more complex is occurring. Check to see if NETACP is running, using the following command:**

```
$  SHOW SYSTEM
```

Look for the NETACP process. NETACP must be running for the network to be running. If NETACP is not running, check to see if the image has been corrupted, or whether you have defined a logical name for NET. If you have a logical name definition for NET, the network cannot start because DECnet uses NET as a device name.

Other factors that may interfere with NETACP include the following:

- Insufficient quotas
- Incorrect system parameters, such as the number of process slots

Dialup Problems

Symptoms

Users cannot dial up to a remote node.

Explanation

This symptom indicates a cross-category problem.

The failure of dialup connections may be due to a problem with any of the following:

- Local end
- Remote end
- Telephone lines
- Modems
- Connecting cables

Troubleshooting Strategy

To solve this problem, evaluate and repair each of the potential problem areas in this order: first the local end, then the remote end, and finally the telephone lines.

Make sure that the setup parameters (such as speed, parity, modem control, and so forth) on the local and remote ends are properly defined. Ensure that the telephone lines are operational.

Troubleshooting Procedure

A. **On the local end, make sure that the speed, parity, bits, modem control, flow control, and other terminal characteristics are set up properly for the type of modem you have.**

The following example shows how to set these parameters for a VMS system using a DF242 modem.

```
$ SET TERMINAL/PERMANENT/MODEM/DIALUP/HANGUP/SPEED=xxxx tta0:
$ SET HOST/DTE tta0:
REM-I-TOEXIT, connection established, type ^\ to exit
   ^B
Ready
```

If the process fails, check the settings and cabling from the modem to the device. If a response other than "Ready" comes back from the modem, the problem is probably with the modem. Consult the modem manual for further information on how to resolve this problem.

B. **Dial the number to the remote node.**

If successful, the following message is displayed:

```
Attached (Speed:2400)
```

1. If you get the "Attached" message, but not a login prompt such as "Username:", check the terminal server or VAX node at the remote end to be sure that the terminal port is set up properly.
2. If you get a message other than "Attached," plug a telephone handset into the local telephone line to check for a dial tone.
   - If you hear a dial tone, the telephone line is working. Continue with step 3.
   - If you do not hear a dial tone, call your local carrier to fix this problem.
3. If you get no message, make sure that the cabling between the local system and the modem is intact, and that the local system and the modem do not have hardware problems. Continue with step 3.

C. **If you get a dial tone, do the following to further isolate the problem:**

1. If the modem has local loopback capabilities, use the local loopback and type characters on the local node or terminal's keyboard.
   - If the characters echo back on the local system, connectivity is intact between the local system and the modem, and the modem parameters are properly set. Go to step 4.
   - If the characters do not echo back, use a loopback connector or breakout box at the back of the local terminal or node, then type characters again.

     If characters echo back on the local system now, the local system is operating but the cable between the modem and the DTE is faulty, or there are set up problems (such as bits per character, parity and speed settings) between the DTE and DCE. If the characters do not echo back, the DTE is faulty.

2. If your modem does not have local loopback capabilities, do the following to isolate the problem:

   a. If either the local or remote end is connected to a terminal server or VAX, temporarily connect a terminal directly to the modem interface so that you have a terminal at each end to use for testing.

   b. Verify that the interface accepts connections by checking to see that the characters you type at one of the terminals are also displayed on the terminal attached to the other end of the modem.

3. Check the display on the modem.

   If the modem is operating properly, the modem displays data terminal ready (DTR) and data carrier detect (DCD) signals. If the modem does not display the DTR and DCD signals, use a breakout box to check the signals between the modem and the interface. The normal progression of RS232 signals between the modem and the interface is as follows:

   a. Ring indicator (RI, pin 22) toggles on and off to the DTE.

   b. DTE responds with data terminal ready (DTR, pin 20).

Note

When the DTE answers the ring indicator and responds with DTR, RI stops toggling.

   c. Modem responds with data carrier detect (DCD, pin 8) and data set ready (DSR, pin 6).

   d. Data passes until the connection ends.

   e. DTE disconnects and the DTR stops.

D. **From another handset, dial the local telephone line. If the local telephone rings and you can carry on a conversation, then the telephone line on the local end is good.**

   If you cannot pass voice traffic, or if there is no ring, call your local carrier to fix this problem.

E. **Repeat steps B and C on the remote node to resolve problems with the remote end.**

Insufficient Resources at Remote Node

Symptoms

Users receive the following message when attempting any network operation:

```
%SYSTEM-E-REMRSC, Insufficient system resources at remote node
```

Explanation

This symptom indicates a DECnet-VAX node problem that results from the remote node rejecting a connection because it does not have enough resources to process the request. The message can be caused by the following parameter values:

- SYSGEN parameter, MAXPROCESSCNT
- NCP parameters, MAXIMUM LINKS and ALIAS MAXIMUM LINKS
- AUTHORIZE parameters, MAXJOBS and MAXACCTJOBS

The current settings for these parameters may not be sufficient. For example, the NETACP page file quota may be exhausted, and may need to be modified. The NETACP page file holds the NCP node database. As the number of nodes in the database increases, the page file quota requirements for NETACP increase as well.

> **Note**
>
> This message may not indicate a problem. The parameter values may be set intentionally to disallow network connections beyond a certain number. If someone on the remote node logs out, the local user trying to establish a connection to the remote node may be successful.
>
> Be sure you understand the reason for the current setting before you take any action to solve this problem.

Troubleshooting Strategy

A. To resolve problems related to the MAXPROCESSCNT parameter, do the following:

1. Check the number of free process slots.
2. Check the current value of MAXPROCESSCNT.

3. Increase the value of MAXPROCESSCNT.
4. Execute AUTOGEN.COM.

B. To resolve problems related to the MAXIMUM LINKS and ALIAS MAXIMUM LINKS parameters, do the following:

1. Check the current values for MAXIMUM LINKS and ALIAS MAXIMUM LINKS on the remote node.
2. Check the number of links in use at the remote node.
3. Increase the values for MAXIMUM LINKS and ALIAS MAXIMUM LINKS, if necessary.

C. To resolve problems related to the NETACP page file quota, do the following:

1. Check the current page file quota value.
2. If the page file quota value is 0, then increase the value and shut down and restart the network.

D. To resolve problems related to MAXJOBS and MAXACCTJOBS, do the following:

1. Check the current values for MAXJOBS and MAXACCTJOBS specified in the SYSUAF file for the user who received the insufficient resources error.
2. Use AUTHORIZE to increase the values, if necessary and appropriate.

Troubleshooting Procedure

A. **Do the following to display the current value for MAXPROCESSCNT, and to increase the value, if necessary:**

1. Use the following command on the remote node to determine the total number of process entry slots, as well as the number of free process entry slots:

   ```
   $ SHOW MEMORY
   ```

   The MAXPROCESSCNT value determines the maximum number of process entry slots to be allocated. The default is 32. The maximum is 8192.

   The default value for MAXPROCESSCNT normally is sufficient. However, if there have been changes to the system since it was booted, you may need to increase the MAXPROCESSCNT value. For example, if the workload and number of users has changed, you may require a higher number of processes.

2. Edit MODPARAMS.DAT to include the following line, which increases the values for MAXPROCESSCNT:

   ```
   MAXPROCESSCNT=n
   ```

3. Execute the AUTOGEN.COM file to cause the changes to take effect.

Note

The AUTOGEN.COM command procedure reboots the system. Be sure you really want to reboot the system at this time before you execute the command.

```
$ @SYS$UPDATE:AUTOGEN GETDATA REBOOT NOFEEDBACK
```

B. **To display the current values for MAXIMUM LINKS [1] and ALIAS MAXIMUM LINKS[2], and to increase the values if necessary:**

1. Run NCP on the remote node, and use the following command to display the values for MAXIMUM LINKS and ALIAS MAXIMUM LINKS:

   ```
   NCP> SHOW EXECUTOR CHARACTERISTICS
   ```

2. Use the following NCP command on the remote node to display the known links:

   ```
   NCP> SHOW KNOWN LINKS
   ```

3. Count the number of links and compare that number with the results of the SHOW EXECUTOR CHARACTERISTICS command. If the number of known links equals the value for MAXIMUM LINKS or ALIAS MAXIMUM LINKS, use one of the following commands to increase the maximum links value:

   - If the insufficient resources message occurred when the user was connecting to a cluster alias, increase the ALIAS MAXIMUM LINKS value on the cluster using the following command:

     ```
     NCP> SET EXECUTOR ALIAS MAXIMUM LINKS n
     ```

[1] The MAXIMUM LINKS value determines the maximum number of logical links permitted on a node simultaneously. You must consider the network configuration when determining an appropriate setting for the MAXIMUM LINKS parameter. However, a reasonable range for most networks is 25 to 50. The maximum value for MAXIMUM LINKS is 960. You must reduce this value to 512, however, if you also specify the ALIAS MAXIMUM LINKS parameter.

[2] The ALIAS MAXIMUM LINKS value determines the number of logical links permitted simultaneously on the cluster alias node. The maximum value for ALIAS MAXIMUM LINKS is 200. The default value is 32. If you specify ALIAS MAXIMUM LINKS, the maximum value permitted for the MAXIMUM LINKS parameter is reduced.

- If the insufficient resources message occurred when the user was connecting to a nonalias node, increase the MAXIMUM LINKS value using the following command:

  ```
  NCP> SET EXECUTOR MAXIMUM LINKS n
  ```

C. **Do the following to check the page file quota value, and to increase it, if necessary:**

1. Use the following command to display the process identification number (PID) for the NETACP process:

   ```
   $ SHOW SYSTEM
   ```

2. Use the following command to display the current value for the page file quota value:

   ```
   $ SHOW PROCESS/ID=netacp_pid/QUOTAS
   ```

3. If the page file quota is 0, increase the value specified for NETACP$PAGE_FILE, using the following DCL command. Note that the default NETACP$PAGE_FILE value is 8192.

   ```
   $ DEFINE/SYSTEM NETACP$PAGE_FILE value
   ```

4. To cause the NETACP$PAGE_FILE value to be permanently changed, modify the SYSTARTUP.COM file with the new value and execute the SYSTARTUP.COM file before STARTNET.COM executes.

5. Run NCP and use the following command to shut down the network:

   ```
   NCP> SET EXECUTOR STATE OFF
   ```

6. Use the following command to restart the network:

   ```
   $ @STARTNET.COM
   ```

D. **Do the following to check the MAXJOBS and MAXACCTJOBS values for the user who received the insufficient resources error, and to increase the values, if necessary and appropriate:**

1. Run the Authorize utility and use the following command to display information about the user's account:

   ```
   UAF> SHOW user-id
   ```

2. Check the current values for MAXJOBS and MAXACCTJOBS.

   MAXJOBS specifies the maximum number of batch, interactive, and detached processes that may be active at one time.

   MAXACCTJOBS specifies the maximum number of batch, interactive, and detached processes that may be active at one time for all users who are on the same account as the specified user.

   A value of 0 for MAXJOBS or MAXACCTJOBS indicates that an unlimited number of batch, interactive, and detached processes may be active at one time.

3. If an increase in the values is necessary or appropriate, use the following command to modify the values:

   ```
   UAF> MODIFY user-id/MAXJOBS=n/MAXACCTJOBS=n
   ```

Recommendations

Some network servers (such as VTX and VAX Notes) can be heavily used. As a result, users who try to connect to these servers may encounter the insufficient resources message. You may want to allow more links to these servers by specifying a higher MAXIMUM LINKS value. However, specifying a higher MAXIMUM LINKS value can adversely affect performance, so weigh your decision to provide more links against the performance needs of the local users.

Invalid Parameter Value

Symptoms

While starting DECnet, the system displays the following message from NCP:

```
%NCP-W-INVPA, Invalid parameter value, Physical Ethernet address
Line = xxx-n
```

Explanation

This symptom indicates a DECnet-VAX node problem that results from protocols (such as LAT, DECelms, customer-written applications, or other Ethernet applications) starting before DECnet. Usually, this is because the LTLOAD.COM file is called before STARTNET.COM.

Troubleshooting Strategy

Make sure that DECnet starts first. To do this, stop all other protocols, restart DECnet, and then restart the other protocols.

Troubleshooting Procedure

A. **Use the following command to see if other protocols are running, specifying the device type, as shown in Table 3–3.**

```
$  SHOW DEVICE device-type
```

The display from this command shows the device name and its current status.

Table 3–3 Specifying the Device Type

Device-type designation	Device
XE	DEUNA, DELUA
ET	DEBNA
XQ	DEQNA, DELQA, DESQA
TR	DEQRA
ES	DESVA

B. **Make sure that SYS$MANAGER:LTLOAD.COM is called from SYSTARTUP.COM, and is called after STARTNET.COM. To do this, make sure that the SYS$SYSTARTUP.COM file contains the following lines, in the following order:**

```
@SYS$MANAGER:STARTNET.COM
@SYS$MANAGER:LTLOAD.COM
```

Or you can submit a user-specified command file that contains the preceding commands in the correct order.

C. **Run LATCP, and use the following command to stop the LAT protocol:**

```
LCP>  STOP NODE
```

D. **Use the following command to execute the STARTNET.COM file and restart the network:**

```
$  @STARTNET.COM
```

E. **Use the following command to execute the LTLOAD.COM file and restart the LAT protocol:**

```
$  @LTLOAD.COM
```

LAN Bridge Cannot Downline Load

Symptoms

A LAN Bridge 100 or 150, intended to be used as a LAN Traffic Monitor (LTM), cannot downline load.

Explanation

This symptom indicates a LAN problem involving maintenance operation protocol (MOP). The bridge has successfully completed the self-test, but cannot downline load the LTM image due to a problem with the bridge setup or with the load host.

Troubleshooting Strategy

A. Verify the setup of the bridge.

B. Check the load host for problems preventing it from downline loading the LTM software.

C. Use either DECelms or the switches on the bridge to correct the setup and enable the bridge to downline load. (Do not use both DECelms and the switches.)

Troubleshooting Procedure

A. **Do one of the following to verify the hardware version:**

- Check the metal tag on the bridge for the hardware version.
- Run DECelms, and use the following command to display the hardware version:

```
ELMS>  USE bridge-id
ELMS>  SHOW CHARACTERISTICS
```

To be able to downline load and function as a LAN Traffic Monitor, the bridge hardware must be at least Rev. E. The display shows various bridge characteristics including the ROM firmware version. A firmware version of 2.0 or greater equates to hardware Rev. E.

B. **Use the following NCP command to see if circuit service is enabled on the host node:**

```
NCP>  SHOW CIRCUIT circuit-id CHARACTERISTICS
```

If circuit service is not enabled, use the following NCP commands to enable it:

```
NCP>  SET CIRCUIT circuit-id STATE OFF
NCP>  SET CIRCUIT circuit-id SERVICE ENABLED
NCP>  SET CIRCUIT circuit-id STATE ON
```

Note

The following command is optional. It enables service for the circuit in the NCP permanent database. However, you may not want to permanently enable service for the circuit due to the effect it has on performance.

```
NCP>  DEFINE CIRCUIT circuit-id SERVICE ENABLED
```

C. **Make sure that the cabling is connected securely.**

D. **Check the bridge indicator lights.**

When the bridge is set up to function as a bridge, the indicator lights normally operate as follows:

a. When you turn the bridge on, all the lights go on briefly, then all go out except the DC OK light.

b. After about 15 seconds, the self-test completes and the SELF TEST light goes on.

c. After about 30 seconds, the ONLINE light goes on, unless the bridge is in a loop with another bridge or repeater connecting the two segments. In this case, the bridge may go into BACKUP state, and the ONLINE light may not come on.

d. Finally, the activity lights begin blinking to indicate network activity. If the network is very busy, the lights blink very quickly and appear to be on continuously.

However, when the bridge is set up to function as a LAN Traffic Monitor, and the LTM software has been loaded, the ONLINE light blinks on and off in a pattern. This pattern indicates that the bridge is operating as a LAN Traffic Monitor.

E. **If the bridge is intended to operate as a LAN Traffic Monitor, but the ONLINE light is not blinking, insert loopback connectors into the A and B ports, wait about 45 seconds, and check the lights again.**

Table 3–4 shows the status of the bridge when various indicator lights are on.

Table 3–4 LAN Bridge 100 or 150 Indicator Lights

Indicator Lights	Status
SELF TEST is off	The bridge has a hardware problem.
ONLINE, DC OK, and SELF TEST are on, and ACTIVITY lights are blinking approximately once per second	The bridge is set up to function as a bridge.
SELF TEST and DC OK are on, ONLINE is off, and the activity lights are blinking	The bridge is set up for downline loading and use as a LAN Traffic Monitor.

F. **If the indicator lights show that the bridge is not set up properly for downline loading, use DECelms or the switches on the bridge to set up the bridge for downline loading.**

G. **Make sure that the downline load switch (number 5) is disabled (UP).**

Note

You can use either DECelms or the bridge switches. Do not use both for the same load. Step a, as follows, describes how to use DECelms to set up the bridge for downline loading. Step b describes how to use the bridge switches.

a. To use DECelms to set up the bridge for downline loading, do the following:

   i Use the following command to specify the environment for the remaining commands of this procedure:

   ```
   ELMS> USE bridge-id
   ```

   ii Use the following command to set the software downline load request flag:

   ```
   ELMS> SET LOAD SWITCH TRUE
   ```

   For a LAN bridge 150, you can also specify a password with this command.

iii Use the following command to specify the downline load file name:

```
ELMS> SET LOAD FILE filename
```

Note

The file name must be exactly 10 characters long.

For a LAN bridge 150, you can also specify a password with this command.

iv Use the following command to cause DECelms to reset itself with the new information you specified:

```
ELMS> INIT
```

b. To use the bridge switches to set up the bridge for downline loading, do the following:

i Clear the downline load switch and downline load information in NVRAM using the following steps:

Note

The following procedure sets *all* bridge parameters to the default settings. If you do not want to reset all the parameters, use DECelms instead.

a. Press switch 2 (NVRAM RESET) down.

b. Turn the bridge off.

c. Turn the bridge on.

d. When the self-test completes, turn the bridge off.

e. Press switch 2 (NVRAM RESET) up.

ii Make sure that the load host is properly set up, as described in the LTM installation documentation.

iii Connect at least one port to the same LAN or extended LAN as the load host. You can connect the other port to another LAN segment, or insert a loopback connector in it.

iv Set the bridge switches as follows:

Note

For switches 3 and 4, you need not set both switches as long as you set the port switch that is in the same segment as the load host.

Table 3–5 shows the switch settings for the LAN Bridge 100 or 150.

Table 3–5 LAN Bridge 100 or 150 Switch Settings

Switch Number	Name	Setting
1	Manufacturing Mode	Up (Off)
2	NVRAM Reset	Up (Off)
3	Port A Access	Down (On)
4	Port B Access	Down (On)
5	Downline Load	Down (On)
6	Not Used	Up (Off)

v Turn the bridge on.

The load takes less than five minutes, unless the load host is extremely busy.

LAN Segment Communication Problem

Symptoms

All the systems on a LAN segment are unable to communicate with systems beyond their segment. However, all the systems on the isolated LAN segment can still communicate among themselves.

Explanation

This symptom indicates a LAN problem involving the physical layer. The symptoms could be related to problems causing a bridge or repeater to segment.

Bridges connect Ethernet LANs to create extended LANs, and repeaters connect Ethernet segments to expand a LAN. Bridges keep the traffic between systems on a LAN segment within that LAN segment, and out of the general network traffic on the extended LAN. Restricting network traffic this way keeps segment traffic to a minimum and prevents unnecessary traffic from entering the extended LAN.

Repeaters do not isolate traffic; however, if a repeater detects faulty signals that cause a high number of collisions, the repeater automatically stops repeating the signals until it detects good signals again.

An Ethernet LAN and a Token Ring LAN can exchange data by using a bridge or a router that is connected to both networks. The bridge or router examines the traffic on each LAN and copies a message if its destination is on the other LAN. This allows Ethernet nodes and Token Ring stations to communicate with each other by using the bridge or router.

Potential causes of this problem include the following:

- Occasionally, a repeater or bridge may fail, or may be disconnected accidentally, causing an entire segment to become isolated from the rest of the extended LAN.
- A problem may exist on the LAN on the other side of the device (for example, a babbling device) that causes the bridge or repeater to segment.
- A faulty H4000 tap for the bridge or repeater may cause the device to segment.

Troubleshooting Strategy

To begin solving this problem, use your knowledge of the network topology, and your network map to isolate the source of the problem to the interconnecting device for the isolated LAN segment. After you determine the device that is causing the problem, continue with the following steps:

- For bridge problems at sites where DECelms is available, use step A.
- For bridge problems at sites where DECelms is not available, use step B.
- For bridge problems at sites using ETHERnim, use step C.
- For repeaters (including DEREP and DEREN (Ethernet Repeaters), DEMPR (ThinWire multiport repeater), and DESPR (ThinWire singleport repeater), use step D.
- For H4000 problems, use step E.

Troubleshooting Procedure

A. **If DECelms is available at your site, do the following to check the bridge:**

1. Run DECelms, and use the following command to verify that the bridge lines are operating and are in the FORWARDING state:

   ```
   ELMS>  USE bridge_id
   ELMS>  SHOW KNOWN_LINES STATUS
   ```

   The display shows line characteristics for the lines on the bridge, and whether the lines are in the forwarding state.

2. Use the following command to display the bridge counters:

   ```
   ELMS>  SHOW COUNTERS
   ```

   The value for the bridge seconds counter tells you how long the bridge has been running.

3. At sites where several users have access to the DECelms software, another user may have mistakenly set up the bridge to filter all packets destined for certain addresses. If you suspect this is the case, use the following command to verify the forwarding database status on the bridge:

   ```
   ELMS>  SHOW ADDRESS address
   ```

   The display shows the forwarding entry for the address specified.

4. Check the display for the destination address.

The designation NONE means that the bridge does not forward packets to that address. If the designation is NONE, do the following:

a. Make sure that the bridge should be forwarding packets to that address.

   Sometimes packet forwarding is intentionally disabled for a particular address.

b. If packets should be forwarded to the address, use the following command to enable the bridge to forward packets to the address:

   ```
   ELMS>  REMOVE ADDRESS address PASSWORD password
   ```

   In the normal course of operation, the bridge learns the correct action to take for packets destined for this address.

B. **If DECelms is not available at your site, do the following to check whether the bridge is off line for segmentation:**

1. Go to the bridge for the isolated LAN segment.
2. Make sure that the power is on.
3. Make sure that the cable connecting the bridge to the H4000 transceiver or DELNI is properly connected.
4. Check the indicator lights on the bridge.

   Normally, the activity lights blink on and off for each packet sent. If the bridge is processing many packets, the lights are on continuously. This is not unusual, and does not indicate a problem. However, if the lights are off, there is probably a hardware or power problem with the bridge.
5. If the activity lights are off, replace the bridge.
6. If the ONLINE light is off, try to connect with a network node on the other side of the bridge to make sure the bridge is not in a loop configuration with another bridge or repeater (and is in a backup state). If the connection succeeds, there is a loop, and this bridge is in backup mode. In this case, the loop is not a problem. If a failure occurs on the network, this bridge changes from backup to online mode.
7. If no unexpected loops exist and the problem persists, replace the problem bridge with another bridge to verify if the problem is hardware related. If the new bridge functions properly, the problem with the old bridge is probably hardware-related.

C. **If you have ETHERnim at your site, use it to poll or show nodes on the segment in question, and on each previous segment, until you locate the source of the problem.**

D. **Use the following procedure to solve problems relating to repeaters:**

1. Go to the repeater for the isolated LAN segment.
2. Make sure that the power is on.
3. Make sure that the cable connecting the repeater to the H4000 transceiver or DELNI is properly inserted.
4. Run the self-test.
5. Check the indicator lights on the repeater.

   The SEGMENTED light usually indicates a circuit problem.
6. See the appropriate repeater manual for further corrective actions.

E. **If the bridge is still not reachable, the H4000 transceiver that connects the bridge to the local segment may be faulty. To determine if this is a problem, do the following:**

1. Go to a node on the other segment to see if that node can communicate through the bridge.

   If the node on the other segment can reach the bridge, then the H4000 transceiver that connects the bridge to the local segment is probably broken.
2. Check that connections are secure.
3. If the connections are secure and the bridge is still unreachable, move the bridge to another H4000 tap or DELNI port.

Recommendations

- If possible, include redundant bridges and repeaters on your network. The redundant devices provide service if a primary device fails, helping to ensure uninterrupted service for your users.

  Digital's bridges and repeaters perform automatic failover when the network includes redundant devices. To provide backup service for bridges on your network, you need only provide one bridge to act as the backup for all bridges on your network, because bridges use a spanning tree algorithm.
- If you are using the bridge as a LAN Traffic Monitor, and are not using both of the bridge's ports (A and B), insert a loopback connector in the unused port. If you do not use the loopback connector, the bridge cannot complete the self-test when it starts running. In the event of a bridge failure elsewhere

on the network, you can temporarily use the LAN Traffic Monitor bridge as a backup.

- Be sure to follow the guidelines for configuring your network with bridges. The maximum number of bridges permitted in a linear setup (from point A to point B) is seven.
- Be sure to follow the guidelines for configuring repeaters on your network. The maximum number of repeaters permitted in a linear setup (from point A to point B) is two. (A pair of fiber-optic repeaters count as one repeater.)
- Keep track of when and where new taps are installed on the network.

Line Synchronization Lost

Symptoms

A circuit goes down and up every two or three seconds, and the system displays the following DECnet event messages:

```
%%%%%%%%%%%   OPCOM  27-JUN-1990 14:22:06.17   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.7, circuit down, circuit fault
From node x.xxx (NODE2), 27-JUN-1990 14:17:58.10
Circuit DMC-3, Line synchronization lost

%%%%%%%%%%%   OPCOM  27-JUN-1990 14:22:06.17   %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.10, circuit up
From node x.xxx (NODE2), 27-JUN-1990 14:18:01.79
Circuit DMC-3, Adjacent node = x.xxx (NODE3)
```

Explanation

This symptom indicates an Ethernet or Token Ring DECnet problem in which the data link protocols between the two nodes cannot be initialized. This symptom usually indicates a hardware or line problem, such as the following:

- Transceiver cable that is not properly connected
- Faulty communications board
- Improper system parameter settings for IRPCOUNT, LRPCOUNT, and SRPCOUNT

It can also indicate the following:

- Local Area VAXcluster set up improperly as a boot node
- Synchronous line problems (for example, modem or digital service unit problems)
- Faulty H4000 connection to the Ethernet

Troubleshooting Strategy

To solve this problem, determine if the problem is on the local node or the network, then complete the appropriate actions below:

A. If the problem is on the local node, do the following on the local node:

   1. Make sure that the current values have not reached or exceeded the initially allocated values for IRPCOUNT, LRPCOUNT, SRPCOUNT.

2. Check the circuit counters.
3. Make sure that the cable connections are secure.

B. If the problem is on the network, do the following on the local node:

1. If the node is set up as a Local Area VAXcluster boot node, make sure that the VAXCLUSTER parameter in SYSGEN is set properly.
2. Make sure that the current counter values have not reached the maximum permitted values.
3. Check the circuit counters.
4. Check the line counters for open or short circuits on transmit and receive.
5. Make sure that the cable connections are secure.
6. Make sure that the network controller module is properly seated.
7. Use loopback tests as necessary if the problem relates to synchronous devices and modems.

Troubleshooting Procedure

To begin solving this problem, check the events displayed on several nodes on the network to determine if the problem is related to the local node or the network. If the line synchronization lost message is displayed only on one node, the problem is on that node. If the line synchronization lost message is displayed on multiple nodes, the problem is on the network.

A. **Use the following steps to resolve problems on the local node:**

1. If the node is a VMS 3XXX or 4000 series system with a Token Ring DEQRA board, run the DEC TRNcontroller 100 (DEQRA) diagnostic program included in the DEC TRNcontroller 100/DEC Token Ring Device Driver for VMS kit. Run the diagnostic as a foreign command by entering the following:

```
$ TR_DIAG :==$SYS$TEST:DEQRA$DIAGS.EXE
$ TR_DIAG/DEVICE=TRA0/SPEED=16
```

Note

The speed value in the previous command must match your Token Ring network transmission speed and the speed value in the DEQRA's TRDRIVER.INI configuration file. Therefore, the speed value must be 4 or 16.

The diagnostic program displays the following menu.

```
DEQRA Diagnostics

1 = Board Status
2 = Lobe Loopback Test
3 = Ring Loopback Test
q = Quit

Enter Option:
```

Choose test number one (Board Status). This test verifies the DEQRA board is performing correctly by checking the following components:

- Program to driver interface
- Driver to board interface
- DEC TRNcontroller 100 software

If there is no error message, proceed to the next numbered step.

2. Use the following command to display the current values for IRPCOUNT (I/O request packet count), LRPCOUNT (large request packet count), and SRPCOUNT (small request packet count):

   ```
   $  SHOW MEMORY/POOL/FULL
   ```

   IRP, LPR, and SRP are three preallocated memory pools in the nonpaged pool area. The nonpaged pool area is a portion of physical memory permanently allocated to the system for the storage of data structures and device drivers. Its initial size is determined by AUTOGEN but automatic expansion of the area occurs if necessary.

3. Compare the current values of IRPCOUNT, LRPCOUNT, and SRPCOUNT to the initial allocation.

4. If the current values equal or exceed the initial allocation, edit MODPARAMS.DAT to increase both IRPCOUNT, LRPCOUNT, and SRPCOUNT values, as well as IRPCOUNTV, LRPCOUNTV, and SRPCOUNTV values. IRPCOUNTV, LRPCOUNTV, and SRPCOUNTV values are the upper limits to which the IRPCOUNT, LRPCOUNT, and SRPCOUNT values can be automatically increased by the system.

In determining the amount to increase the values, you must trade off the permanent allocation of memory for nonpaged pool against the small amount of CPU overhead required to do pool expansion. If physical memory on your system is limited, it may be reasonable to accept a low to moderate amount of expansion.

5. Execute the AUTOGEN.COM file to cause the changes to take effect.

Note

The AUTOGEN.COM command procedure reboots the system. Be sure you really want to reboot the system at this time before you execute the command.

```
$ @SYS$UPDATE:AUTOGEN GETDATA NOFEEDBACK REBOOT
```

6. For point-to-point circuits, the problem usually involves a cable that is not connected properly, a faulty communications board, or a faulty or noisy circuit. Run NCP and use the following command to check the counters on the failing circuit for any errors:

```
NCP> SHOW CIRCUIT circuit-id COUNTERS
```

7. If the counters display the greater than symbol (>), then the counters have reached their maximums and cannot record any further changes. In this case, zero the counters.

```
NCP> ZERO CIRCUIT circuit-id
```

8. After a short time, check the counters again to see whether there is a change, and follow up on any unusual counter changes, such as high error rates.
9. If the counter information does not help determine the problem, use loopback tests.
10. Make sure that the cable connections are secure.

B. **Use the following steps to resolve problems on the Ethernet:**

1. Perform all the steps in **A**, then continue with the following steps.
2. If the node is the boot node for a Local Area VAXcluster, make sure that the SYSGEN parameter, VAXCLUSTER, is set to 1, and execute the AUTOGEN.COM file to cause the changes to take effect.

The VAXcluster parameter controls loading of the cluster code. The default setting is 1, which means TO LOAD if SCSLOA is being loaded. A setting of 0 means TO NEVER LOAD. A setting of 2 means TO ALWAYS LOAD SCSLOA.

Note

The AUTOGEN.COM command procedure reboots the system. Be sure you really want to reboot the system at this time before you execute the command.

```
$ @SYS$UPDATE:AUTOGEN GETDATA NOFEEDBACK REBOOT
```

3. For Ethernet circuits, if the circuit down counter has incremented, the problem is due to a faulty hardware device, improperly terminated cables, or loose cable connections. In particular, the problem may be related to open or short circuits. Use the following command to check the counters on the circuit:

   ```
   NCP> SHOW CIRCUIT circuit_id COUNTERS
   ```

   Check the transmit and receive counters for open or short circuits. On Ethernet circuits, if there are no open or short circuits, the problem is probably due to a faulty communications board.

4. Make sure that the cable connections are secure.

5. Connect the transceiver cable to another H4000 or DELNI to determine if the problem is related to an H4000 transceiver failure or to a faulty H4000 connection to the Ethernet.

   If the new connection works, then the problem was related to the H4000 tap into the Ethernet, or to the H4000 transceiver itself.

6. To resolve H4000 problems, first try to retap the H4000 into the Ethernet.

   If the problem persists after retapping the H4000, the H4000 may be faulty.

7. Replace the H4000, and check the DECnet event messages again.

8. For problems relating to synchronous devices and modems, use loopback tests.

9. For controller or device level problems, ask Customer Services to make sure that the Ethernet controller module is seated properly.

Login Information Invalid

Symptoms

Users receive an error message such as the following when attempting any network operation except SET HOST:

```
%MAIL-E-LOGLINK, Error creating network link to node NODEID
  -SYSTEM-F-INVLOGIN, login information invalid at remote node
```

Explanation

This symptom indicates a DECnet-VAX node problem involving the session layer. It can be caused by any of the following:

- User-supplied access control information is incorrect.
- Proxy access is set up incorrectly.
- The user and password for a specific object on the remote node does not match a valid account in the System User Authorization (SYSUAF) file.
- The nonprivileged password defined in the executor characteristics on the remote node does not match the password defined in the remote node's SYSUAF file.
- The executor does not have a nonprivileged user or nonprivileged password defined.
- AUTHORIZE parameter settings for the default DECnet account may cause this message. For example, this message can occur if the DISUSER flag is set or the account is expired.

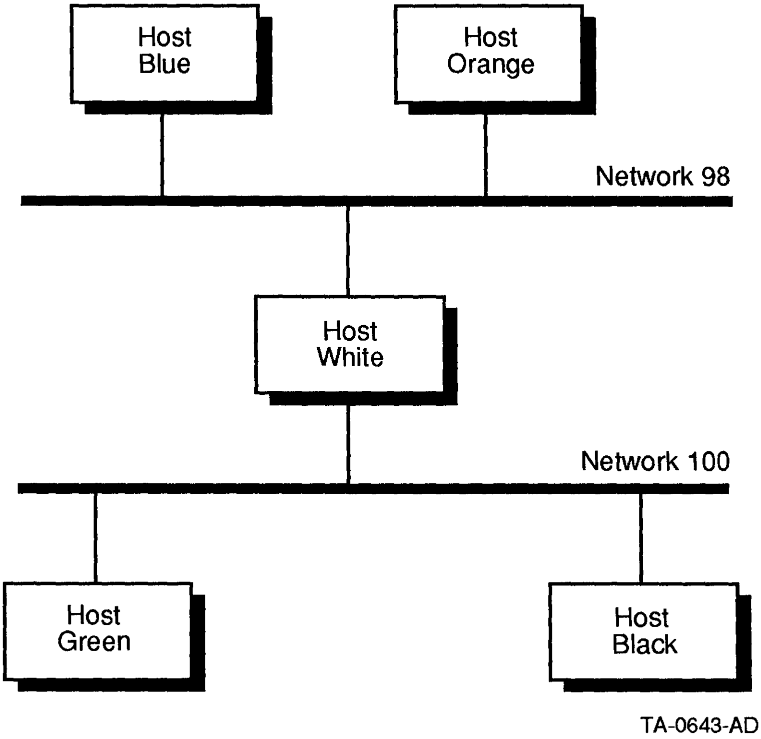
If the login information invalid error occurs intermittently, the remote system is probably a cluster system that has a node or nodes set up improperly. When the login information goes to the improperly set up node, the error message occurs. However, if the login information goes to a properly set up node, the login is successful.

To troubleshoot this problem effectively, you need to understand the order of access control for VMS systems. VMS systems permit access based on the type of access control information the system receives.

VMS systems check first for user-supplied access control information. If user-supplied information does not exist, the VMS system checks for proxy access information. If proxy access information does not exist, the VMS system checks for default access information.

Figure 3–1 shows the order of access control for VMS systems in more detail.

Figure 3–1 VMS Access Control



Note

NCP parameters determine the type of proxy access permitted, if any, for objects on a node or for the node itself. NCP information specified for an object always supersedes the executor information. This is true for proxy as well as default account information.

Proxy access for objects and the executor is determined according to the parameters shown in Table 3–6.

Table 3–6 NCP Proxy Access Parameters

Object Parameter	Function
PROXY INCOMING	Allows proxy login to the object.
PROXY OUTGOING	Allows the object to initiate proxy login.
PROXY BOTH	Allows both incoming and outgoing proxy login access. This is the default.
PROXY NONE	Prohibits incoming and outgoing proxy login access.
	If you omit the PROXY parameter, proxy access is determined according to the executor parameters.

Executor Parameter	Function
INCOMING PROXY DISABLED	Ignores all incoming proxy requests, and instead, relies exclusively on access control information supplied in the connect requests to validate the logical link.
INCOMING PROXY ENABLED	Invokes the appropriate proxy, based on the source user, source node, and supplied access control information, if any. This is the default.
OUTGOING PROXY DISABLED	Specifies that proxy login is not requested on any outgoing logical links.
OUTGOING PROXY ENABLED	Specifies that proxy login is requested on outgoing logical links. This is the default.

Troubleshooting Strategy

Before you attempt to solve this problem, do the following:

- Determine the type of access control the user specified when trying to access the remote node.
- Determine the objects the user tried to access.
- If the error occurs intermittently, the remote node may be a cluster system. Determine which node of the cluster is improperly set up, and correct the set up.

A. For user-specified access control problems, do the following:

   1. Check the user-specified access control information.

   2. Make sure that the account the user wants to access exists on the remote node.

   3. Modify the password information on the remote account.

B. For proxy access control problems, do the following on the source (local) and target (remote) nodes:

   1. Do the following on the source (local) node:

      a. Make sure that PROXY OUTGOING or PROXY BOTH is enabled for the object.

      b. Make sure that OUTGOING PROXY is enabled for the executor.

   2. Do the following on the target (remote) node:

      a. Make sure that PROXY INCOMING or PROXY BOTH is enabled for the object.

      b. Make sure that INCOMING PROXY is enabled for the executor.

      c. Make sure that NETPROXY.DAT has the correct proxy definitions.

      d. Make sure that the proxy account exists in the SYSUAF file.

C. For default access control problems, do the following:

   1. If the requested object has a user name and password associated with it, make sure that the definitions in the SYSUAF file match those specified in NCP.

   2. If the requested object does not have a user name and password associated with it, check to see if the remote node's executor has a nonprivileged user and nonprivileged password specified.

      If they are specified, make sure that the definitions in the SYSUAF file match those specified in NCP.

   3. If neither the object nor the executor have a nonprivileged user name and password, define them as necessary.

Troubleshooting Procedure

Before you try to solve this problem, do the following:

1. Use the following list to help determine which step to use to solve the problem:
2. If the user specified explicit access control information when trying to access the remote node, use step A to solve the problem.
3. If the user tried to access the remote node using proxy access, use step B to solve the problem.
4. If the user did not try to access the remote node using proxy access, use step C.
5. If you do not know if the user tried to access the remote account using proxy access, use step B first, and continue with step C if necessary to solve the problem.
6. If the error has been occurring intermittently, the remote node may be a cluster system. Determine which node of the cluster is improperly set up, and correct the set up.

Note

> To help solve this problem faster, you can try to connect to a different object on the remote node. If the connection succeeds when directed toward the new object, then the problem is probably object-specific, and you can focus your efforts on ensuring that the object on the remote node is set up properly.

A. **For explicit access control problems, do the following:**

   1. Try to log in to the remote account that the user tried to access, using the access information the user specified.

      If you cannot log in, the access information is probably incorrect.

   2. Log in to an account on the remote node that has SYSNAM and SYSPRV privileges, and perform the following steps.

   3. Use the following AUTHORIZE command to check that the user has an account in the remote node's system user authorization file (SYSUAF):

      ```
      UAF> SHOW user-id
      ```

4. Use the following AUTHORIZE command to define a new password for the user's account:

   ```
   UAF> MODIFY user-id/PASSWORD=password
   ```

5. Try logging in to the user's account with the new password.

B. **For proxy access control problems, do the following on the source (local) and target (remote) nodes:**

1. Do the following on the source (local) node:

   a. Run NCP and use the following command to display the current settings for proxy access to the object:

      ```
      NCP> SHOW OBJECT object-name CHARACTERISTICS
      ```

      If PROXY OUTGOING is not specified, and if proxy access is required for the requested object, use the following NCP command to enable OUTGOING proxy access for this object only:

      ```
      NCP> SET OBJECT object-name PROXY OUTGOING
      ```

   b. To enable OUTGOING PROXY access for the executor, use the following NCP command:

      ```
      NCP> SET EXECUTOR OUTGOING PROXY ENABLED
      ```

2. Do the following on the target (remote) node:

   a. Run NCP, and use the following command to display the current settings for proxy access to the object.

      ```
      NCP> SHOW OBJECT object-name CHARACTERISTICS
      ```

      If PROXY INCOMING is not specified, and if proxy access is required for the requested object, use the following NCP command to enable incoming proxy access for this object only:

      ```
      NCP> SET OBJECT object-name PROXY INCOMING
      ```

   b. Use the following command to display the current settings for proxy access to the remote executor:

      ```
      NCP> SHOW EXECUTOR CHARACTERISTICS
      ```

      If the executor INCOMING PROXY is not specified for the executor, then incoming proxy access to the executor is denied.

   c. To enable incoming proxy access to the executor, use the following NCP command:

```
NCP> SET EXECUTOR INCOMING PROXY ENABLED
```

Caution

Enabling proxy incoming on the executor can cause security problems. For more secure proxy access, set proxy incoming enabled only on the object.

d. Run AUTHORIZE on the remote node, and use the following command to make sure that the proxy definitions in NETPROXY.DAT are correct:

```
UAF> SHOW/PROXY node::user
```

If the proxy definition for the source node is not correct, use the following command to change it:

```
UAF> MODIFY/PROXY node::user user
```

In this example, *node::user* is the source node and user, and *user* is the user on the target (or current) node.

The source node is the node that originates the proxy login request. The target node is the node that receives the proxy login request, in this case, the current node.

e. Use the following AUTHORIZE command on the remote node to make sure that the proxy account the user is trying to access on the remote node exists:

```
UAF> SHOW user-id
```

If the account does not exist, but should exist, use AUTHORIZE to create the account.

C. **Do the following to resolve problems due to default access control information:**

1. Log in to an account on the remote node that has SYSNAM and SYSPRV privileges, and perform the following steps.
2. Run NCP, and use the following command to check whether the object requested exists, and whether it has a user name and password associated with it:

```
NCP> SHOW KNOWN OBJECTS
```

3. If the object does not exist, create the object.
4. If the object exists, go to the next step.

5. Run AUTHORIZE, and use the following command to check that the object's user ID specified in the SHOW KNOWN OBJECTS command has an account in the remote node's system user authorization file (SYSUAF):

   ```
   UAF> SHOW user-id
   ```

6. If there is an account for the object's user ID, use the following AUTHORIZE command to define a new password for it:

   ```
   UAF> MODIFY user-id/PASSWORD=password
   ```

7. Use the following NCP command to display the nonprivileged user ID and nonprivileged password for the remote node:

   ```
   NCP> SHOW EXECUTOR CHARACTERISTICS
   ```

8. Run AUTHORIZE, and use the following command to check that the nonprivileged user specified in the executor characteristics has an account in the remote node's system user authorization file (SYSUAF):

   ```
   UAF> SHOW user-id
   ```

9. If there is an account for the nonprivileged user, use the following AUTHORIZE command to define a new password for it:

   ```
   UAF> MODIFY user-id/PASSWORD=password
   ```

10. If an account does not exist for the nonprivileged user, run AUTHORIZE, and use the ADD command to define an account.

11. Run NCP, and use the following command to define a nonprivileged user, and to specify the same password for the nonprivileged account that you defined in the SYSUAF:

    ```
    NCP> SET EXECUTOR NONPRIVILEGED USER user-id PASSWORD password
    ```

Recommendations

You might want to use security alarms to provide information for troubleshooting login failure problems. Security alarms can provide information such as the user name and password used in failed login attempts. See the SET AUDIT command in the *VMS DCL Dictionary* for more information on setting up security alarms. Use the DCL command, REPLY/ENABLE=SECURITY, to display security alarms. Use of the REPLY/ENABLE=SECURITY command requires SECURITY privilege.

Because the security auditing features involve some system overhead, be careful to select the security features that provide the most benefit in your work environment. Overuse of alarm messages diminishes their usefulness; and, because alarm messages have priority over any other I/O, they can tie up the security operator's terminal.

Network Object Unknown

Symptoms

Users receive the following message when trying to access a remote node:

```
%SYSTEM-F-NOSUCHOBJ, Network object is unknown at remote node
```

Explanation

This is a DECnet-VAX node problem involving the session layer, and can be caused by any of the following:

- The object requested is not defined in NCP, is not started, or the file specified in the requested object does not exist.
- The user tried to access an object with an alias name, and ALIAS INCOMING is disabled for the object.
- If the user operation resulting in this message was SET HOST, SYS$SYSTEM RTTLOAD.COM has not been run. As a result, the REMACP process is not running on the remote system, the drivers are not loaded, and the CTERM and REMACP objects do not exist.

Note

If the operation was SET HOST, and the REMACP process is not running, it may be that the system has just rebooted and has not yet executed RTTLOAD.COM. In this case, wait a few minutes, and try the operation again before beginning the troubleshooting procedure.

Troubleshooting Strategy

A. For problems related to the requested object, do the following:

1. Check to see if the object is defined in NCP.
2. If the object is not defined, define it.
3. Check to see if the file specified for the requested object exists.
4. If the file for the requested object does not exist, create it.
5. Check to see if the object is started.
6. If the object is not started, start it.

B. For problems related to the setting of ALIAS INCOMING on the requested object, do the following:

   1. Check the current setting of ALIAS INCOMING on the object.
   2. Enable ALIAS INCOMING on the object if necessary.

C. For problems related to SET HOST and RTTLOAD.COM not running, do the following:

   1. Check if the REMACP process is running.
   2. Execute RTTLOAD.COM to run the REMACP process.

Troubleshooting Procedure

A. **This step explains how to solve problems related to the requested object.**

   Objects can be associated with command and executable files, or they can be associated with a process. For objects associated with command and executable files, start with step 1. For objects associated with a process, start with step 5.

   To determine the type of association the requested object has, run NCP and use the following command to see if the object is defined on the remote node:

   ```
   NCP> TELL remote-node-id SHOW KNOWN OBJECTS
   ```

   1. If the object is not defined, run NCP on the remote node, and define it using the following command and additional parameters, as required:

      ```
      NCP> SET OBJECT object-id
      ```

   2. If the object is defined, run NCP and use the following command to see if the object has a file specified:

      ```
      NCP> TELL remote-node-id SHOW KNOWN OBJECTS
      ```

   3. Use the DIRECTORY command to see if the file specified for the requested object exists.
   4. If the file for the requested object does not exist, create it.
   5. Use the following command on the remote node to see if the object is started:

      ```
      $ SHOW SYSTEM
      ```

      If the object's process is not displayed, the object is not started.

   6. If the object is not started, start it.

The method for starting the object depends on which object needs to be started. For example, to start REMACP, execute the SYS$MANAGER:RTTLOAD.COM command procedure.

B. **Do the following on each node in the cluster to resolve problems related to ALIAS INCOMING:**

Note

Because the problem may be due to the improper setup of any of the cluster nodes, it is important to check the object on each node. If you do not resolve setup problems on each node, the problem may continue to occur intermittently, when an access request from a remote node reaches the improperly set up node.

1. Run NCP and use the following command to display the current setting for ALIAS INCOMING on the object:

   ```
   NCP> SHOW OBJECT object-name CHARACTERISTICS
   ```

2. If ALIAS INCOMING is disabled for the object, enable it using the following command:

   ```
   NCP> SET OBJECT object-name ALIAS INCOMING ENABLED
   ```

C. **Do the following to address the problem if the user action was SET HOST and RTTLOAD.COM was not run:**

1. Use the following command to see if the STARTNET job is running on the local node:

   ```
   $ SHOW QUEUE batch-queue-id
   ```

   The remote node may currently be unknown because the local node has not completed the STARTNET job. If the STARTNET job is still running, wait until it completes, then try the operation again. If the remote node is still unreachable, continue with the following steps.

2. Run NCP, and use the following command to determine if the REMACP process is running on the remote node:

   ```
   NCP> TELL remote-node-id SHOW KNOWN OBJECTS
   ```

   The NCP utility displays the list of objects running and their process identification numbers (PIDs). If the display does not include a PID for the REMACP object, the REMACP process is not running.

3. If the REMACP process is not running, execute the SYS$MANAGER:RTTLOAD.COM command procedure on the remote node.

The SYS$MANAGER:RTTLOAD.COM command procedure loads RTTDRIVER and CTDRIVER, and runs the REMACP process.

Network Partner Exited

Symptoms

Users receive the following message when attempting to perform any network operation except SET HOST:

```
%SYSTEM-F-LINKEXIT, network partner exited
```

Explanation

This is a DECnet-VAX node problem involving the session layer. The error message indicates a problem on the remote node, potentially caused by any of the following:

- Improper protection on any of the following:
  - Requested object's executable and command files on the remote node
  - SYS$SYSTEM directory
  - NETSERVER.COM and NETSERVER.EXE files in the SYS$SYSTEM directory
  - Files pointed to by the SYS$LOGIN command file
  - Default DECnet directory
  - DCL tables in SYS$LIBRARY
- An error in the SYS$LOGIN command file
- An error in the default DECnet account's LOGIN.COM file (errors in this file force a logout)
- No LOGIN.COM file specified in the SYSUAF record for the default DECnet account (assuming the default DECnet account is captive)

  Other parameters in the SYSUAF record for the default DECnet account may also cause this symptom, such as an insufficient value for the BYTLM parameter.
- A user attempting to access a disabled account on the remote node
- An error in starting the requested object
- The LOGIN.COM file for the account may specify some kind of interactive use

  For example, the LOGIN.COM file may start a menu on login. This kind of interactive use may not work for remote DECnet connections.

Troubleshooting Strategy

A. Obtain the following information:

- Operation the user was performing
- Account the user attempted to access
- Object the user was accessing

B. Check the following:

- Setup of the account the user was accessing
- Protection on the object's executable and command files

C. Examine the NETSERVER.LOG file associated with the account for information explaining why the network link was aborted. Using the information in the NETSERVER.LOG file, you can correct the problem that caused the remote node to abort the link.

Troubleshooting Procedure

A. **Find out what operation the user was performing when the error occurred, and what account the user was accessing during the operation.**

The account might have been the user's account or the default nonprivileged DECnet account.

The type of access control the user specified helps you determine what account the user was accessing, for example:

- If the user specifies explicit access control information, access is through the account specified.
- If the user did not specify explicit access control information, access is through the default DECnet account or through a proxy account.
  - When access is through the default DECnet account, the system uses the account associated with the object requested. If no account is associated with the object requested, access is through the nonprivileged user account specified for the executor.
  - If a proxy exists, access is through the account pointed to by the proxy.

B. **Make sure that the accounts are set up properly on the remote node.**

For example, for proxy accounts, do the following:

1. Run AUTHORIZE, and use the following command to see if a proxy account is defined for the user's node and user name:

   ```
   UAF>  SHOW/PROXY local-node-id::user-id
   ```

2. If a proxy exists for the account, run NCP and use the following commands to see if incoming proxy access is enabled for both the object and the executor. (See Table 3–6 for information on proxy access settings.)

   ```
   NCP>  SHOW OBJECT object-name  CHARACTERISTICS
   NCP>  SHOW EXECUTOR CHARACTERISTICS
   ```

   NCP displays the current setting for incoming proxy access. If incoming proxy access is not enabled, then the system does not use the proxy to determine access. Instead, it grants access through the account associated with the object or the nonprivileged user account specified for the executor.

C. **Log in to the remote node and use the following command to check the network objects on the remote node:**

```
NCP>  SHOW KNOWN OBJECTS CHARACTERISTICS
```

Note the names of the files specified for the requested object.

D. **Use the following command to check whether the executable and command files for the requested object on the remote node have the proper file protection:**

```
$  DIRECTORY filename.exe, filename.com/PROTECTION
```

The file protection for the object's executable and command files should be world:read,execute. For example, if the user was attempting to copy a file, make sure that FAL.EXE and FAL.COM exist and have world:read,execute access specified.

E. **If the file protection for world access is other than read, correct it using the following DCL command:**

```
$  SET PROTECTION filename.exe, filename.com/PROTECTION=(W:R)
```

F. **Use the following command to display the NETSERVER.LOG file for the account on this node:**

```
$  DIRECTORY/DATE device:[directory]NETSERVER.LOG
```

If no NETSERVER.LOG file exists, go to step 9.

G. **Make sure that you have the correct NETSERVER.LOG file for the user's operation, and examine the NETSERVER.LOG file for errors.**

Often, the problem may be with a login command file. Some common error messages are:

- Error opening captive command procedure
- Duplicate process name
- Insufficient privilege or file protection violation

H. **Correct the error and tell the user to try the operation again.**

I. **If no current NETSERVER.LOG file exists, do the following:**

1. Make sure that you check the correct directory for the NETSERVER.LOG file.
2. If you have checked the correct directory, but no current NETSERVER.LOG file exists, check directory protections and file protections to see if they are preventing a NETSERVER.LOG file from being created. Possible reasons that a NETSERVER.LOG file has not been created include the following:
   - Improper protection on any of the following:
     - SYS$SYSTEM directory
     - Executable and command files in the SYS$SYSTEM directory for the object requested
     - NETSERVER.COM and NETSERVER.EXE files in the SYS$SYSTEM directory
     - Files pointed to by the SYS$SYSLOGIN command file
     - Default DECnet directory
     - DCL tables in SYS$LIBRARY
   - The user attempting to access a disabled account
   - No write access to the directory
   - No disk space
   - The existence of a NETSERVER.LOG file, version 32767 (NETSERVER.LOG;32767)
3. Correct the problem preventing creation of the NETSERVER.LOG file.
4. Recreate the original user action.

   If the original user action results in the Network Partner Exited message and the creation of a NETSERVER.LOG file, return to step G.

Node Out of Range Packet Loss

Symptoms

OPCOM displays one of the following messages:

```
Node out of range packet loss

Partial routing update loss
```

Explanation

These messages indicate a DECnet-VAX node problem, and usually occur when a new node joins the network. The messages result from one or both of the following:

A. A node on the network has a DECnet address that is too high for the network area of which it is a part.

   When this is the cause of the problem, the OPCOM messages usually occur on multiple nodes in the network.

   A DECnet network can consist of a maximum of 63 areas, and each DECnet area can consist of a maximum of 1,024 nodes. However, a DECnet network can define a maximum number of areas that is less than 63, and each DECnet area can define a maximum number of nodes that is less than 1,024.

   For example, assume a network has a maximum of 5 areas, with a maximum of 500 nodes per area. In this case, all DECnet addresses in the area must be 500 or less. If the DECnet area number is 5, the range of node addresses for that area is 5.1 through 5.500.

   If a node uses an area number that is greater than 5 or a node address greater than 500, the "node out of range packet loss" and "partial routing update loss" messages occur on nodes throughout the network when the incorrectly configured node announces its adjacency.

B. The routing tables on one or more nodes in the network are not large enough to perform routing or end node updates for another node's valid DECnet address.

   When this is the cause of the problem, the OPCOM messages usually occur on fewer nodes in the network than if the cause is an invalid (too high) DECnet address. In this case, the OPCOM messages occur only on the node or nodes that have insufficient routing tables.

Troubleshooting Strategy

Determine if the problem affects one node or multiple nodes.

A. If the problem affects many nodes on the network, check to see if a new node on the network has misdefined its DECnet address, and redefine the new node's address, if necessary.

B. If the problem affects only one or a few nodes, check the routing tables on the affected node or nodes to see if the routing tables are adequate. Increase the size of the routing tables, if necessary.

Troubleshooting Procedure

A. **If the problem affects many nodes, use the following steps to determine whether a node's DECnet address is too high, and to correct the address, if necessary.**

1. Log in to any node that displayed the OPCOM messages, and use the following command to enable the display of OPCOM messages on your terminal:

   ```
   $ REPLY/ENABLE=NETWORK
   ```

   OPCOM periodically displays various messages on your terminal, including the "node out of range" or "partial routing update packet loss" messages.

2. Run NCP and use the following command to display the local node's maximum address and maximum area definitions:

   ```
   NCP> SHOW EXECUTOR CHARACTERISTICS
   ```

3. Make a note of the maximum address and maximum area definitions.

   Step 5 uses this information to help you identify the problem node.

4. Set the maximum address and maximum area to the highest values possible, as follows:

   ```
   NCP> SET EXECUTOR MAXIMUM ADDRESS 1023
   NCP> SET EXECUTOR MAXIMUM AREA 63
   ```

   Setting the maximum address and maximum area parameters as shown prevents any further "node out of range" or "partial routing update packet loss" messages.

   Any nodes with DECnet addresses that were previously too high for the network now generate adjacency messages, which OPCOM displays on your terminal.

5. Look for an adjacency message for a node whose address is higher than your original maximum address and maximum area definitions.

   These messages indicate the node whose address is misdefined.

6. Get a correct address for the misdefined node from the person who assigns DECnet addresses on your network.

7. Log in to the misdefined node.

8. Run NCP and use the following commands to redefine the DECnet address correctly:

   ```
   NCP> DEFINE EXECUTOR ADDRESS address
   NCP> SET EXECUTOR STATE OFF
   NCP> EXIT
   ```

9. Restart the network on the redefined node using the following command:

   ```
   $ @SYS$STARTUP:STARTNET
   ```

10. Log in to the original node.

11. Use the following command to restart the network, thereby resetting the node's maximum address and maximum area parameters to their original settings:

    ```
    $ @SYS$STARTUP:STARTNET
    ```

B. **If the OPCOM message occurs on only one or a few nodes, do the following:**

   1. Log in to a node that is displaying the OPCOM message.

   2. Run NCP and use the following command to display the local node's maximum address and maximum area definitions:

      ```
      NCP> SHOW EXECUTOR CHARACTERISTICS
      ```

   3. Use the following commands to increase the size of the routing tables on the local node:

      ```
      NCP> DEFINE EXECUTOR MAXIMUM ADDRESS address
      NCP> SET EXECUTOR MAXIMUM ADDRESS address
      NCP> DEFINE EXECUTOR MAXIMUM AREA area
      NCP> SET EXECUTOR MAXIMUM AREA area
      ```

Partial Routing Update Loss

See Node Out of Range Packet Loss message.

Partitioned Area

Symptoms

A group of nodes in one area are unreachable from another area, or a significant number of areas are unreachable from an area. Users receive a variety of messages indicating that nodes or areas are not reachable, including "Path to network node lost" and "Remote node is not currently reachable," as well as various timeout messages.

With this symptom, some nodes in the unreachable area or areas may still be able to communicate with nodes in other areas.

> **Note**
>
> These symptoms do not necessarily indicate a partitioned area. What distinguishes the partitioned area problem from other related problems is that with partitioned areas, the group of nodes that is unreachable from a given location or locations can still be reached by other nodes on the network.

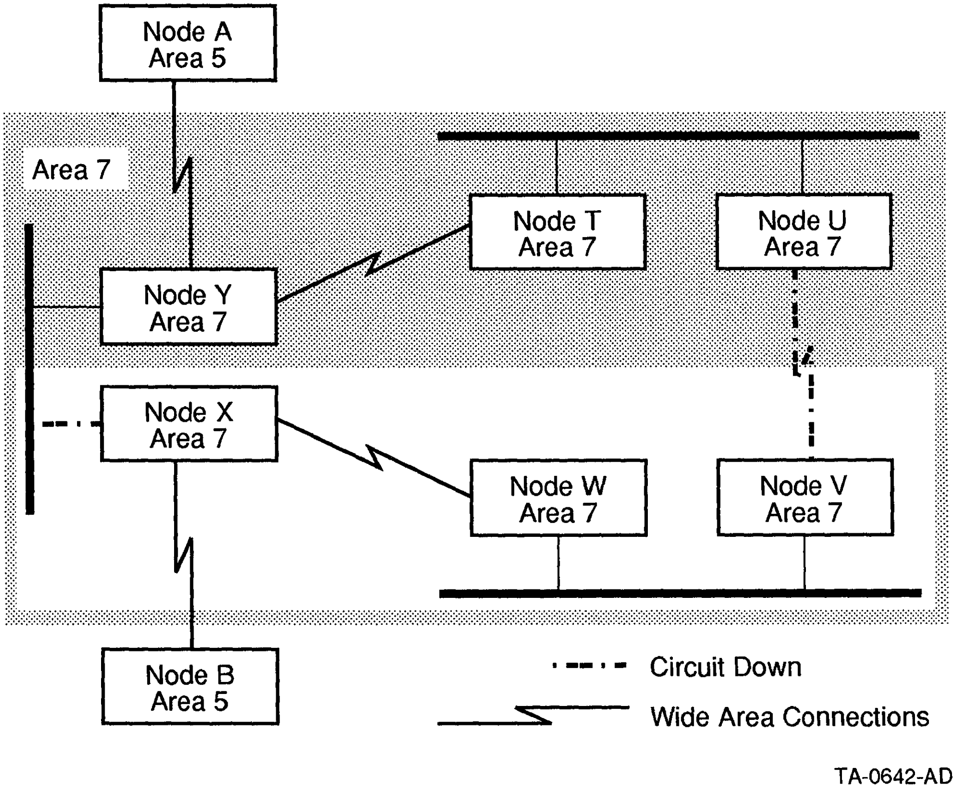
Explanation

This symptom indicates a DECnet WAN problem, which may be caused by one of the following:

- Failure of two or more area routers or circuits in an area, causing sections of an area to be unreachable.
- Failure to provide redundant circuits in an area. Redundant circuits help to ensure that no single point of failure exists between the level 2 routers in an area, by providing an alternate circuit to use in case one circuit fails. The path between level 2 routers cannot contain any level 1 routers.
- Failure of an area router's Ethernet controller.

Figure 3–2 shows how an area with redundant paths can become partitioned if two or more circuits fail. The dashed lines indicate the circuits that have failed. Because both of these circuits are unavailable, nodes V, W, and X are partitioned from nodes T, U, and Y.

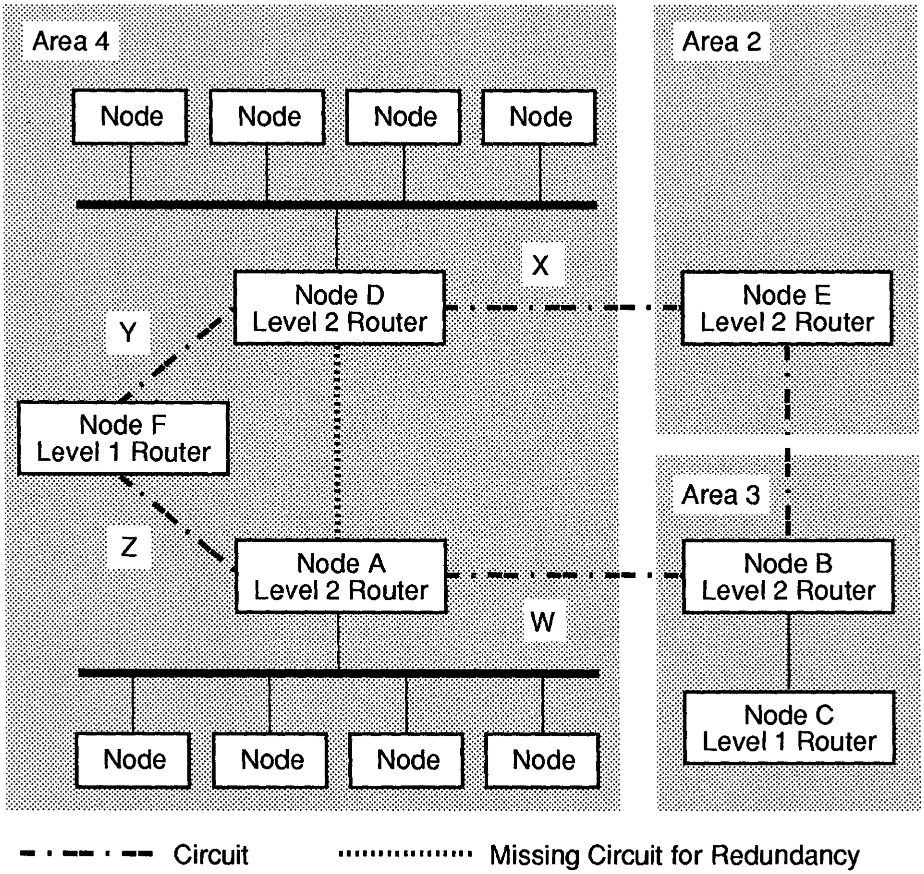
Figure 3–2 Area Partitioned Due to Multiple Failures



Partitioned Area

Figure 3–3 shows how an area that lacks redundant paths can become partitioned if one or more circuits fail.

Figure 3–3 Area Partitioned Due to Configuration Weaknesses



TA-0641-AD

In this figure, all circuit costs are equal to 1. The only path in Area 4 between the level 2 routers is through a level 1 router and circuits Y and Z. If all circuits are working, no problem exists. For example, node C in Area 3 attempts to communicate with node D in Area 4. If either circuit W or X fails, no problem arises because the remaining path into Area 4 provides a route to node D.

However, if circuits Y or Z fail, the level 2 router in Area 3 finds the path to the level 2 router in Area 4 on the basis of the least-cost algorithm: the path is from node C to node B to node A. Because circuit Y or Z is down, however, it is not possible to get to destination node D.

Another type of partitioned area problem occurs when a node in Area 4 tries to communicate with a node in Area 3, and circuit X is unavailable. The traffic cannot leave Area 4 because, with circuit X unavailable, there is no place for the traffic to go after it reaches the level 2 router, D. Circuit X is unavailable, and the traffic cannot revert to a level 1 router at this point. However, traffic coming into the area will be routed to the node without a problem. This is because incoming traffic is not subject to the same restrictions going through level 2 to level 1 routers as is outbound traffic.

Troubleshooting Strategy

The most important information to have in mind if you suspect a partitioned area problem on your network is what the network topology looks like. Specifically, you need to know the sites that make up the DECnet areas, the nodes used at each site for wide area routing, and the wide area circuits from the routers in an area to other sites and areas on the network.

You can use the Network Control Program (NCP) to query remote routers regarding the reachability of the suspected nodes and area. To query the correct routers, you must be familiar with the overall topology of your network.

To solve this problem, try to determine which areas can communicate with the suspected partitioned area, and which nodes within that partitioned area are reachable. By doing this, you isolate the cause of the failure and the partitioning, and you can focus on repairing the circuit or router that is causing the problem.

NMCC/DECnet Monitor can be especially helpful in isolating the cause of the problem.

Troubleshooting Procedure

A. **Determine which area is unreachable.**

B. **Trace the routing path from various areas in the network to determine which routers and circuits or which circuits are down.**

Look for circuits that are in the on-starting state and for malfunctioning routers.

C. **If it is possible to implement an interim solution that enables part of the partitioned area to communicate with the rest of the network, do so.**

D. **Repair the faulty circuits and routers, or faulty circuits.**

E. **Remove the interim solution.**

Recommendations

Try to avoid configurations, such as the one illustrated in Figure 3–3, that use straight-line configurations (as in Area 4). Also, provide a direct link between all level 2 routers. For example, in Figure 3–3, installing a link between nodes A and D provides an alternate path for nodes in that area.

Permission Denied

Symptoms

When using commands which are executed on remote hosts (such as rsh and rcp), the user receives the following message, and the operation fails:

```
Permission denied
```

Explanation

This problem affects ULTRIX hosts and involves the internet protocol (IP).

ULTRIX systems determine whether to permit access for remote users through one of the following files:

- .rhosts file
- /etc/hosts.equiv file

When the permission denied message occurs, the problem may be due to one or more of the following:

- Incorrect host and user definitions in the user's .rhosts file on the remote host
- Improper setup of the /etc/hosts.equiv file
- Improper directory or file protection on files to be copied or the .rhosts file

Note

This symptom may not indicate a problem. It is possible that the remote host may be intentionally preventing remote access. Before you try to resolve this problem, be sure that the user is intended to have access to the remote host.

Troubleshooting Strategy

Make sure that the following conditions are met:

- The .rhosts file on the remote host contains the proper host and user definitions.
- The /etc/hosts.equiv file is set up properly.

Permission Denied

- The directory and file protections are correct on the following files:
  - file to be copied
  - remote .rhosts file

Troubleshooting Procedure

Do the following on the remote host:

1. Display the contents of the /etc/hosts.equiv file, to determine if the user's host name is in that file:

   ```
   # grep hostname /etc/hosts.equiv
   ```

   - If the command returns you to the prompt, no entry exists in the /etc/hosts.equiv file for the host name you specified. If your site's security policy permits, you can edit the /etc/hosts.equiv file and add the host name.

   Note

   If you mistype the host name in the grep command, grep will not locate the host name even if the host name is in the file. Before you make any changes to the /etc/hosts.equiv file confirm that the host is not already in the /etc/hosts.equiv file.

   - If the command displays an entry, make sure the host name is correct for the user.
   - If the entry is incorrect, modify the file to contain the correct definitions.
2. Use the following command to move to the user's login directory so you can check the .rhosts file:

   ```
   # cd users_login_directory_name
   ```
3. Use the ls command to determine if a .rhosts file exists.
4. If the user's login directory does not contain a .rhosts file, use a text editor to create one that contains the correct user name and host name for the user.
5. If the user's login directory has a .rhosts file, use the following command to display its contents:

   ```
   # grep hostname .rhosts
   ```

If the user or host name is missing or incorrect, modify the .rhosts file so that it contains the correct definitions.

Note

Be aware that some name services require the full domain name form of a host name, some require only a shortened form of the domain name. Be sure to use the proper form for the name service you use.

Also, if you are *not* running the domain name system with long names, your /etc/hosts file must not define host names with a long name directly following the IP address. If you are using short host names, then make sure your /etc/hosts file has short names only.

6. Make sure that the local host knows about the remote host.

   Although the local host may receive the message, permission denied, the true cause of the problem may be that the remote host is unknown. See "Unknown Host" in this chapter for more information on how to correct this problem.

7. Use the following command to confirm that you are in the user's login directory:

```
# pwd
```

8. From the user's directory, use the following command to check the directory and file protections on any files the users wants to access (including .rhosts):

```
# ls -l file-name
```

   The user needs read access at the file level.

9. If the files do not have read privilege, use the following command to change the file and directory protection:

```
# chmod u+r file-name
```

10. Use the following command to display the protection on the directory:

```
# ls -l -d
```

   The user needs read and write privileges to use rcp.

11. If the directory does not have read and write privileges, use the following command to change the file and directory protection:

```
# chmod u+w,r directory-name
```

Remote Node Is Not Currently Reachable

Symptoms

A user gets the following message when attempting any network operation:

```
%SYSTEM-F-UNREACHABLE, remote node is not currently reachable
```

This message occurs when a user tries to establish a connection to a remote node, or when a user tries to reestablish a connection that was lost. This message may also occur when a user tries to connect to a cluster system using the cluster alias. The connection fails when the user specifies the cluster alias, but succeeds if the user specifies a particular node in the cluster.

Explanation

This symptom indicates a node, LAN, or WAN problem, and means that the remote node is not reachable through DECnet. This symptom may be due to any of the following:

- The remote node is not running.
- The lines and circuits may not be operating properly on the local or remote node.
- A routing node may not be running or operating properly.
- A problem exists on the routing path.
- The remote node may be incorrectly defined in the NCP node database of the local node.
- The local node may have setup problems such as the following:
  - Circuit, line, or both may not be defined.
  - Values for MAXIMUM HOPS, MAXIMUM COSTS, and MAXIMUM VISITS might be too low.
- If the remote system is a cluster system, there may be setup problems such as the following:
  - MAXIMUM BROADCAST NONROUTER parameter for the routing node is set too low.
  - Cluster system has not defined one of the nodes to be the routing node for the cluster. In a cluster system, at least one node has to be the routing node.

- ENQUEUE limit on NETACP on the routing system is too low.

Troubleshooting Strategy

The troubleshooting procedure explains how to solve the problem if it is on the local node, the routing path, or the remote node.

A. Check the following on the local node:

- Remote node's address in the local node's volatile node database
- Local node's circuits and lines
- Values of MAXIMUM HOPS, MAXIMUM COSTS, and MAXIMUM VISITS
- ENQUE limit values for NETACP

B. Trace the routing path to determine if the problem is on the routing path or the remote node.

If the problem is on the routing path, do loopback tests or reachability tests to determine the cause.

C. If the problem is on the remote node, check the following on the remote node:

- Remote node is running.
- DECnet is running.
- Circuits and lines are operating properly.
- Cluster aliasing is set up properly.
- ENQUE limit for NETACP is correct.

Troubleshooting Procedure

A. **Do the following to determine if the local node is the cause of the problem:**

1. Use the following steps to determine if the remote node's node address is correctly defined in the local node's volatile node database, and to redefine it, if necessary.

   a. Determine if the node address for the remote node is properly defined by checking the local node's definition against the master list of node definitions maintained for your network. Usually a single node (called *master-list-node* in the following example) maintains the master list of node definitions.

Run NCP, and use the following commands to get this information:

```
NCP> SHOW NODE node-id
NCP> TELL master-list-node SHOW NODE node-id
```

b. If the preceding commands display different node definitions for the remote node, use the following command to define the node address to the definition displayed by the master-list-node:

```
NCP> CLEAR NODE node-id ALL
NCP> PURGE NODE node-id ALL
NCP> DEFINE NODE node-address NAME node-id
NCP> SET NODE node-id ALL
```

2. Use the following steps to check the lines and circuits on the local node:

   a. Run NCP and use the following commands to determine the status of the lines and circuits:

   ```
   NCP> SHOW KNOWN LINES
   NCP> SHOW KNOWN CIRCUITS
   ```

   b. If the circuit state is on-starting, go to the corrective action for "Circuit State Problems" in this chapter.

   c. If the lines and circuits are not on, use the following commands to turn them on:

   ```
   NCP> SET LINE line-id STATE on
   NCP> SET CIRCUIT circuit-id STATE on
   ```

3. Check the MAXIMUM HOPS, MAXIMUM COSTS, and MAXIMUM VISITS values, and modify them, if necessary, using the following NCP commands:

   a. Use the following command to display the current values for the MAXIMUM HOPS, MAXIMUM COSTS, and MAXIMUM VISITS:

   ```
   NCP> SHOW EXECUTOR CHARACTERISTICS
   ```

   A value of 15 for MAXIMUM HOPS is usually sufficient, unless your network is particularly wide. The MAXIMUM VISITS value should be two times the value of MAXIMUM HOPS.

Note

Use care in increasing the MAXIMUM HOPS value because a higher MAXIMUM HOPS value on routing systems can cause increased routing traffic. The increased traffic can cause the network to take longer to stabilize when a system stops running.

b. Use the following NCP commands to increase the MAXIMUM HOPS, MAXIMUM COSTS, and MAXIMUM VISITS values:

```
NCP>  SET EXECUTOR MAXIMUM HOPS value
NCP>  SET EXECUTOR MAXIMUM COSTS value
NCP>  SET EXECUTOR MAXIMUM VISITS value
```

4. If the local node is part of a Local Area VAXcluster, the problem may be related to ENQUE limits. Do the following to resolve problems related to ENQUE limits:

   a. Use the following command to display the current ENQUE limit value:

   ```
   $  SHOW LOGICAL NETACP$ENQUEUE_LIMIT
   ```

   The ENQUE limit on the routing node for NETACP must be two times the number of satellites plus 10.

   b. If the ENQUE limit is too low (as determined in step a), and DECnet has not started, use the following command to increase the value, otherwise, go to step c:

   ```
   $  DEFINE/SYSTEM NETACP$ENQUEUE_LIMIT xxx
   ```

   c. If the ENQUE limit is too low (as determined in step a), and DECnet has started, use the following commands to increase the value:

   ```
   $  DEFINE/SYSTEM NETACP$ENQUEUE_LIMIT xx
   $  MCR NCP
   NCP>  SET EXECUTOR STATE OFF
   NCP>  EXIT
   $  @STARTNET.COM
   ```

B. **Trace the routing path to determine if the problem is on the routing path or on the remote node.**

If the problem is on the routing path, use loopback, modem, and circuit tests on the routing path (at the disconnect point) to help determine the source of the problem.

If the problem is on the remote node, go to the next step.

C. **If the problem is on the remote node, do the following:**

1. Make sure that the remote node is running.
2. On the remote node, use the following command to make sure that DECnet is running:

   ```
   $ SHOW NETWORK
   ```

3. On the remote node, use the following steps to check the lines and circuits on the node:

   a. Run NCP, and use the following commands to make sure that the lines and circuits are on:

   ```
   NCP>  SHOW KNOWN LINES
   NCP>  SHOW KNOWN CIRCUITS
   ```

   b. If the circuit is on-starting, go to the corrective action for "Circuit State Problems" in this chapter.

   c. If the lines and circuits are not on, use the following command to turn them on:

   ```
   NCP>  SET LINE line-id STATE ON
   NCP>  SET CIRCUIT circuit-id STATE ON
   ```

4. If the remote node is part of a VAXcluster, use the following steps to resolve problems related to the MAXIMUM BROADCAST NONROUTER parameter:

   a. Run NCP, and use the following command to display the value for the MAXIMUM BROADCAST NONROUTER parameter:

   ```
   NCP> SHOW EXECUTOR CHARACTERISTICS
   ```

   The value for MAXIMUM BROADCAST NONROUTER specifies the number of nonrouting nodes (end nodes) the executor node can have on its Ethernet circuits. The value for MAXIMUM BROADCAST NONROUTER should be at least the number of nonrouting (end nodes) on the Ethernet. The default value is 64.

   b. If it is necessary to increase the MAXIMUM BROADCAST NONROUTER parameter, use the following NCP command:

   ```
   NCP> SET EXECUTOR MAXIMUM BROADCAST NONROUTER n
   ```

5. If the remote node is part of a VAXcluster, use the following commands to resolve problems resulting from improper setup of the cluster:

   a. Run NCP, and use the following command on each node in the cluster to display the routing status of each:

   ```
   NCP> TELL NODE node-id SHOW EXECUTOR CHARACTERISTICS
   ```

Check the type displayed for the node. The cluster must have a router defined (designated as ROUTING IV) and the router must be running for the cluster alias to work.

b. If the cluster does not have a router defined, define one, using the following commands:

   1. Shut down the network on the cluster using the following NCP command:

      ```
      NCP> SET EXECUTOR STATE OFF
      ```

   2. Change the executor type using the following command:

      ```
      NCP> DEFINE EXECUTOR TYPE ROUTING IV
      ```

   3. Execute the STARTNET.COM file to restart the network:

      ```
      $ @STARTNET.COM
      ```

   4. If the router is defined but not running, restart it or define another node to be the routing node.

c. If the remote node is part of a Local Area VAXcluster, the problem may be related to ENQUE limits. Use the following commands to resolve problems related to ENQUE limits:

   1. Check LOADNET.COM for the current value of ENQLM.

      The ENQUE limit on the routing node in NETACP must be two times the number of satellites plus 10.

   2. If the ENQUE limit is too low, and DECnet *has not* started, use the following command to increase the value; otherwise, go to step 3:

      ```
      $ DEFINE/SYSTEM NETACP$ENQUEUE_LIMIT xx
      ```

   3. If the ENQUE limit is too low (as determined in step a), and DECnet *has* started, use the following commands to increase the value:

      ```
      $ DEFINE/SYSTEM NETACP$ENQUEUE_LIMIT xx
      $ MCR NCP
      NCP> SET EXECUTOR STATE OFF
      NCP> EXIT
      $ @STARTNET.COM
      ```

Verification Reject

Symptoms

A circuit alternates between the on-starting and on-synchronizing states, and OPCOM displays verification reject messages, such as the following. This problem is most common with dial-in connections to DECnet networks.

```
       %%%%%%%%%%%  OPCOM  19-OCT-1990 15:37:07.40  %%%%%%%%%%%
       Message from user DECNET on NODE1
DECnet event 4.6, verification reject
From node 56.689 (NODE1), 19-OCT-1990 15:37:07.35
Circuit TX-0-6, Node = 56.1014 (NODE2)

%%%%%%%%%%%  OPCOM  19-OCT-1990 15:37:20.65  %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.6, verification reject
From node 56.689 (NODE1), 19-OCT-1990 15:37:20.59
Circuit TX-0-6, Node = 56.1014 (NODE2)

%%%%%%%%%%%  OPCOM  19-OCT-1990 15:37:30.66  %%%%%%%%%%%
Message from user DECNET on NODE1
DECnet event 4.6, verification reject
From node 56.689 (NODE1), 19-OCT-1990 15:37:30.59
Circuit TX-0-6, Node = 56.1014 (NODE2)
```

Explanation

This symptom indicates a DECnet-VAX node problem. The DECnet routing layer provides a means for verifying passwords between adjacent nodes, known as *circuit verification*. Because circuit verification can disallow access from one node to another, it provides additional security for DECnet nodes.

You can set passwords and enable circuit verification on a node-by-node basis. Because of this, nodes can be adjacent to a node through different circuits, and multiple nodes can be adjacent to a node through a single circuit.

A node may receive a verification reject message from a node to which it is intended to have access because the passwords between the two nodes have been improperly defined.

Troubleshooting Strategy

1. Determine whether the two nodes in question are intended to have verification enabled.
2. If verification is not required, disable it.
3. If verification is required, ensure that the transmit and receive passwords for each node are properly defined.

Troubleshooting Procedure

A. **Find out if the verification is required for the two nodes.**

B. **If verification is not necessary, run NCP, and disable verification on each node using the following command:**

```
NCP> SET CIRCUIT circuit-id VERIFICATION DISABLED
```

C. **If verification is required, make sure that the local and remote node passwords are properly defined.**

1. On each node, use the following command to display the other node's executor characteristics, including transmit and receive passwords, if any exist.

   ```
   NCP> SHOW NODE remote-node-id CHARACTERISTICS
   ```

   If the remote node has transmit or receive passwords defined, the local node's transmit password must match the remote node's receive password. Likewise, the local node's receive password must match the remote node's transmit password.

2. Use the following commands to set up coordinated transmit and receive passwords on the local and remote nodes.

   On the first node:

   ```
   NCP> SET NODE remote-node TRANSMIT PASSWORD password_a-
   _NCP> RECEIVE PASS password_b
   ```

   On the second node:

   ```
   NCP> SET NODE remote-node TRANSMIT PASSWORD password_b-
   _NCP> RECEIVE PASSWORD password_a
   ```

PC-Based Messages

This section lists PC-based DECnet messages in alphabetical order. Each message is followed by an explanation of its probable cause.

Configuration parameters in DECPARM.DAT exceed the data segment size. Use NCP to lower settings to reduce memory usage.

Explanation: The memory used in the combination of the following resources:

- MAX LINKS (NCP option or /MAX: command line switch)
- MS-NET names (stored in DECNODE.DAT plus /MSN:nn switch)
- REMOTE ADAPTER names (stored in DECREM.DAT, plus /REM:nn)
- Request blocks (/REQ:nn switch)
- Small Data Blocks (/SDB:nn switch)

exceeds 64K, or the size of available memory. Reduce NCP or command-line parameters to make DNP smaller so it will fit in memory.

Could not activate DECnet portal in the datalink.

Explanation: DNNETH could not register itself with the datalink driver, or datalink did not bind to NDIS driver. This indicates a potentially serious configuration problem in the datalink. This error should never happen.

Could not activate DECnet processes in the scheduler.

Explanation: DNNETH could not register itself with the scheduler. This indicates a potentially serious configuration problem in the scheduler. This error should never happen.

Could not open DECPARM.DAT, using defaults.

Explanation: This message indicates that DNP could not open DECPARM.DAT, which contains essential DECnet parameters such as the node name and node address. The "defaults" cause DNP to be loaded without a node name or address. Node name and address must be set with NCP before DNP will run normally.

Could not read DECPARM.DAT (file error).

Explanation: A file read error occurred on DECPARM.DAT. Restore DECPARM.DAT from a backup or recreate it with NCP.

DECnet node name or address not initialized. Use NCP to set node name before starting DNP.

Explanation: The DECnet node name and address in DECPARM.DAT is invalid. Use NCP to DEFINE the name and address (NCP DEF EXEC NAME/ADDR) before starting DNP.

DNP cannot be loaded under Windows or the task switcher.

Explanation: All PATHWORKS Terminate and Stay Resident (TSR) software must be loaded before invoking a task switcher, such as DOS V5 DOSSHELL, or any shell program, such as Microsoft Windows.

DNP has already been installed.

Explanation: DNNETH has already been installed.

DNP installed successfully.

Explanation: This message indicates that DNP has been installed successfully into conventional memory.

DNP loaded into EMS successfully.

Explanation: This message indicates that DNP has been installed successfully into EMS (expanded) memory.

Invalid parameter on command line switch.

Explanation: The parameter to the command line switch is invalid (out of range, and so on).

Invalid switch on command line

Explanation: One of the command line switches to DNP is invalid. Run DNNETH /? for a list of valid switches.

Not enough parameters to start DECnet. You must specify both the /NAME: and /ADDR: switches.

Explanation: If you specify the /NAME: parameter, you must also specify the /ADDR: parameter. Both parameters must be specified, or neither. If both are specified, it overrides DECPARM.DAT and starts DNP without reading it.

Parameter missing on command line switch.

Explanation: The command-line parameter required a value, and it was not specified. Use DNNETH /? for help.

The datalink is not loaded. Run DLL before running DNNETH.

Explanation: The datalink must be present in order to run DNNETH. If using DLLNDIS, the NETBIND program must be run before DNNETH will run.

The scheduler is not loaded. Run SCH before running DNNETH.

Explanation: The network scheduler (SCH) must be loaded before running DNNETH.

Warning: DNP should be used with datalink version 4.1 or later.

Explanation: DNP will issue this message when you try to run it with a pre-4.1 datalink.

You cannot run the debugging version on an 8086/8088.

Explanation: This message is displayed if the debug version is run on an 8086 or 8088—a 286 processor or greater must be used to run the debug version.

Part 2

Transmission Control Program and Internet Protocol (TCP/IP)

4
TCP/IP Tools

This chapter describes the TCP/IP troubleshooting tools used with each operating system. It includes the following sections:

- VMS Tools
- ULTRIX Tools
- DOS Tools

Locate the section with the operating system you need and use the tools as described.

Table 4–1 lists the troubleshooting tools with operating system(s), function, and use.

Table 4–1 Troubleshooting Tools

Tool	Operating System(s)	Function	Use
arp command	ULTRIX, DOS	Displays the internet-to-Ethernet address translation for host name entered.	Helps find incorrect addresses or duplicate names.
Log files	VMS, ULTRIX	Collects system and network information.	Helps identify point of failure.
LOOP command	VMS	Tests connectivity between two computers.	Verifies two computers can communicate.

(continued on next page)

Table 4–1 (Cont.) Troubleshooting Tools

Tool	Operating System(s)	Function	Use
IVP	VMS	Performs Installation Verification Procedure.	Verifies correct installation of protocols.
netstat command	ULTRIX, DOS	Displays statistics about network operations.	Helps identify failing network operations.
ping command	ULTRIX, DOS	Sends a test packet to host and checks for a response.	Helps find network routing problems and single-point failures.

VMS Tools

This section describes the TCP/IP troubleshooting tools used with the VMS operating system.

Log Files

VMS provides several log files that collect information useful for troubleshooting. The log files are listed with a brief description and instructions on their use. The information provided by the log files includes the following:

- System events
- User requests
- Network operations
- Hardware error messages
- Accounting statistics

SYS$MANAGER:OPERATOR.LOG

This log file receives information from the operator communications manager (OPCOM) about system events and user requests. OPCOM can provide information about events preceding a network problem. This can help you anticipate and prevent hardware/software failures.

Perform the following steps to start OPCOM:

1. Log in to a VMS account with OPER privileges.
2. Enter the following command:

```
$ @SYS$SYSTEM:STARTUP.COM OPCOM
```

Perform the following steps to enable event logging using OPCOM:

1. Run NCP.
2. At the NCP prompt, enter the following commands:

   ```
   NCP> SET LOGGING MONITOR KNOWN EVENTS
   NCP> DEFINE LOGGING MONITOR KNOWN EVENTS
   NCP> SET LOGGING MONITOR STATE ON
   NCP> DEFINE LOGGING MONITOR STATE ON
   ```

VMS Netserver Log File

These log files obtain information from the account that initiates the login sequence. The location of the log file depends upon how access is attempted. The log file can be in one of the following locations:

- Default nonprivileged DECnet account
- Object account
- Proxy account
- Any account accesses using explicit access control information

SYS$ERRORLOG:ERRLOG.SYS

This log file contains all hardware errors for the VMS system. Because it documents the errors and events preceding a failure, it is useful in diagnosing network problems.

You can display the log file information by typing in the following DCL command:

```
$ SHOW ERROR
```

You can generate a complete report of the errors with a history and detailed description by performing the following steps:

1. Verify that you have SYSPRV privilege (required to access the error log).
2. Set default to SYS$ERRORLOG.
3. Display the directory to see which error log you want to analyze.
4. Enter the following command:

   ```
   $ ANALYZE/ERROR_LOG/OUTPUT=ERRORS.LIS
   ```

SYS$MANAGER:ACCOUNTNG.DAT

This log file contains statistics on the use of system resources. You must have read access to use the accounting log file. It is useful for tracking job-specific problems such as those involving NETACP and REMACP.

LOOP Command

The LOOP command enables you to test the connectivity between two computers. You can use the LOOP command to test the connection between the server and client(s).

To execute a loop test between a client and a server, enter the LOOP command with the node address of the server as follows:

```
UCX>  LOOP NODE node_id
```

If the LOOP command does not work, check the physical network connections and verify the Internet parameters.

Installation Verification Procedure (IVP)

The VMS/ULTRIX Connection (UCX) kit includes a command procedure named the Installation Verification Procedure (IVP). IVP verifies that the installation and operation of Internet software is correct. IVP does not measure Internet or computer performance.

If a Product Authorization Key (PAK) has been loaded, IVP verifies that the complete Internet software is installed correctly. If a PAK has not been loaded, IVP only verifies that the TCP/IP component has been installed to ensure that TCP/IP DECwindows will work correctly.

The IVP procedure is named UCX$IVP.COM and is placed in the SYS$TEST directory when you install the Connection.

The UCX$IVP.EXE image file is independent of the Connection software and can be deleted. However, it is strongly recommended you keep the file in case you need to run IVP again.

You must successfully execute the network configuration procedure (UCX$CONFIG.COM) before running IVP the first time. You can optionally run IVP as part of the network configuration procedure, or by itself at any time afterwards.

To run IVP, you need the following account privileges:

- SYSPRV
- OPER
- NETMBX
- TMPMBX or SETPRV (to set the other privileges)

RUNNING IVP

To run IVP independently of UCX$CONFIG.COM, enter the following command:

```
$ @SYS$TEST:UCX$IVP
```

IVP Messages

IVP messages use the same format as standard VMS messages, as follows:

```
UCX-E-IDENT, text_message
```

IVP tests the TCP/IP protocols by transferring device-socket packets between a sender and receiver. Optional testing of UDP/IP and IP protocols occurs if a PAK is installed.

The packets continuously vary in size. The UDP/IP and TCP/IP packets start at 8 bytes and stop at 8195 bytes. The IP packets start at 8 bytes and stop at 2048 bytes. The sent and received packets are compared to detect corrupted data or invalid lengths.

IVP provides information and error messages to inform you of test status and results.

Information Messages

IVP provides information messages to show IVP startup, completion, and results.

Startup Message

IVP provides the following message format at startup:

```
%%% VMS/ULTRIX Connection Internet IVP started
at 'system time' %%%
```

Completion Message

IVP provides the following message format at completion:

```
%%% VMS/ULTRIX Connection Internet IVP completed
at 'system time' %%%

'protocol' test started at 'system time'

        - communication protocol IVP completion

'protocol' test ended at 'system time'
'protocol' transferred successfully in 'time interval'
seconds nnn bytes
```

Results Message

IVP provides the following message format when a PAK is installed. A similar format is used when a PAK is not installed. The execution times depend upon your installation.

```
%%% VMS/ULTRIX Connection Internet IVP started
at dd-mmm-yyyy hh:mm:ss.cc %%%

UDP/IP test started at dd-mmm-yyyy hh:mm:ss.cc

UDP/IP test ended at dd-mmm-yyyy hh:mm:ss.cc

UDP/IP transferred successfully in nn seconds
nnn bytes

TCP/IP test started at dd-mmm-yyyy hh:mm:ss.cc

TCP/IP test ended at dd-mmm-yyyy hh:mm:ss.cc

TCP/IP transferred successfully in nn seconds
nnn bytes

RAW_IP test started at dd-mmm-yyyy hh:mm:ss.cc

RAW_IP test ended at dd-mmm-yyyy hh:mm:ss.cc

RAW_IP transferred successfully in nn seconds
nnn_bytes

%%% VMS/ULTRIX Connection Internet IVP completed
at dd-mmm-yyyy hh:mm:ss.cc %%%
```

Error Messages

If an error is detected, IVP informs you of the failure and exits. All IVP errors are fatal because they indicate incorrect installation. Error messages are in the following format:

```
%%% VMS/ULTRIX Connection Internet IVP error 'error message'
'system time' %%%
```

The following is a list of possible error messages:

- Internet (BG0:) Device Assign
- Local Host Not Found
- Local Host Name Not In Hosts Data Base
- Create and Bind Sender Device-Socket
- Create and Bind Receiver Device-Socket
- Connect on Device-Socket
- Listen on Device-Socket
- Accept on Device-Socket

- Sender Device-Socket
- Receiver Device-Socket
- Invalid Length
- Data Corruption
- Send Shutdown on Device-Socket
- Receive Shutdown on Device-Socket
- Close Sender on Device-Socket
- Close Receiver on Device-Socket
- Deassign Sender Device-Socket
- Deassign Receiver Device-Socket

Typical error conditions and corrective actions are listed in Table 4–2.

Table 4–2 IVP Error Messages

Error Condition	Corrective Action
Incorrect network configuration.	Reconfigure the network.
Startup failure.	Restart the server. SYSGEN parameters may need to be increased before restarting.
Bad installation kit.	Replace the installation kit.

ULTRIX Tools

This section describes the TCP/IP troubleshooting tools used with the ULTRIX operating system.

arp Command

This command displays and changes the internet-to-Ethernet address translation tables used by the Address Resolution Protocol (ARP).

The **arp** command helps you find direct routing problems caused by incorrect internet addresses or hosts with identical names.

You must log in to the superuser account to use the **arp** command for changing entries in the address translation tables.

To run **arp**, enter the following command:

```
# /etc/arp hostname
```

Examples

The following example shows the Ethernet address for the internet host named sleepy as aa:0:3:0:7a:10.

```
# /etc/arp sleepy

sleepy (14.20.30.4) at aa:0:3:0:7a:10
```

netstat Command

This command displays the status of network-related data. You can also use it to obtain network routing path information for a remote host.

The **netstat** command enables you to display the following information:

- List of active sockets for each protocol
- Contents of network data structures
- Packet traffic information
- State of active sockets
- Memory management routines
- Statistics for each protocol

To run **netstat**, enter the following command:

```
# netstat [options]
```

The **netstat** command options specify the network information you want. The case-sensitive options are listed in Table 4–3.

Table 4–3 netstat Command Options

-A	Address of associated protocol control blocks.
-a	Information for all sockets.
-f {address_family}	Statistics or address control block reports for the specified address family.
-h	State of the IMP host table.
-I {interface}	Information about the specified interface only.
-i	Status information for autoconfigured interfaces.
-m	Information for the memory management routines.

(continued on next page)

Table 4–3 (Cont.) netstat Command Options

-n	Network addresses in number form rather than symbolic form.
-r	Routing tables.
-s	Statistics per protocol.
-t	Time until interface watchdog routine starts.

Perform the following steps to obtain the network routing path for a remote host:

1. Display the local host's routing tables and find the IP router used to reach the destination network.
2. Display the routing tables for the local host's IP router.
3. Continue displaying routing tables for each IP router in the path until you reach the destination network and host.

ping Command

This command performs an ICMP request to the specified host. The **ping** command sends a packet to the host you specify and tells you whether the host responds or not.

You can use the **ping** command for direct and indirect routing problems such as host unreachable, connection timed out, and network unreachable.

To run **ping**, enter the following command:

```
# /etc/ping [options] hostname
```

The **ping** command options are listed in Table 4–4.

Table 4–4 ping Command Options

-l	Displays the long version of the ping results.
-v	Displays the verbose version of the ping results. This includes other ICMP packets in addition to the ECHO RESPONSE packets.
-r	Bypasses normal routing tables and sends the request to a host directly attached to the same network.
no options	If you do not enter an option the remote host replies with the message "hostname is alive". If there is no response to the Echo Request packet, the ping command displays the message "no answer from host".

Log Files

ULTRIX provides a log file that collects information useful for troubleshooting. This information includes the following:

- Hardware errors
- Software errors
- Information messages
- Emergency messages
- Warnings on abnormal conditions
- Debugging information

The ULTRIX error log file is:

```
/usr/adm/syserr/syserr.hostname
```

You must use the **uerf** command to decode the file. The log file contains information about system hardware and the software kernel, as well as system status, startup, and diagnostic information.

ULTRIX Counters

Counter information and resulting calculations are provided by SNMP-based tools. Because these tools are site-specific, you need to refer to your site documentation for the tool used and details about the ULTRIX counters.

DOS Tools

This section describes the troubleshooting tools used with the DOS operating system.

arp Command

This command displays and changes the internet-to-Ethernet address translation tables used by the Address Resolution Protocol (ARP).

The **arp** command helps you find direct routing problems caused by incorrect internet addresses or nodes with identical names.

The **arp** program first resolves the host name to its IP address and then looks for the IP address in the ARP table. If the IP address is not in the ARP table the program displays the host name and the message no entry.

To run **arp**, enter the following command:

```
arp [options]
```

The **arp** command options are listed in Table 4–5.

Table 4–5 arp Command Options

-a	Displays all the current ARP table entries.
-c	Clears the entire ARP table.
no options	If you do not enter an option, the command syntax and options are displayed.

Examples

The following example contains a valid host name and displays the ARP entry.

```
C:> arp goofy
29.212.18.123
```

The following example contains an invalid host name and the ARP response.

```
C:> arp sherlock
unknown host sherlock
```

The following example contains a valid host name without an IP address in the ARP table.

```
C:> arp panda
No ARP Entry for panda
```

netstat Command

This command displays the statistical information gathered by the protocol driver from the different levels of the TCP/IP protocol stack.

The information is modeled after the Management Information Base (MIB) described in RFC-1066.

To run **netstat**, enter the following command:

```
netstat [options]
```

The **netstat** command options are listed in Table 4–6.

Table 4–6 netstat Command Options

-t	Displays the TCP MIB objects and TCP connection information.
-u	Displays the UDP MIB objects.

(continued on next page)

Table 4–6 (Cont.) netstat Command Options

-i	Displays the IP and ICMP MIB objects.
-c	Displays the static configuration information at startup, including the drivers' version strings.
-a	Displays all of the above.
no options	If you do not enter an option the command syntax and options are displayed.

ping Command

This command performs an ICMP request to the specified host. The **ping** command sends a packet to the host you specify and tells you whether the host responds or not.

You can use the **ping** command for direct and indirect routing problems such as host unreachable, connection timed out, and network unreachable.

The **ping** command sends an ICMP ECHO_REQUEST datagram to the host and waits for an ICMP ECHO_RESPONSE.

To run **ping**, enter the following command:

```
ping hostname [timeout]
```

The host name can be a name or internet address.

The default timeout period is 20 seconds. You can enter an optional value in seconds, up to a maximum of 300 seconds.

If you enter the command without a host name, the command syntax and options are displayed.

5

Isolating TCP/IP Problems

This chapter consists of the TCP/IP problem-isolation flowcharts and a series of troubleshooting procedures. The flowcharts help you isolate a network problem. When you isolate the problem, a decision point leads you to a specific procedure or set of procedures to fix the problem. You can locate the starting page for each procedure in the Contents or in the Index.

This chapter provides the following master procedures:

- VMS Server Master Procedure (TCP/IP)
- ULTRIX Server Master Procedure (TCP/IP)
- DOS Client Master Procedure (TCP/IP)
- Troubleshooting Hardware and Configuration (TCP/IP)

TCP/IP Problem-Isolation Flowcharts

You must consider several key questions to isolate a network problem. The answer to each question determines which procedures you should perform. This section contains a table and a series of flowcharts that guide you through the procedures.

The first key question asks if the network has ever carried traffic. If the answer is no, perform the VMS or ULTRIX Server Master Procedure. This master procedure combines three procedures into one. You may not have to perform all of the subprocedures in the master procedure.

The remaining flowcharts ask questions specific to your network. The procedure you use depends on your answer to the questions. You may have to perform client, file server, or printer server procedures.

Note

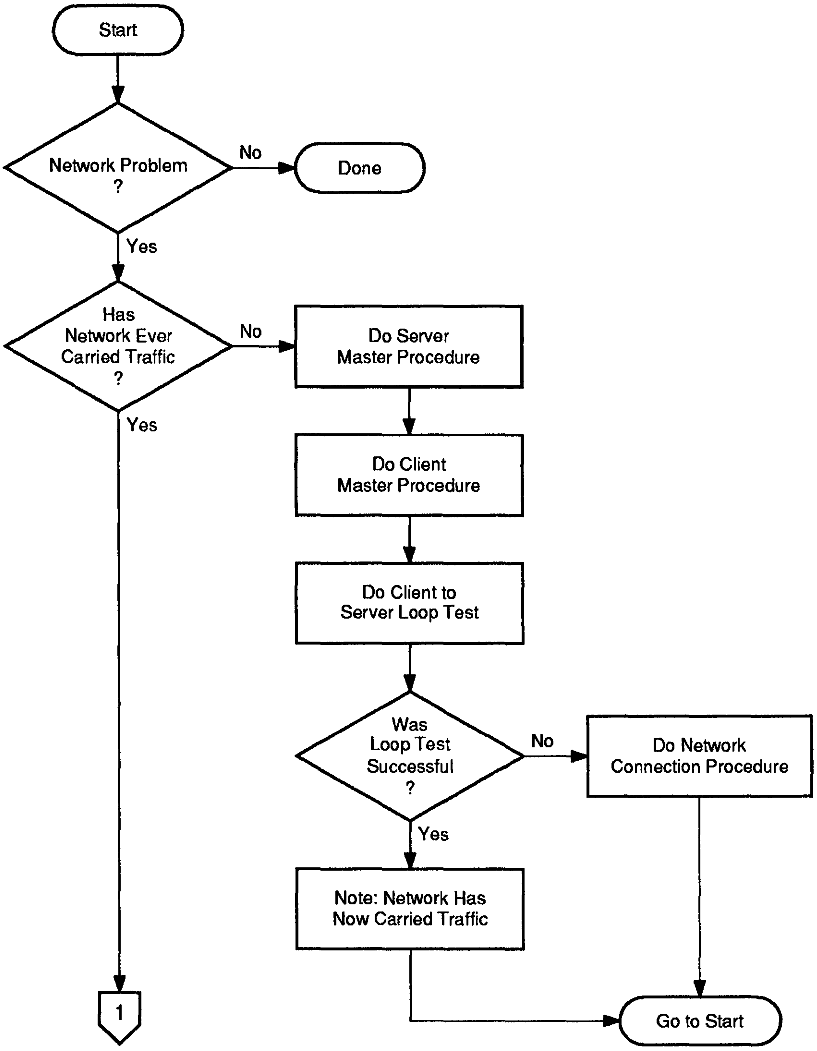
You should address each question in order. The answers to each question help you rule out unlikely problems.

Table 5–1 lists the key questions in order and indicates the path you should take. For example, if your answer to key question 1 is No, go to Figure 5–1, Problem with Untried Network (TCP/IP Flowchart 1). If your answer is Yes, then go to key question 2.

Table 5–1 Key Questions for TCP/IP

	Key Question	If...	Go to ...
1.	Has the network ever carried traffic?	No	Figure 5–1, Problem with Untried Network (TCP/IP Flowchart 1)
		Yes	Key Question 2
2.	Has hardware been added or changed?	Yes	Figure 5–2, When Hardware Has Been Changed (TCP/IP Flowchart 2)
		No	Key Question 3
3.	Has software been modified?	No	Figure 5–3, When Software Is Unmodified (TCP/IP Flowchart 3)
		Yes	Key Question 4
4.	Is there an error message? If not, is there a transport problem?	Yes	Figure 5–4, Transport Problem (TCP/IP Flowchart 4)
		No	Key Question 5
5.	Is there a problem with the file server?	Yes	Figure 5–5, File Server Problem (TCP/IP Flowchart 5)
		No	Key Question 6
6.	Is there a problem with remote printing?	Yes	Figure 5–6, Remote Printing Problem (TCP/IP Flowchart 6)

Figure 5–1 Problem with Untried Network (TCP/IP Flowchart 1)


Start
Network Problem ?
No
Done
Yes
Has Network Ever Carried Traffic ?
No
Do Server Master Procedure
Yes
Do Client Master Procedure
Do Client to Server Loop Test
Was Loop Test Successful ?
No
Do Network Connection Procedure
Yes
Note: Network Has Now Carried Traffic
1
Go to Start

TA-0601-AC

Figure 5–2 When Hardware Has Been Changed (TCP/IP Flowchart 2)

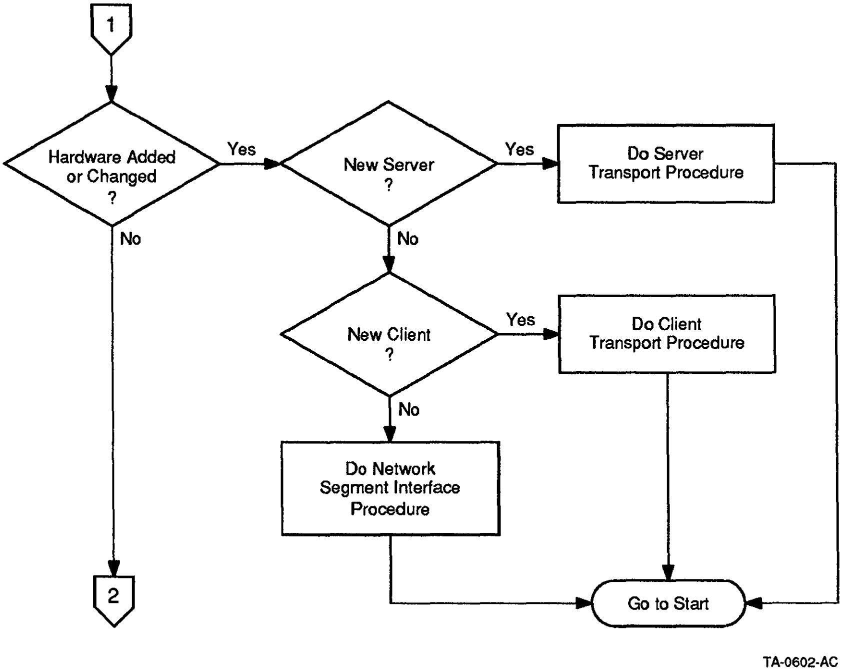
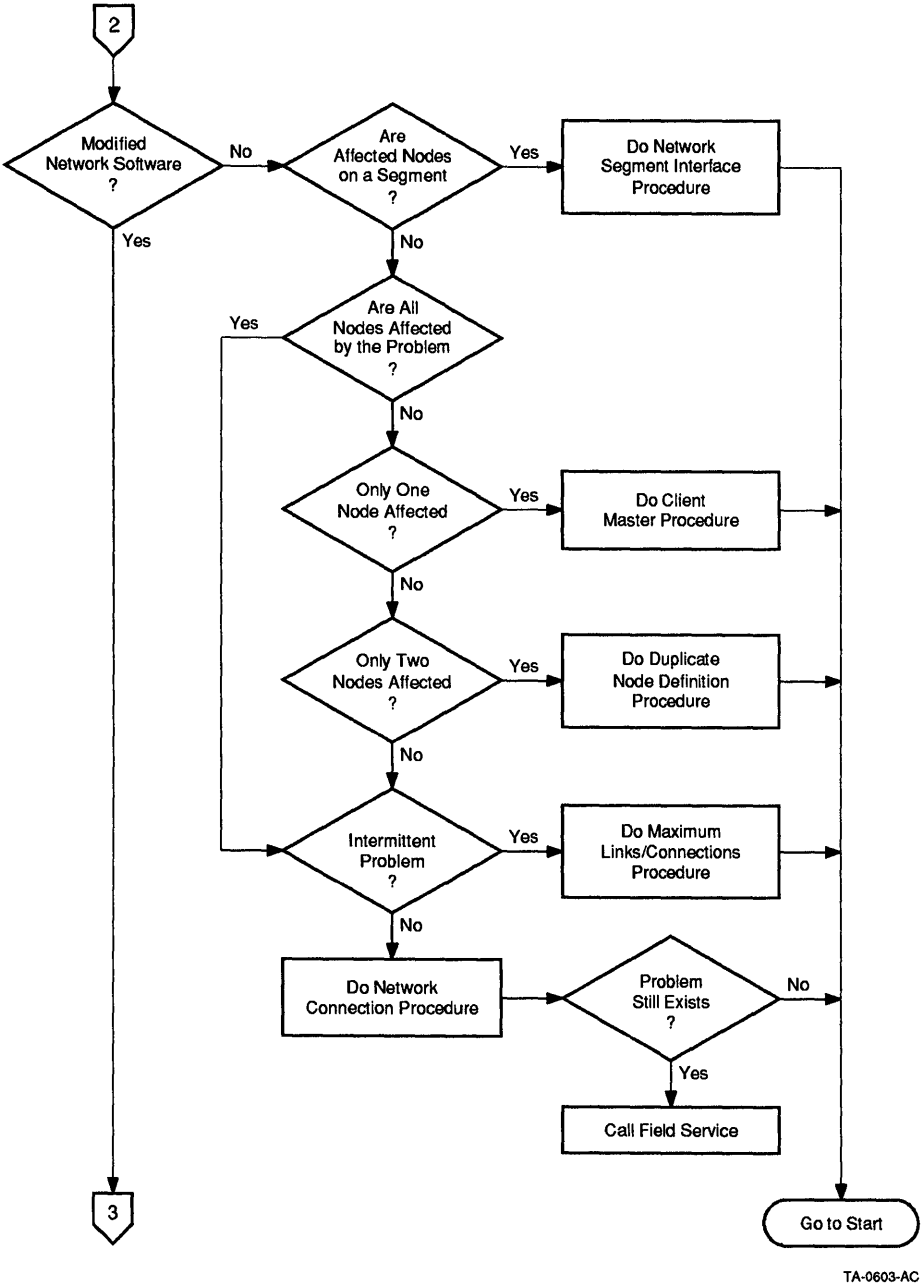

1
Hardware Added or Changed ?
Yes
No
New Server ?
Yes
No
Do Server Transport Procedure
New Client ?
Yes
No
Do Client Transport Procedure
Do Network Segment Interface Procedure
2
Go to Start
TA-0602-AC

Figure 5–3 When Software Is Unmodified (TCP/IP Flowchart 3)



2
Modified Network Software ?
No
Yes
Are Affected Nodes on a Segment ?
Yes
Do Network Segment Interface Procedure
No
Are All Nodes Affected by the Problem ?
Yes
No
Only One Node Affected ?
Yes
Do Client Master Procedure
No
Only Two Nodes Affected ?
Yes
Do Duplicate Node Definition Procedure
No
Intermittent Problem ?
Yes
Do Maximum Links/Connections Procedure
No
Do Network Connection Procedure
Problem Still Exists ?
No
Yes
Call Field Service
3
Go to Start
TA-0603-AC

Figure 5–4 Transport Problem (TCP/IP Flowchart 4)

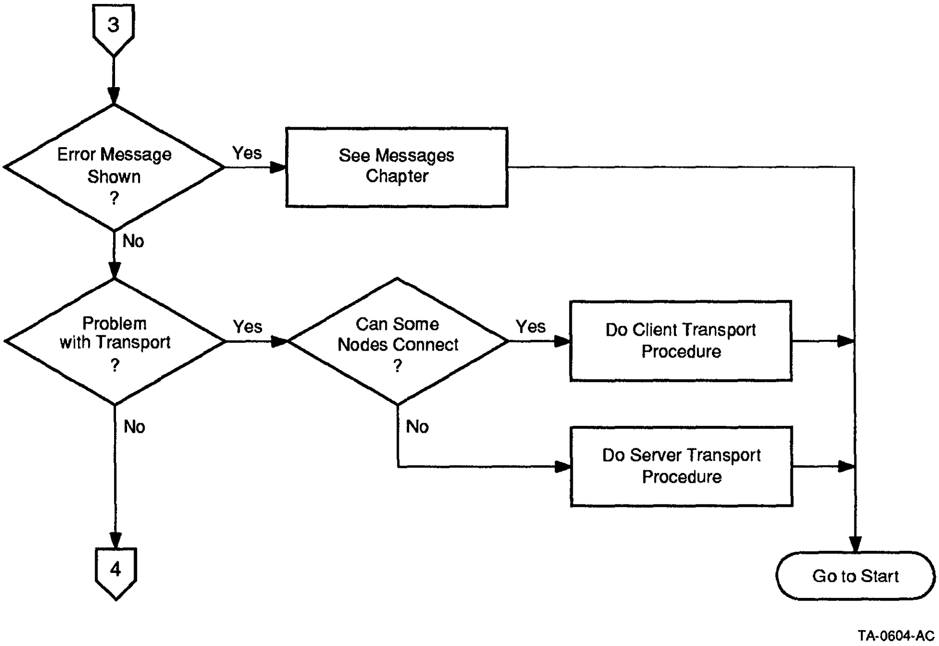


Figure 5–5 File Server Problem (TCP/IP Flowchart 5)

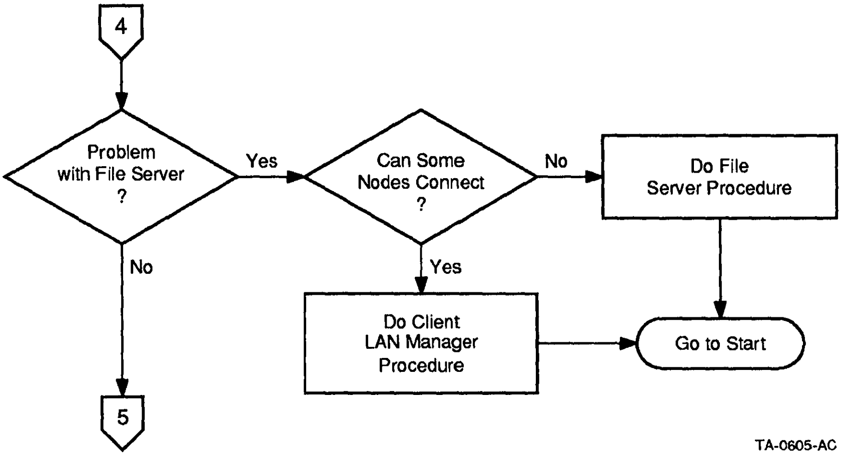
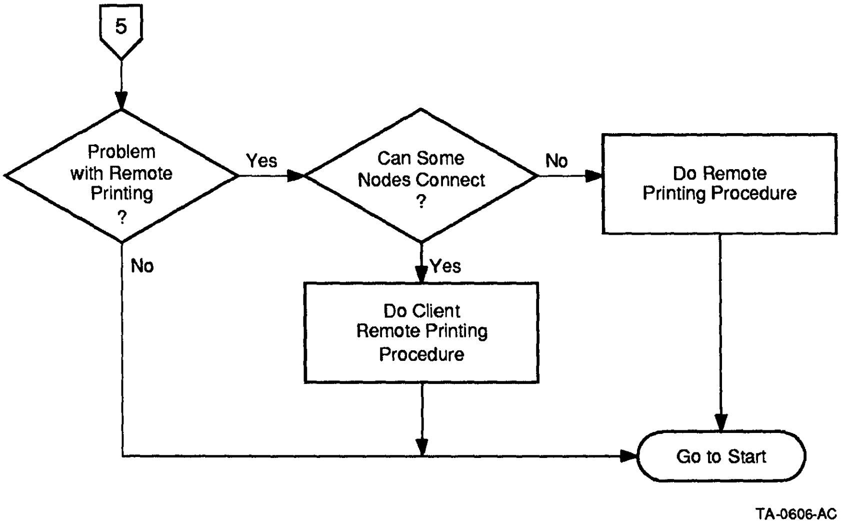


Figure 5–6 Remote Printing Problem (TCP/IP Flowchart 6)


5
Problem with Remote Printing ?
Yes
Can Some Nodes Connect ?
No
Do Remote Printing Procedure
No
Yes
Do Client Remote Printing Procedure
Go to Start
TA-0606-AC

VMS Server Master Procedure (TCP/IP)

This section contains a set of procedures that together make up the VMS Server Master Procedure. Use these procedures in conjunction with TCP/IP Problem-Isolation Flowcharts to isolate and fix network problems.

The VMS Server Master Procedure is composed of the following:

- VMS Server Transport Procedure (TCP/IP)
- VMS File Server Procedure (TCP/IP)
- VMS Remote Printing Procedure (TCP/IP)

VMS Server Transport Procedure (TCP/IP)

This procedure lists the requirements for the TCP/IP transport and verifies that both DECnet and UCX transports are running correctly.

The TCP/IP transport requires the following:

- UCX (VMS/ULTRIX Connection Product) software
- UCX PAK (Product Authorization Key)
- DECnet software (included with VMS license)

Note

Systems running the TCP/IP transport must have DECnet running locally (on the same node) for the PCSA Manager to provide file services and print service information. However, no PAK is required to run local DECnet because the right to use DECnet locally is included with your VMS license.

DECnet Transport Verification (TCP/IP)

This procedure verifies that DECnet is operating correctly on a VMS server. Refer to the VMS Server Transport Procedure in the DECnet part of this guide to verify correct operation of DECnet.

UCX Transport Verification

This procedure verifies that UCX is operating correctly on a VMS server.

1. Ensure that UCX is installed and running by entering the following command:

   ```
   $ SHOW LOGICAL UCX$INET_HOST
   ```

   If the response is an error message, UCX is not installed or running. Restart UCX with your network startup command file by entering:

   ```
   $ @UCX$STARTUP
   ```

2. Ensure that the host is operating correctly by pinging the host from itself with the following command:

   ```
   UCX> loop local_hostname
   ```

   The response shows whether the local host is alive or not.

3. Enter a SHOW HOST command to display a listing of known remote hosts that can be pinged.

4. Attempt to ping a known remote host with the following command:

   ```
   UCX> loop remote_hostname
   ```

5. Attempt to ping the server node from a client node with the following command:

   ```
   C:\> ping host_name
   ```

VMS Server Transport Procedure Completion (TCP/IP)

This completes the VMS Server Transport procedure. Successfully completing this procedure indicates that DECnet and UCX are set up and running correctly on the VMS server.

VMS File Server Procedure (TCP/IP)

This procedure verifies that the file server is operating correctly on a VMS server. Before using this procedure, verify that DECnet and UCX are running on the server. Otherwise, the file server will not operate correctly.

1. Display general UCX information with the following commands:

   ```
   UCX>  SHOW COMMUNICATION

   UCX>  SHOW INTERFACE
   ```

2. Ensure that the VMS file server is running and accepting connections by entering:

   ```
   $  ADMINISTER /PCSA
   PCSA_MANAGER>  SHOW FILE_SERVER STATUS


   File Server status:


   Server is accepting connection requests.
   Server will refuse unregistered users.


   File Server logging status:


   Logfile : PCFS$LOG_FILES:PCFS_SERVER.LOG
   Logging events : CONNECTIONS, ERRORS, FATAL, LOCKS, OPENS, OPERATOR,
                    PROTOCOL, READS, SECURITY, SESSIONS, SMBS
   ```

   If the PCSA Manager response indicates that the file server is either accepting or not accepting connections, then the server is running.

   If the file server is not running, an error message similar to the following is displayed:

   ```
   %PCSA-E-NOFSVRLINK, unable to establish link to File Server
   %PCSA-E-FILESRVNOTRUN, File Server not running
   ```

   Start the file server with the appropriate command as follows:

   - For TCP/IP only:

     ```
     $  @SYS$STARTUP:PCFS_STARTUP TCP
     ```

   - For TCP/IP and DECnet:

     ```
     $  @SYS$STARTUP:PCFS_STARTUP DECNET/TCP
     ```

   If the server is running, but not accepting connections, allow only registered connections by using the following PCSA Manager command:

   ```
   $  ADMINISTER /PCSA
   PCSA_MANAGER>  START FILE_SERVER CONNECTIONS /REGISTERED
   ```

3. Enter a SHOW SYSTEM command to verify that the following processes exist:

   - NBNS (TCP netbios process)
   - NETBIOS process
   - PCFS_SERVER process

4. Verify that the name server exists and is operating by entering the following command:

   ```
   UCX  SHOW DEVICE/PORT=137
   ```

5. Verify that the file server exists and is running with UCX operational by entering the following command:

   ```
   UCX  SHOW DEVICE/PORT=139
   ```

6. Verify that the service you want exists by entering the following:

   ```
   $ ADMINISTER /PCSA
   PCSA_MANAGER> SHOW FILE_SERVER SERVICES /AUTHORIZED


   File Server Authorized Services:


   User name     Alias name    Service name  Access  RMS protection
   ------------  ------------  ------------  ------  --------------------
   <PUBLIC>      LN03_DPORT    LN03_DPORT    RWC     S:AWED,O:AWED,G:,W:
   <PUBLIC>      PCAPPS        PCAPPS        R       S:AWED,O:AWED,G:,W:
   SYSTEM        PCAPPS        PCAPPS        RWC     S:AWED,O:AWED,G:,W:
   USER1         WRITERS       WRITERS       RWC     S:AWED,O:AWED,G:,W:
   ```

   - If the service you are trying to connect to is not listed, use PCSA Manager to register the service.

     It is not necessary to register the default directory or subdirectories of an authorized VMS user's account. It is only necessary that the VMS directory exist and that the VMS account name and password provide access to the directory at the desired RMS protection level.

   - On a client node, use the following command to connect to the default login directory:

     ```
     A:\> USE ?:\\internet_hostname\account password
     ```

     internet hostname — Is the VMS server running UCX (indicated by showing logical UCX$INET_HOST).

     account — Is a valid account name as defined in the VMS UAF.

password — Is a valid password for the user name.

Note

You cannot enumerate services if the client is only running TCP\IP. This should not be considered a server failure.

7. If the service is not a PUBLIC service, ensure that the user is authorized to use the service:

```
$ ADMINISTER /PCSA
PCSA_MANAGER> SHOW FILE_SERVER SERVICES-
_PCSA_MANAGER> /AUTHORIZED /USERNAME=USER1


File Server Authorized Services:


User name     Alias name    Service name  Access  RMS protection
------------  ------------  ------------  ------  --------------------
USER1         WRITERS       WRITERS       RWC     S:AWED,O:AWED,G:,W:
```

   If the user is not authorized to connect to the desired service, use the GRANT command to authorize the connection:

```
PCSA_MANAGER> GRANT USER1 WRITERS WRITERS-
_PCSA_MANAGER>   /ACCESS=(READ,WRITE,CREATE)
%PCSA-I-SERGRANTED, service "WRITERS" granted to user/group "USER1"


PCSA_MANAGER>
```

8. Ensure that the VMS file server is within its limit for the number of sessions or connections. Determine the server limits by entering:

```
PCSA_MANAGER> SHOW FILE_SERVER CHARACTERISTICS


File Server characteristics:
Total server wide sessions      : 32
Total server wide connections   : NO LIMIT
Total connections per session   : NO LIMIT
Total server wide open files    : NO LIMIT
Total open files per session    : NO LIMIT
File server buffer size in Kbyte :       8
Open file buffer cache enabled   :    TRUE
File read on seek enabled        :    TRUE
Server default account       : PCFS$ACCOUNT
```

   Determine the number of current sessions or connections established with the server by entering the following commands:

```
PCSA_MANAGER> SHOW FILE_SERVER SESSIONS
PCSA_MANAGER> SHOW FILE_SERVER CONNECTIONS
```

The server limit is reached if the number of sessions or connections displayed is equal to the number of session or connection limits, as displayed by the PCSA Manager SHOW FILE_SERVER CHARACTERISTICS command.

If the server session or connection limit has been reached, new sessions or connections cannot be established until enough of the existing sessions or connections are closed to reduce the number(s) to less than the limit(s).

9. Ensure that the value of "Total server wide sessions" is at least two less than the DECnet executor parameter "maximum links."

VMS File Server Procedure Completion (TCP/IP)

The VMS file server procedure is complete. Successfully completing this procedure indicates that the file server is set up correctly on the VMS server.

VMS Remote Printing Procedure (TCP/IP)

This procedure verifies that remote printing is operating correctly on a VMS server. For remote printing to operate properly, the file server must be operating properly.

1. To ensure that the printer is ready to print, verify that:
   - The printer is connected to a power source.
   - The printer is connected to the VAX computer.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is online.
2. Log in to the system manager's account on the server node.
3. Ensure that the printer queue is defined and running by entering:

   ```
   $ SHOW QUEUE queuename
   ```

   The response should indicate that the queue is a generic printer queue.

   If the response from the command is "no such queue," the print queue should be set up. Use PCSA Manager to set up the printer queue.

   If the response indicates that the queue is stopped, the queue should be started with the START/QUEUE command.

   ```
   $ START/QUEUE queuename
   ```
4. Ensure that you can print with the VMS PRINT command, specifying a queue that the VMS server uses. For example, to print a file and specify the queue LN03_DPORT, enter:

   ```
   $ PRINT/QUEUE=LN03_DPORT filename.ext
   ```

5. **Ensure that the VMS file server is running and accepting connections by entering:**

```
$ ADMINISTER /PCSA
PCSA_MANAGER> SHOW FILE_SERVER STATUS


File Server status:


Server is accepting connection requests.
Server will refuse unregistered users.


File Server logging status:


Logfile : PCFS$LOG_FILES:PCFS_SERVER.LOG
Logging events : CONNECTIONS, ERRORS, FATAL, LOCKS, OPENS, OPERATOR,
                 PROTOCOL, READS, SECURITY, SESSIONS, SMBS
```

   If the PCSA Manager response indicates that the file server is accepting (or not accepting) connections, the server is running.

   If the response contains the following error message, the file server is not running.

```
PCSA_MANAGER> SHOW FILE_SERVER STATUS
%PCSA-E-NOSVRLINK, unable to establish link to File Server
%PCSA-E-FILESRVNOTRUN, File Server is not running
```

   For help on starting the file server and ensuring that it is operating properly, refer to the VMS File Server Procedure in this chapter.

   If the server is not accepting connections, allow only registered connections by using the following PCSA Manager command:

```
$ SET DEFAULT SYS$SYSTEM
$ ADMINISTER /PCSA
PCSA_MANAGER> START FILE_SERVER CONNECTIONS /REGISTERED
```

6. **Ensure that the service you are attempting to connect to exists and that the alias is correct by entering:**

```
$ SET DEFAULT SYS$SYSTEM
$ ADMINISTER /PCSA
PCSA_MANAGER> SHOW FILE_SERVER SERVICES /AUTHORIZED /ALIAS=account


File Server Authorized Services:


User name     Alias name    Service name Access RMS protection
------------  ------------  ------------ ------ --------------------
<PUBLIC>      LN03_DPORT    LN03_DPORT   RWC    S:AWED,O:AWED,G:,W:
```

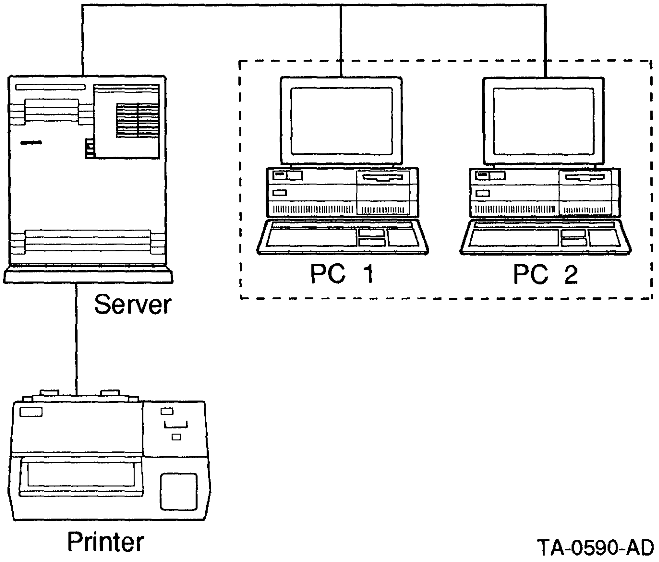
VMS Remote Printing Procedure Completion (TCP/IP)

The VMS Remote Printing Procedure is complete. Successfully completing this procedure indicates that the printer services are set up correctly on the VMS server.

VMS Server Master Procedure Completion (TCP/IP)

The VMS Server Master Procedure is complete. If successful, you know that the VMS TCP/IP transport (UCX), file server, and remote printing on your network are set up correctly as shown in Figure 5–7.

Figure 5–7 Correct Setup for VMS Server



ULTRIX Server Master Procedure (TCP/IP)

This section contains a set of procedures that together make up the ULTRIX Server Master Procedure. Use these procedures in conjunction with TCP/IP Problem-Isolation Flowcharts to isolate and fix network problems.

The ULTRIX Server Master Procedure is composed of the following:

- ULTRIX Server Transport Procedure (TCP/IP)
- ULTRIX File Server Procedure (TCP/IP)
- ULTRIX Remote Printing Procedure (TCP/IP)

ULTRIX Server Transport Procedure (TCP/IP)

This procedure verifies that the TCP/IP transport software is running correctly on an ULTRIX server.

1. Ensure that TCP/IP is installed and running by entering the following command:

   ```
   # ifconfig device_name
   ```

   If the response is an error message, TCP/IP is not installed or running.

   Examine the file /etc/rc.local and verify that the ifconfig line is set correctly. If it is not, then you must run the **netsetup** program by entering the command:

   ```
   # netsetup install
   ```

2. Ensure that the host is operating correctly by pinging the host from itself with the following command:

   ```
   # ping local_host
   ```

   The response shows whether the local host is alive or not.

3. Enter the following command to display a listing of known remote hosts that can be pinged:

   ```
   # cat /etc/hosts
   ```

4. Attempt to ping a known remote host with the following command:

   ```
   # ping remote_hostname
   ```

5. Attempt to ping the server node from a client node with the following command:

   ```
   C:\> ping host_name
   ```

ULTRIX Server Transport Procedure Completion (TCP/IP)

This completes the ULTRIX Server Transport Procedure. Successfully completing this procedure indicates that TCP/IP is set up and running correctly on an ULTRIX server.

ULTRIX File Server Procedure (TCP/IP)

This procedure verifies that the file server is operating correctly on an ULTRIX server. Before using this procedure, verify that TCP/IP is running on the server. Otherwise, the file server will not operate correctly.

1. Display general TCP/IP information with the following commands:

   ```
   # ifconfig device_name
   ```

2. Ensure that the ULTRIX file server is running and accepting connections by entering the following:

   ```
   # pcsamgr
   ```

   Select the CONFIG menu item, then select the Start Server submenu item. The correct response is the message ERROR: File Server is Active, indicating the file server is running. If the file server is not active, this selection starts the server.

   Alternately, you can enter the following command line:

   ```
   # ps -aux|grep pcsa
   ```

   The correct response shows that **pcsanbud** and **pcsaadmd** are running. If they are not running, enter the **pcsamgr** command and use the CONFIG and Start Server menu to start them.

3. Enter a SHOW SYSTEM command to verify that the following processes exist:

   - pcsanbud
   - pcsaadmd

4. Ensure the service you are attempting to connect to exists by entering the following:

   ```
   # pcsamgr
   ```

   Select the VIEW menu item and the File Services submenu item. If the service you are trying to connect to is not listed, use **pcsamgr** to register the service.

   It is not necessary to register the default directory or subdirectories of an authorized ULTRIX user's account. It is only necessary that the ULTRIX directory exists and that the account name and password provide access to the directory at the desired protection level.

   On a client node, use the following command to connect to the default login directory:

   ```
   A:\> USE ?: \\internet_hostname\account password
   ```

In the command:

internet hostname	Is the ULTRIX server running TCP/IP
account	Is a valid account name as defined in the ULTRIX /etc/passwd file.
password	Is a valid password for the user name.

Note

You cannot enumerate services if the client is only running TCP. This should not be considered a server failure.

5. If the service is not a PUBLIC service, ensure that the user has access to the directory.
   - Enter the following command:

     ```
     # ls -lgd service_directory
     ```

   - Examine the directory protection

     If the user does not have access via the ULTRIX protection mask, the user cannot connect to the service. Add the user to the group the service is in and verify that the group has, at minimum, the "r" and "x" set.
6. Ensure that the ULTRIX file server has not reached its limit for the number of sessions or connections.

   Enter the following command:

   ```
   # pcsamgr
   ```

   Choose the CONFIG menu item and the Server Setup submenu item. Verify that the Max Sessions and Max Connections values are correct.

   List the current sessions or connections established with the server by viewing the File Services and Zooming on each File Service.

   The server limit is reached if the number of sessions or connections displayed are equal to the number of session or connection limits, as displayed by the PCSA Manager SHOW FILE_SERVER CHARACTERISTICS command.

   If the server session or connection limit has been reached, new sessions or connections cannot be established until enough of the existing sessions or connections are closed to reduce the number(s) to less than the limit(s). Or, you can increase the limits and restart the server.

ULTRIX File Server Procedure Completion (TCP/IP)

The ULTRIX file server procedure is complete. Successfully completing this procedure indicates that the file server is set up correctly on the ULTRIX server.

ULTRIX Remote Printing Procedure (TCP/IP)

This procedure verifies that remote printing is operating correctly on an ULTRIX server. For remote printing to operate properly, the file server must be operating properly.

1. To ensure that the printer is ready to print, verify that:
   - The printer is connected to a power source.
   - The printer is connected to the VAX/RISC computer.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is online.
2. Log in to the system manager account on the server node.
3. Ensure that the printer queue is defined and running by entering:

   ```
   # lpstat -z(queue_name)
   ```

   The response should indicate that queuing is enabled.

   If the response from the command is unknown printer, the print queue must be set up. Use **pcsamgr** to set up the print queue.

   If the response indicates that queuing is disabled, the queue should be started with the following command:

   ```
   # lpc enable queue_name
   ```
4. Verify that you can print with the ULTRIX **lpr** command, specifying a queue that the ULTRIX server uses. For example, to print a file and specify a queue, enter the following command:

   ```
   # lpr -p queue_name filename
   ```
5. Ensure that the ULTRIX file server is running and accepting connections by entering the following:

   ```
   # pcsamgr
   ```

   Select the CONFIG menu item, then select the Start Server submenu item. The correct response is the message ERROR: File Server is Active, indicating the file server is running. If the file server is not active, this selection starts the server.

   Alternately, you can enter the following command line:

   ```
   # ps -aux|grep pcsa
   ```

The correct response shows that **pcsanbud** and **pcsaadmd** are running. If they are not running, enter the **pcsamgr** command and use the CONFIG and Start Server menu items to start them.

For help to start the file server and to ensure that it is operating properly, refer to the ULTRIX File Server Procedure in this chapter.

If the server is not accepting connections, allow only registered connections by using the **pcsamgr** command and use the CONFIG and Start Server menu.

Choose the View menu to examine the Printer submenu Services and Queues items to verify correct operation.

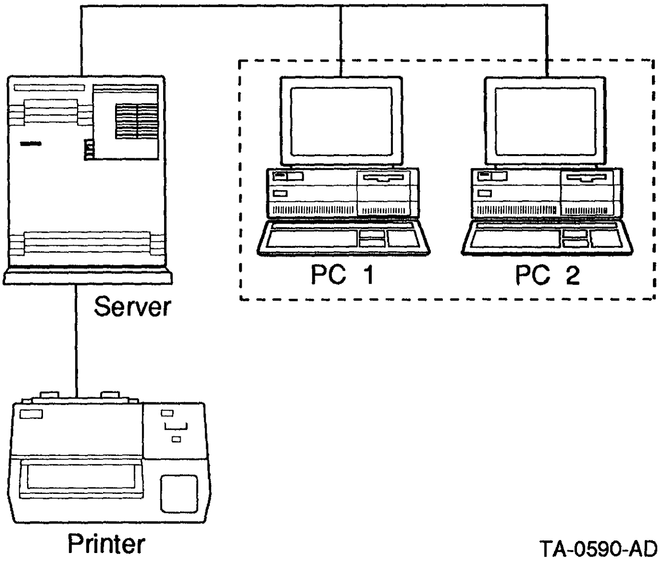
ULTRIX Remote Printing Procedure Completion (TCP/IP)

The ULTRIX Remote Printing Procedure is complete. Successfully completing this procedure indicates that the printer services are set up correctly on the ULTRIX server.

ULTRIX Server Master Procedure Completion (TCP/IP)

The ULTRIX Server Master Procedure is complete. If successful, you know that the ULTRIX server on your network is set up correctly, as shown in Figure 5–8.

Figure 5–8 Correct Setup of ULTRIX Server



DOS Client Master Procedure (TCP/IP)

This section contains a set of subsidiary procedures, which together make up the DOS Client Master Procedure. Use these procedures in conjunction with TCP/IP Problem-Isolation Flowcharts. The DOS Client Master Procedure is composed of the following:

- DOS Client Transport Procedure (TCP/IP)
- DOS Client LAN Manager Procedure (TCP/IP)
- DOS Client Remote Printing Procedure (TCP/IP)

Use these procedures to verify that your DOS client is operating correctly. First, verify that TCP/IP is installed and running correctly. You can then use the LAN manager procedure to verify that the LAN manager is operating correctly on the DOS client. You can then use the DOS Client Remote Printing Procedure to verify that your printing service is set up and working correctly. If you are having problems with the DOS client, you may have to perform one or more of the following tests:

- Client-to-server ping test
- Client-to-client ping test
- Daisy-chain segment test
- DEMPR configuration segment test

To perform these tests, boot the client with the key diskette. Then insert the PATHWORKS Version 4.0 diskette and perform the indicated test.

DOS Client Transport Procedure (TCP/IP)

This procedure verifies that TCP/IP is operating correctly on a DOS client.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Verify that TCP/IP is operational by pinging another known working node by entering the following command:

   ```
   C:\>  ping node_name
   ```

   If the response is an error message, continue with the following steps:

2. Verify the software configuration on the DOS client.

   The following is required to run Network Maintenance Facilities (NMF). The device drivers listed in Table 5–2 must be in your CONFIG.SYS file. The Terminate-and-Stay-Resident (TSR) programs listed in Table 5–3 must be loaded at the DOS command line or from a batch file before you use NMF.

Table 5–2 DOS-Based NMF Device Drivers

Program Component	Module Name	Type of Component
Protocol Manager	PROTMAN.DOS	driver
NDIS MAC	<mac>.DOS	driver
EMS Memory Management	NEMM.DOS	driver
TCP Resident Driver	TCPDRV.DOS	driver

Table 5–3 DOS-Based NMF TSR Programs

Program Component	Module Name	Type of Component
TCP/IP Protocol	TCPTSR.EXE	TSR
Domain Name Resolver (optional)	DNRTSR.EXE	TSR
Netman	NMTSR.EXE	TSR
NMF	ARP.EXE, NETSTAT.EXE, PING.EXE	applications

Note

If you change the CONFIG.SYS file on your computer, you must restart the computer for the changed file to be loaded.

Note

To use domain name services instead of a host IP address with FTP, NMF, or terminal emulation, you must first load the TSR program named DNRTSR.EXE at the DOS command line or from a batch file.

3. Verify the DOS client connection to the network.
   - Use the **netstat** command to look for outgoing errors.
   - If the netstat display shows outgoing errors, check the client's cabling to the network.
   - If the client's cabling is intact, check the client for possible hardware or controller errors.
4. Ensure the node address is correctly defined at the client. At the client, enter the following command to display static configuration information:

   ```
   C:\> netstat -c
   ```

   Verify that the client node address matches the client address known to the server. If the node address is not the same at the client and at the server, reregister the client with the server or redefine the client address.
5. Verify that the client memory configuration is correct.

   ### EMS Memory

   Use the following verification procedure if you are using EMS memory:

   a. Display the CONFIG.SYS file with a text editor.

   b. Check to be sure the following line is in the file:

   ```
   device = <ems.driver>
   ```

   <ems.driver> is the EMS driver name, as supplied by the EMS adapter manufacturer. If it is not present, your client EMS is not configured correctly. Reconfigure it according to the manufacturer's instructions.

Note

The EMS driver must be installed before all other drivers that use EMS. The EMS, such as Intel Above Board Plus or equivalent, must meet the LIM Expanded Memory Specification.

c. Check the CONFIG.SYS file for the following two lines:

```
device = nemm.dos
device = tcpdrv.dos
```

These two lines are for the TCP driver, and must be placed somewhere in CONFIG.SYS following the EMS driver entry.

If the lines are present, then the client is configured correctly.

If the lines are not present, you need to reinstall TCP.

The following listing is a sample of a correctly configured CONFIG.SYS file for a client with EMS. The example assumes that EMM.SYS is in the root directory of the C drive.

```
DEVICE = C:\EMM.SYS AT D000 258 ND
DEVICE = C:\3OPEN\DOSWKSTA\LANMAN\DRIVERS\NEMM.DOS
DEVICE = C:\3OPEN\DOSWKSTA\LANMAN\DRIVERS\PROTMAN.DOS /I:C:\3OPEN\
     DOSWKSTA\LANMAN/DRIVERS
DEVICE = C:\3OPEN\DOSWKSTA\LANMAN\DRIVERS\ELINKII.DOS
DEVICE = C:\3OPEN\DOSWKSTA\LANMAN\DRIVERS\TCPDRV.DOS /I:C:\3OPEN\
     DOSWKSTA\LANMAN/DRIVERS
```

DOS Client Transport Procedure Completion (TCP/IP)

The DOS Client Transport Procedure is complete. Successfully completing this procedure indicates that TCP/IP is set up correctly on the DOS client.

DOS Client LAN Manager Procedure (TCP/IP)

This procedure verifies that the basic LAN Manager is operating correctly on the DOS client. To use the basic LAN Manager, TCP/IP must be operating correctly.

Note

> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Ensure that the basic LAN Manager is running by entering:

   ```
   A:\>  USE /STATUS
   ```

   If the LAN Manager is running, the response is similar to the following example. If the LAN Manager is not running, then continue to the next step.

   ```
   USE Version V4.0.19 PCSA Network Connection Manager

   Status  Dev   Type   Connection name                       Mode     Size
   ------  ---   ----   ------------------------------------  -------  -------
           E:    FILE   \\RWS\PCSAV40
           F:    FILE   \\RAINBO\USER1
   ```

2. Check the client memory configuration by entering the following:

   ```
   A:\>  memman
   ```

   The response is similar to the following example:

   ```
   MEMMAN V4.0.13  PCSA Memory Information Utility
   Copyright (C) 1989 by Digital Equipment Corporation

   Memory Usage Summary

       DOS memory allocation scheme    first fit

       Physical conventional memory    640K
       Reported conventional memory    640K
       Available conventional memory   488K

       Physical extended memory       3072K
       Reported extended memory          0K

       Expanded memory size           3680K
       Expanded memory available      2928K

       XMS extended memory available  2928K
       Largest available EMB          2928K
   ```

3. Verify that the TCP/IP network programs are loaded by entering the following:

   ```
   C:\>  tcpunld/status
   ```

The response is similar to the following example:

```
3Com v1.2Network Unload ()
Copyright (c) Hewlett-Packard Co., 1989-1990.  All rights reserved.

              -- Network Load Status --

The following network programs are loaded.   They are listed in
reverse load order, i.e. the first one in the list would be the
first one to unload.

   Network Program Name       Approx. Resident Memory
===========================  =======================
Network Management Services         5952 bytes
BAPI                                16592 bytes
Telnet                              2256 bytes
Sockets                             17824 bytes
Domain Name Services                1920 bytes
EM                                  1168 bytes
RFC NetBIOS                         6080 bytes
TCP/IP                              66304 bytes
```

4. Check network operations and setup by entering the following:

   ```
   C:\> netstat -a
   ```

   Verify that the Internet Address and Subnet Mask values are set correctly. Examine the statistical information to identify any recurring problems.

5. Examine the client file PROTOCOL.INI and verify that the following values are set correctly:

   - IPADDRESS0
   - SUBNETMASK0
   - HOSTNAME
   - NETFILES
   - NAMESERVER0
   - DOMAIN

DOS Client LAN Manager Procedure Completion (TCP/IP)

The DOS Client LAN Manager Procedure is complete. Successfully completing this procedure indicates that the LAN Manager is operating correctly on the DOS client.

DOS Client Remote Printing Procedure (TCP/IP)

This procedure verifies that remote printing is operating correctly on a DOS client. To use remote printing, the basic LAN Manager must be operating correctly.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. To ensure that the printer is ready to print, verify that:
   - The printer is connected to a power source.
   - The printer is connected to the server.
   - The printer has an adequate supply of paper.
   - The paper passes through the printer correctly.
   - The printer is on line.
2. At the system prompt, enter the following commands:

   ```
   A:\> USE print_device \\server_node\print_service%user_name password
   A:\> NET PRINT /D:print_device
   ```

   You can use the DOS COPY command to copy a file to the remote printing service.

   In Microsoft Windows, use the configuration aid to select the redirected print device and printer type.
3. Use the USE command to determine the print devices that are redirected and the remote printing services to which they are redirected.

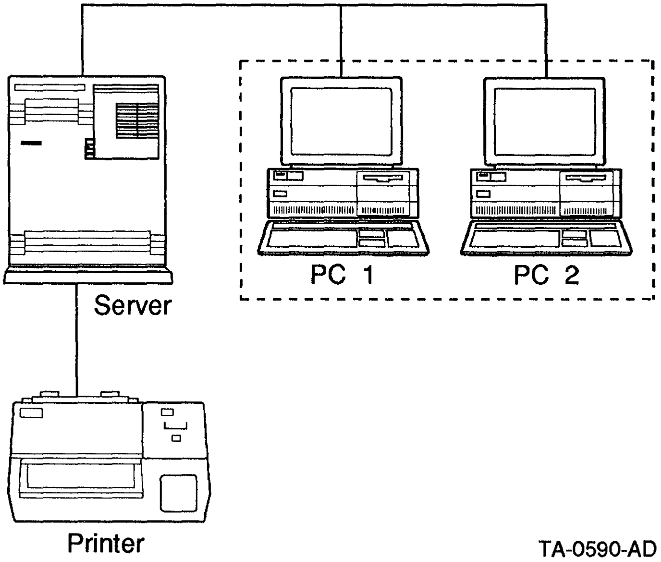
DOS Client Remote Printing Procedure Completion (TCP/IP)

Completing this procedure indicates that remote printing is set up correctly on the DOS client.

DOS Client Master Procedure Completion (TCP/IP)

The DOS Client Master Procedure is complete. If successful, you know that the DOS client on your network, shown in Figure 5–9, is set up correctly.

Figure 5–9 Correct Setup for DOS Client



Troubleshooting Hardware and Configuration (TCP/IP)

This section contains a set of procedures you use for isolating problems with the configuration of your network or with network hardware. Use it in conjunction with TCP/IP Problem-Isolation Flowcharts. The following procedures and tests are included:

- Duplicate Node Definition Procedure (TCP/IP)
- Maximum Links/Connections Procedure (TCP/IP)
- Network Connection Procedure (TCP/IP)
- Network Segment Interface Procedure (TCP/IP)

Duplicate Node Definition Procedure (TCP/IP)

Use this procedure to confirm that two nodes do not have the same node names and/or node addresses.

Ensure that the node names and node addresses are consistent at all nodes on the network.

1. Ensure that the same key diskette was not used to boot two clients. Also, ensure that a copy of a key diskette was not used to boot a client while the original key diskette was used to boot another client. This applies to network key diskettes as well as physical key diskettes.
2. On each node, use the NCP SHOW EXECUTOR command to display the node's name and address. Enter the data you collect in a table. Use this table to verify that node names and addresses are set up as expected.

Duplicate Node Definition Procedure Completion (TCP/IP)

The Duplicate Node Definition procedure is complete.

Maximum Links/Connections Procedure (TCP/IP)

This procedure verifies that the number of allowed links, connections, or sessions has not been exceeded.

1. Use the command SHOW EXECUTOR CHARACTERISTICS to determine the maximum number of links.
2. Use the PCSA Manager command SHOW FILE_SERVER CHARACTERISTICS to determine the maximum limit for total server-wide sessions.

   The number of links that the server must support is three times the number of PC clients on the network, plus the number of nodes in the cluster, plus the number of additional links required by individual applications. Ensure that the maximum limit for total server-wide sessions is larger than this number.
3. Ensure that the number of file server total server-wide sessions is at least two less than the maximum number of links.

Maximum Links/Connections Procedure Completion (TCP/IP)

The Maximum Links/Connections Procedure is complete.

Network Connection Procedure (TCP/IP)

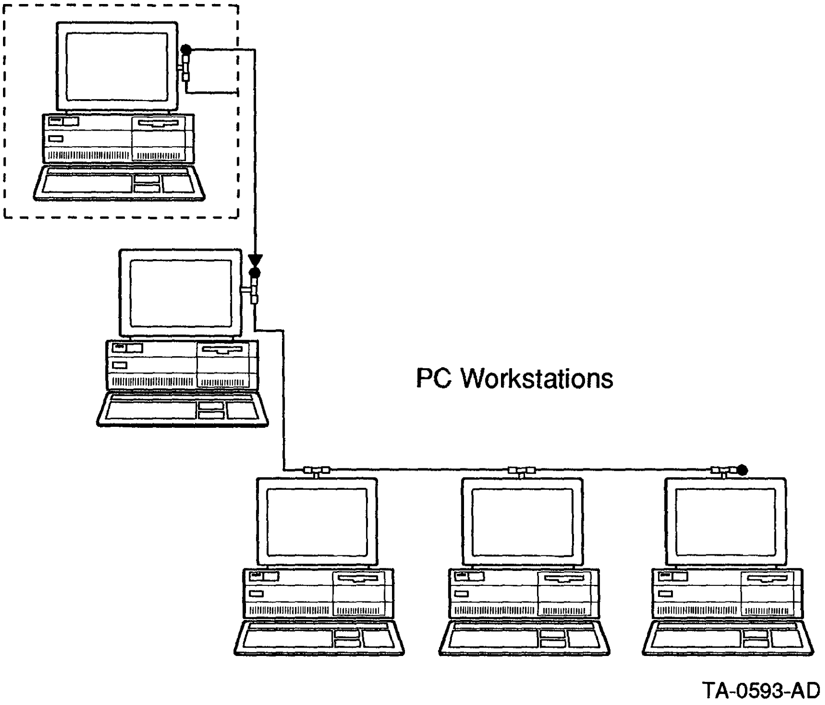
To troubleshoot a problem on the cable, follow the instructions for either Daisy Chain Segment Test (TCP/IP) or DEMPR Configuration Segment Test (TCP/IP). Before doing either test, make sure that the server is cabled to the network correctly.

Daisy Chain Segment Test (TCP/IP)

Starting at the end of a segment:

1. Remove the terminator from the end of the chain.
2. Insert the terminator at the next T-connector, as shown in Figure 5–10.
3. Run the Client Loopback Test on the last node in the chain.
4. Run the appropriate server troubleshooting test from the server node to the last node.
   - If successful, the segment removed was bad. Replace that segment and retest. (A bad T-connector or terminator can cause a problem.)
   - If failure still occurs, return to step 1 above. Repeat these steps until you find the bad segment or network component.

Figure 5–10 Checking Daisy Chain Configuration Segments



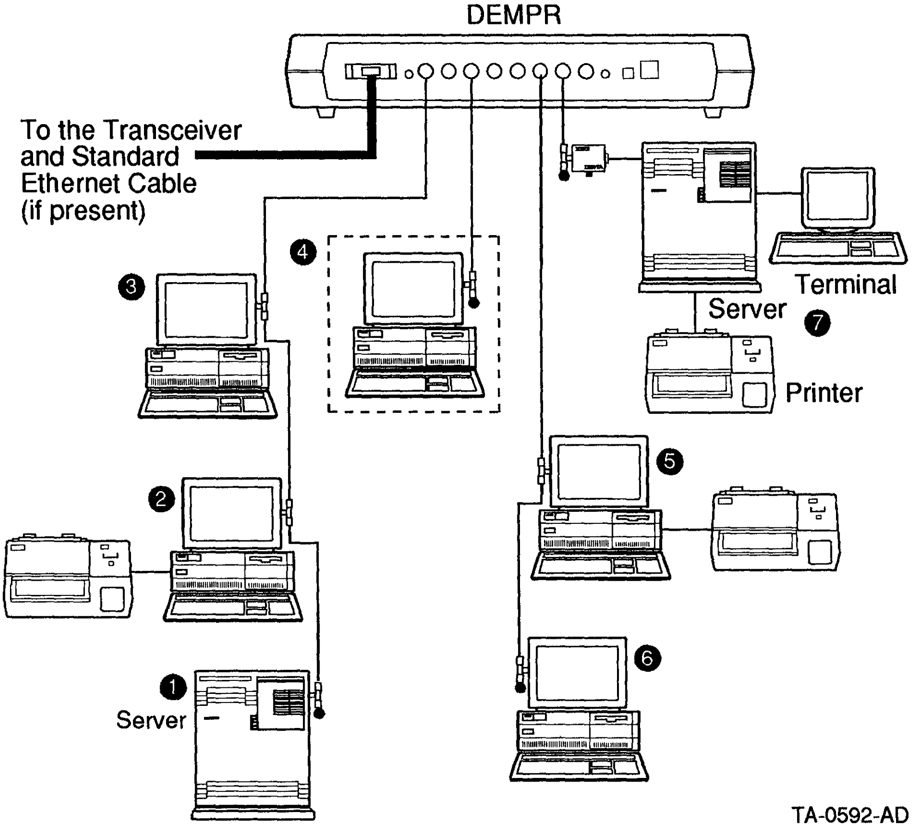
Daisy Chain Segment Test Completion (TCP/IP)

The Daisy Chain Segment Test is complete.

DEMPR Configuration Segment Test (TCP/IP)

Refer to Figure 5–11 to perform the DEMPR configuration segment test.

Figure 5–11 Checking DEMPR Configuration Segments



From the point of failure (node 4) to node 1:

1. Reset the DEMPR if any lights are on or blinking.
2. Follow the daisy chain segment test for nodes 1, 2, and 3.
3. Use the following DEMPR segment test:
   - Remove the connection from the DEMPR port for the failing segment (in this example, node 4).
   - Connect the failing segment to another DEMPR port.
   - Run the Client Loopback Test (DECnet) on this node (node 4).

- Reset the DEMPR to make sure that the segment is not disconnected. If the light remains on or blinking after the reset, the segment is not properly connected.
- Run the appropriate server troubleshooting test from node 1 to node 4, which is now connected to a new port.
  - If successful, reconnect the segment to the original port and retest. If this is successful, resetting the cable connections and the DEMPR may have fixed the problem. If this fails, the original port is faulty. Replace the bad component.
  - If the new port fails, replace the cable between the client and the DEMPR and retest. If successful, the original cable was faulty. If the test fails, the DEMPR has a hardware failure. You can test other DEMPR ports or contact your authorized service representative.

DEMPR Configuration Segment Test Completion (TCP/IP)

The DEMPR Configuration Segment Test is complete.

Network Segment Interface Procedure (TCP/IP)

This procedure verifies that the nodes on a network segment can communicate on the network segment and that the network segment interface is suspect.

If two or more nodes are daisy chained on a network segment, disconnect the end of the ThinWire cable nearest the network segment interface and install a terminator. Using the appropriate loop test (server to server, client to client, or client to server), do a loop test between the two nodes at either end of the segment.

If the loop test is successful, the network segment interface, H4000, DEMPR, or DEREP, is probably faulty. If you have a similar component somewhere else in the network, try temporarily substituting the similar component for the suspect unit.

If the loop test fails, check the terminators at both ends of the network segment. If no problem is observed, disconnect one of the tested nodes and move the terminator to the new end of the segment. Repeat the loop test between the two nodes at either end of the segment. Repeat this process until the loop test is successful or until only two nodes remain.

If after removing a node, the loop test is successful, the removed node is probably faulty.

If the loop test has failed and you are down to two nodes, try connecting and testing, in turn, each of the two remaining nodes with a third node. If one loop test completes successfully, the remaining node is probably faulty.

Network Segment Interface Procedure Completion (TCP/IP)

The Network Segment Interface Procedure is complete.

6 TCP/IP Messages

This chapter lists common TCP/IP network messages with possible problems and solutions.

Following each message is an explanation of why the message occurs and a troubleshooting procedure or action that gives instructions for solving the problem, and general recommendations, if any.

The procedures do not present a complete methodology for solving the problems. Instead, they provide the most likely solutions for the problems—the solutions to try first.

Organization

The messages listed in this chapter are grouped into server-based and client-based sections. The server messages are listed alphabetically, while the client messages are listed by number.

Troubleshooting Notes

Keep the following in mind as you begin troubleshooting:

For VMS Systems

- Using privileged accounts

  Many of the procedures in this chapter require the use of an account with system management level privileges. Many procedures also assume that you have access to accounts with these privileges on all nodes in your network. For procedures requiring use of a privileged account on a node to which you do not have access, ask the system manager of that node to perform the action.

Troubleshooting Notes

- Modifying passwords

  Some procedures call for correcting mismatches between passwords specified in the SYSUAF file. Before you make any changes, be sure that you have the authority to make the modifications. If you do not have the authority to do so, refer the required change to the appropriate system or network manager.

For ULTRIX Systems

- Modifying passwords

  Some procedures call for correcting mismatches between passwords specified in the /etc/passwd file. Before you make any changes, be sure that you have the authority to make the modifications. If you do not have the authority to do so, refer the required change to the appropriate system or network manager.

Server-Based Messages

This section lists server-based messages in alphabetical order. Each message is followed by an explanation of its probable cause(s) and a recommended recovery procedure.

Connection Timed Out

Symptoms

TCP/IP network users receive the following error when attempting any TCP/IP-based network operation:

```
connection timed out
```

Explanation

This message occurs when the TCP software attempts to make a connection to the destination host, and does not receive any packets in response to the packets it sends. Most often, connection timed out is the result of a problem on the source or destination hosts, not a problem on a host on the path between the two.

Potential causes for this problem are as follows:

- Destination host is not running.
- Host's broadcast address or address mask is incorrectly defined in its /etc/rc.local file.
- Local host does not have its IP address properly defined in the /etc/hosts file.

- ARP entries on the source or destination host are inaccurate.
- Cabling problem exists.
- LAN problem exists.
- Intermediate router is not running, but the routing protocols have not discovered this yet.
- WAN problem exists.

Troubleshooting Strategy

A. Determine whether the problem is on the source host, the destination host, or a host on the path between the two.

B. On the problem host, check for problems with the following:

   - Broadcast address
   - /etc/hosts file
   - Hardware
   - ARP entries
   - LAN connections
   - WAN connections

Troubleshooting Procedure

A. **Determine whether the problem is on the source host, the destination host, or a host on the path between the two.**

   1. Use the ping command to determine if the destination host is running:

      ```
      % ping hostname
      ```

      - If the ping command returns the message, "hostname is alive," the destination host is operational. The destination host may have just been coming up when the user tried to reach it before, or the problem may be transient. Try the original network operation again.
      - If the ping command returns the message, "no response from hostname," continue with the next step.

2. Use the ping command to determine if the source host can reach other hosts on its subnet.

   ```
   % ping hostname
   ```

   - If the source host can reach other hosts on its subnet, go to the destination host, if possible. Use the ping command to see if the destination host can reach other hosts on its subnet.

     If you cannot physically check the destination host, or call someone on the destination host to check its availability, then work with your local network administrator to try to determine the status of the destination host.

     - If the destination host can reach other hosts on its subnet, then the problem may involve an IP router between the source and destination hosts. Trace the routing path using the netstat or traceroute tools to locate the problem host, and go to step B.
     - If the destination host cannot reach other hosts on its subnet, then the problem is on the destination host. Go to the destination host and continue with step B.

   - If the source host cannot reach other hosts on its subnet, then source host is the problem host. Go to step B.

B. **Perform the following steps for the problem host.**

The problem host may be the source host, the destination host, or any host on the path between the source and destination hosts, as you determined in step A or through tracing the path.

The following steps use the term "local" to refer to the host on which you perform the action required. The term "remote" refers to any host you try to reach using the action.

1. Confirm that the broadcast address and address mask for the local host are properly setup in the /etc/rc.local file, and that the network device is properly configured.

   If you are not sure what the broadcast address and address mask is for the local host, check with the local network administrator, and make any changes necessary in the /etc/rc.local file.

   Use the following command to display the configured network devices:

   ```
   # netstat -i
   ```

If the network device is not configured, configure it using the /etc/ifconfig command, using the following example as a guideline:

```
# /etc/ifconfig qe0 `/bin/hostname` broadcast 16.0.255.255
# netmask 255.255.0.0
```

2. Make sure the local host's /etc/hosts file has the correct IP address for the local host.

   If the IP address is incorrect, the local host can reach other hosts, but other hosts that try to reach the local host receive connection timed out.

3. Make sure the cabling from the local host to the network is intact and properly connected.

4. Use the following netstat command to determine whether any input or output errors exist.

   ```
   % netstat -i
   ```

   Input errors indicate that a host or hosts are sending bad packets. Most likely, the problem is a hardware error on the host sending the bad packets. Use a protocol analyzer or LTM to determine which host is sending the bad packets.

   Output errors indicate a hardware problem on the problem host. Use the following uerf command to display errors, then call Digital Services:

   ```
   # uerf -R
   ```

Note

If the remote host is connected to the local host through a LAN connection, perform steps 5 through 8.

If the remote host is connected through a WAN connection, go to step 9.

5. If the remote host is on the problem host's LAN, use the following arp command to delete the entry for the remote host from the translation tables:

   ```
   # arp -d hostname
   ```

6. Use the ping command to try to reach the remote host, as follows:

   ```
   # ping hostname
   ```

Because the translation tables no longer contain an entry for the remote host, the ping command generates an ARP request for the remote host to reply with its Ethernet address.

- If the remote host is available, it responds with its Ethernet address and the message, "hostname is alive," indicating it is reachable through IP. Try the original network operation again.

Note

If you are performing this step on a host on the routing path, continue tracing the routing path. If you encounter another problem host, go to that host, and repeat step B for that host.

- If the remote host is not available, the ping command returns the message, "no response from hostname." Continue with the next step.

Note

The recommendations section for this problem provides additional information on ARP-related problems.

7. Verify that the local host's software connection to the network is working properly by using the ping or rlogin command to see if the local host can reach other hosts on the local network.
8. If you cannot get to other directly connected hosts, a LAN problem such as LAN segmentation, a babbling device, or a broadcast storm may exist.

   Use tools such as LAN Traffic Monitor, NMCC/VAX ETHERnim, or DECmcc Management Station for ULTRIX to isolate the problem, and see the troubleshooting procedures in this chapter for "LAN Segment Communication Problem," "Babbling Device," and "Broadcast Storm."

Note

If the remote host is connected to the local host through a WAN connection, perform steps 9 through 12.

9. If the furthest host you were able to reach when tracing the routing path is connected through a point-to-point link (WAN), use the following netstat command to display errors on that host:

   ```
   % netstat -i
   ```

   - If the netstat command displays no errors, the network connections are working properly, but the remote host may be down.
   - If the netstat command displays input or output errors, a host modem, wire, or cable is sending bad packets or corrupting packets. Continue with the next step, performing modem loopback tests to determine if the problem is one of the following:
     - Local or remote hardware
     - Common carrier circuit between hosts
     - Cabling between the modem and the interface
     - Local or remote modem

10. Perform local loop tests on the modems at both the local and remote ends.

    If either the local or remote modems fail, this is the source of the connection timed out problem. Replace the failing modem, and try the original network operation again. Otherwise, continue with the next step.

11. Put the modem on one end in remote loop mode and do a remote loop self-test to test the modem's operation with the common carrier circuit.

    If this test succeeds, go to step 12.

    If the local loop self-test succeeded at both the local and remote ends, and the remote loop self-test fails, the common carrier circuit is out of order.

    Call the common carrier for repair service.

12. Use a breakout box to make sure that the cables are connected and the signaling is correct on both the local and remote ends, and that both ends can transmit and receive data. Repair any broken cables.

Recommendations

- In solving this problem, you may find that an intermittent or transient problem may have caused the original connection timed out message.

  If your site uses tools that record historical data, check to see if any thresholds were reached or surpassed. These threshold values might have caused the connection timed out message.

- ARP tables can contain inaccurate entries due to the way some systems perform ARP cache timeouts. Inaccurate ARP entries can occur in the following cases:
  - When a host's Ethernet interface is replaced
  - When DECnet starts on a host
  - When a system running DECnet reboots but does not restart DECnet

  To help isolate inaccurate ARP entries, check to see if various hosts on the same Ethernet can reach another host on the Ethernet. For example, if Host X can reach Host Y, but Host Z cannot reach Host Y, check the ARP entries for Host Z.

  To solve problems due to inaccurate ARP entries, remove the old ARP entry from the translation tables using the **arp -d** command.

Note

Problems can also occur with ARP entries on hosts running both DECnet and TCP/IP, if the software is not started in the proper order. If a host is running both DECnet and TCP/IP, make sure the DECnet software starts first, so that IP never propagates the non-DECnet Ethernet address through ARP.

When Phase IV DECnet starts, it modifies the Ethernet hardware address with a six-octet DECnet address, even if another protocol is already started and is using the address. DECnet must modify the Ethernet address to be able to function on the Ethernet controller.

If a host is running only TCP/IP, its ARP entries are based on the unaltered Ethernet address. If the host then starts DECnet (which changes the Ethernet address), all the existing ARP entries become incorrect.

DECnet Ethernet addresses start with AA-00-04-00. The last two octets of the Ethernet address are the DECnet node address.

Host Is Unreachable

Symptoms

Users on TCP/IP networks receive the following message when trying to access a remote host:

```
host is unreachable
```

Explanation

This is a TCP/IP problem, resulting from any of the following:

- Remote host is not available because it is not up and running.
- Local host's routing information for the remote host is incorrect.
- Local host has a problem that prevents it from communicating with any other hosts on the network.
- Destination network or the remote host has a problem that does not prevent the local host from reaching the destination network, but prevents the local host from reaching the destination host on that network.

If the remote host is up and running but you still cannot reach it, the problem may be caused by any of the following:

- Misconfigured or unconfigured network devices
- Cabling or connection problems
- Improper routing table setup
- Failure to set up routing tables
- Routing daemon problems

Note

This message may not indicate a problem. Routers along the path to the remote host might have security features enabled that prevent you from reaching the remote host.

Host Is Unreachable

Troubleshooting Strategy

Assuming that the remote host is up and running, make sure that the following are correct:

A. Configuration of the network devices on the local host

B. Routing tables on the local host

C. Remote host's address-to-name translation on the local host, including the ARP translation for the Ethernet address to the IP host name

D. Configuration of the network devices on the remote host

Troubleshooting Procedure

A. Make sure that the network devices are configured properly on the local host, using the following steps:

   To check the configuration, you need to know the netmask and broadcast address for your network. The /etc/ifconfig command sets up the network devices. At system startup, the /etc/rc.local file configures the network devices.

   1. Use the following command to display the configured network devices:

      ```
      # netstat -i
      ```

   2. If the necessary network device is not configured, configure it using either the /etc/ifconfig command or the netsetup command as follows:

      To configure the network device with the /etc/ifconfig command, use the following example as a guideline:

      ```
      # /etc/ifconfig qe0 `/bin/hostname` broadcast 16.0.255.255
      netmask 255.255.0.0
      ```

      This example configures a DEQNA for network 16, with the second octet of the address set for subnet addressing.

      To configure the network device with the netsetup command, log in to the superuser account.

      For first time configurations, use the following command:

      ```
      # /etc/netsetup install
      ```

      For all existing configurations, use the following command:

      ```
      # /etc/netsetup
      ```

The netsetup program prompts you for information about the remote host, and adds the information you supply to the /etc/rc.local file. The changes you make take effect when you reboot the system.

B. Check the local host's routing tables, remembering that routing can occur through a host-specific route, a route specified for the destination network, or a default route.

1. Use the following command on the local host to display the contents of the routing tables.

```
# netstat -r
```

If the Routing Tables Show...	Go to...
A host-specific or destination network route	Step 2
A default route	Step 3
No route information	Step 4

2. If the routing tables show a host-specific or destination network route for the destination host, use the ping command to see if the IP router specified is reachable.

```
# ping IP_router_name
```

- If you cannot reach the IP router, make sure that the local host's cabling to the network is intact, and do the same for the IP router's cabling to the network.
- If you can reach the IP router, obtain the routing information from the router, and go to the table in step B1. The table in step B1 specifies what to do based on the type of routing information in the routing tables.

3. If the netstat command shows a default route, use the ping command to see if the default IP router is reachable:

```
# ping IP_router_name
```

- If the IP router is not reachable, make sure that the local host's cabling to the network is intact, and do the same for the IP router's cabling to the network.
- If the IP router is reachable, obtain the routing table from the router, and go to the table in step B1. The table in step B1 specifies what to do based on the type of routing information in the routing tables.

4. If no route exists to the destination, add a route.

You can run the routing daemon to add routes automatically or use the route command to add the specific route manually to a router.

Using the Routing Daemon to Add Routes Automatically

a. Use the following command to see if the routing daemon (/etc/routed) is running:

```
# ps -aux | grep routed
```

The following example of output from this command shows that routed is running in quiet mode. ❶

```
root        77  0.0  0.8  204   88 ?  S  ❶ 4:42 /etc/routed -q
root      7255  0.0  0.3   40   32 p1 S     0:00 grep routed
```

b. If the routing daemon is running, but there are still no routes, the local host is not receiving the routing updates.

Check the local host's cabling to the network.

c. If the routing daemon is not running, but should be, run the routing daemon in quiet mode as follows:

```
# /etc/routed -q
```

d. Make sure that the /etc/routed -q command is in the /etc/rc.local file.

e. Wait a couple of minutes to allow for the routing tables to be filled and try to reach the remote host again.

If you still get the host is unreachable message, go to step B1, and repeat the procedure, now using the updated routing tables.

Using the Route Command to Add a Route Manually

a. To add a default route to a stable IP router, use the following command:

Note

Use an IP router that is only one hop away.

```
# route add default IP_router_name 1
```

b. Try to reach the remote host again.

c. If you still get the host unreachable message, go to step B1, and repeat the procedure.

C. On the local host, resolve any problems with the ARP entry for the remote host.

1. Clear the ARP table entry for the remote host using the following command:

   ```
   # arp -d hostname
   ```

2. Use the procedures in the "Unknown Host" problem in this chapter to make sure that the IP address is correct for the host name.
3. Try to connect to the remote host.
4. If the connection fails, perform the procedure in step A, then go to step 5.
5. If you make changes when you use step A, use the following command to clear the ARP table entry for the remote host:

   ```
   # arp -d hostname
   ```

6. Check the ARP table to see if the entry is correct, using the following command:

   ```
   # arp hostname
   ```

   If the arp command shows no translation, the remote host is not responding, and may be down.

D. Log in to the remote host, and make sure that the network devices on the remote host are properly configured using the procedure in step A.

Login Incorrect

Symptoms

A user on an ULTRIX system receives the following message when attempting to access a remote host:

```
Login incorrect
```

Explanation

This symptom indicates an ULTRIX host problem involving the Internet Protocol (IP). The user specified an incorrect account or password, or both, when attempting to access a remote host.

Note

This symptom may not indicate a problem. It is possible that the user is not intended to have an account on the remote host. Before you try to resolve this problem, be sure the user is intended to have access to the remote host.

Troubleshooting Strategy

1. If the user is intended to have access to the remote host, but does not have an account on the remote host, log in to the superuser account and create an account for the user.
2. If the user has an account on the remote node but cannot access it due to problems with the password, log in to the superuser account and modify the user's password in the /etc/passwd file.

Troubleshooting Procedure

1. If access is determined according to the /etc/password file, use the following command to display the contents of the /etc/passwd file, where username is the user's login name.

   ```
   # grep username /etc/passwd
   ```

If Yellow Pages (YP) is the method used to determine access, use the following command instead:

```
# ypcat passwd | grep username
```

2. Look for an entry for the user in the /etc/passwd file. If no entry exists for the user, go to step a. If an entry exists, but is incorrect, go to step b.

   a. If no account exists for the user, and the user is intended to have access to the remote host, execute the following command from the superuser account:

   ```
   # adduser
   ```

   When you execute the adduser command, the system displays questions you must answer regarding the account you are creating. Answer the questions appropriately for the user.

   b. If an account exists, but the user cannot recall the password, use the following command to define a new password for the user:

   ```
   # passwd username
   ```

Network Is Unreachable

Symptoms

Users on a TCP/IP network receive the following message when trying to connect to a host on a different network:

```
network is unreachable
```

Explanation

A host or IP router is sending the local host an ICMP message indicating that no path exists to the remote host's network. You can use the information from the ICMP message to help you understand how far your connection request traveled before it failed.

The problem is either on the local host or on the path between the local and remote hosts. If the problem is on the local host, it may involve the local host's hardware, connection to the network, or routing tables. If the problem is not on the local host, it involves the path between the local and remote hosts.

Note

This message may not indicate a problem. Routers along the path to the remote host might have security features enabled that prevent you from reaching the remote host.

Troubleshooting Strategy

Make sure the following are correct:

A. Configuration of the network devices on the local host

B. Routing tables on the local host

Trace the path looking at each IP router's routing tables to ensure that there is an entry for the remote host's network. Repair the incorrect IP router's routing tables.

Note

This step requires a thorough knowledge of your topology.

C. Local host's address-to-name translation for the remote host is correct.

Troubleshooting Procedure

A. Make sure that the network devices are configured properly on the local host, using the following steps:

To check the configuration, you need to know the netmask and broadcast address for your network. The /etc/ifconfig command sets up the network devices. At system startup, the /etc/rc.local file configures the network devices.

1. Use the following command to display the configured network devices:

```
# netstat-i
```

2. If the necessary network device is not configured, configure it using either the /etc/ifconfig command or the netsetup command as follows:

- To configure the network device with the /etc/ifconfig command, use the following example as a guideline:

```
# /etc/ifconfig qe0 '/bin/hostname' broadcast 16.0.255.255
  netmask 255.255.0.0
```

This example configures a DEQNA for network 16, with the second octet of the address set for subnet addressing.

- To configure the network device with the netsetup command, log in to the superuser account.

For first time configurations, use the following command:

```
# /etc/netsetup install
```

For all existing configurations, use the following command:

```
# /etc/netsetup
```

The netsetup program prompts you for information about the remote host, and adds the information you supply to the /etc/rc.local file. The changes you make take effect when you reboot the system.

B. Check the local host's routing tables, remembering that routing can occur through a host-specific route, a route specified for the destination network, or a default route.

1. Use the following command on the local host to display the contents of the routing tables:

```
# netstat -r
```

If the routing tables show...	Go to...
A host-specific or destination network route	Step 2
A default route	Step 3
No route information	Step 4

2. If the routing tables show a host-specific or destination network route for the destination host, use the ping command to see if the IP router specified is reachable.

   ```
   # ping IP_router_name
   ```

   - If you cannot reach the IP router, make sure that the local host's cabling to the network is intact, and do the same for the IP router's cabling to the network.
   - If you can reach the IP router, obtain the routing information from the router, and go to the table in step B1. The table in step B1 specifies what to do based on the type of routing information in the routing tables.

3. If the netstat command shows a default route, use the ping command to see if the default IP router is reachable:

   ```
   # ping IP_router_name
   ```

   - If the IP router is not reachable, make sure that the local host's cabling to the network is intact, and do the same for the IP router's cabling to the network.
   - If the IP router is reachable, obtain the routing table from the router, and go to the table in step B1. The table in step B1 specifies what to do based on the type of routing information in the routing tables.

4. If no route exists to the destination, add a route.

   You can run the routing daemon to add routes automatically, or use the route command to add the specific route manually to a router.

   ### Using the Routing Daemon to Add Routes Automatically

   a. Use the following command to see if the routing daemon (/etc/routed) is running:

   ```
   # ps -aux | grep routed
   ```

The following example of output from this command shows that routed is running in quiet mode. ❶

```
root       77  0.0  0.8  204   88 ?  S  ❶ 4:42 /etc/routed -q
root     7255  0.0  0.3   40   32 pl S     0:00 grep routed
```

b. If the routing daemon is running, but there are still no routes, the local host is not receiving the routing updates.

   Check the local host's cabling to the network.

c. If the routing daemon is not running, but should be, run the routing daemon in quiet mode as follows:

```
# /etc/routed -q
```

d. Make sure that the /etc/routed -q command is in the /etc/rc.local file.

e. Wait a couple of minutes to allow for the routing tables to be filled and try to reach the remote host again.

   If you still get the host is unreachable message, go to step B1, and repeat the procedure, now using the updated routing tables.

Using the Route Command to Add a Route Manually

a. To add a default route to a stable IP router, use the following command:

Note

Use an IP router that is only one hop away.

```
# route add default ip_router_name 1
```

b. Try to reach the remote host again.

c. If you still get the host is unreachable message, go to step B1, and repeat the procedure.

C. Make sure the local host's address-to-name translation for the remote host is correct.

1. Use the procedures shown in the "Unknown Host" problem in this chapter to check the address-to-name translation.
2. Try to connect to the remote host.

Permission Denied

Symptoms

When using commands which are executed remote hosts (such as rsh and rcp), the user receives the following message, and the operation fails:

```
Permission denied
```

Explanation

This problem affects ULTRIX hosts and involves the Internet Protocol (IP).

ULTRIX systems determine whether to permit access for remote users through one of the following files:

- .rhosts file
- /etc/hosts.equiv file

When the permission denied message occurs, the problem may be due to one or more of the following:

- Incorrect host and user definitions in the user's .rhosts file on the remote host
- Improper setup of the /etc/hosts.equiv file
- Improper directory or file protection on files to be copied or the .rhosts file

Note

This symptom may not indicate a problem. It is possible that the remote host may be intentionally preventing remote access. Before you try to resolve this problem, be sure that the user is intended to have access to the remote host.

Permission Denied

Troubleshooting Strategy

Make sure that the following conditions are met:

- The .rhosts file on the remote host contains the proper host and user definitions.
- The /etc/hosts.equiv file is set up properly.
- The directory and file protections are correct on the following files:
  - file to be copied
  - remote .rhosts file

Troubleshooting Procedure

Do the following on the remote host:

1. Display the contents of the /etc/hosts.equiv file, to determine if the user's host name is in that file:

   ```
   # grep hostname /etc/hosts.equiv
   ```

   - If the command returns you to the prompt, no entry exists in the /etc/hosts.equiv file for the host name you specified. If your site's security policy permits, you can edit the /etc/hosts.equiv file and add the host name.

   Note

   If you mistype the host name in the grep command, grep will not locate the host name even if the host name is in the file. Before you make any changes to the /etc/hosts.equiv file confirm that the host is not already in the /etc/hosts.equiv file.

   - If the command displays an entry, make sure the host name is correct for the user.
   - If the entry is incorrect, modify the file to contain the correct definitions.

2. Use the following command to move to the user's login directory so you can check the .rhosts file:

   ```
   # cd users_login_directory_name
   ```

3. Use the ls command to determine if a .rhosts file exists.
4. If the user's login directory does not contain a .rhosts file, use a text editor to create one that contains the correct user name and host name for the user.

5. If the user's login directory has a .rhosts file, use the following command to display its contents:

   ```
   # grep hostname .rhosts
   ```

   If the user or host name is missing or incorrect, modify the .rhosts file so that it contains the correct definitions.

   Note

   Be aware that some name services require the full domain name form of a host name, some require only a shortened form of the domain name. Be sure to use the proper form for the name service you use.

   Also, if you are *not* running the domain name system with long names, your /etc/hosts file must not define host names with a long name directly following the IP address. If you are using short host names, then make sure your /etc/hosts file has short names only.

6. Make sure that the local host knows about the remote host.

   Although the local host may receive the message, permission denied, the true cause of the problem may be that the remote host is unknown. See "Unknown Host" in this chapter for more information on how to correct this problem.

7. Use the following command to confirm that you are in the user's login directory:

   ```
   # pwd
   ```

8. From the user's directory, use the following command to check the directory and file protections on any files the user wants to access (including .rhosts):

   ```
   # ls -l file-name
   ```

   The user needs read access at the file level.

9. If the files do not have read privilege, use the following command to change the file and directory protection:

   ```
   # chmod u+r file-name
   ```

10. Use the following command to display the protection on the directory:

    ```
    # ls -l -d
    ```

    The user needs read and write privileges to use rcp.

11. If the directory does not have read and write privileges, use the following command to change the file and directory protection:

    ```
    # chmod u+w,r directory-name
    ```

Client-Based Messages for DOS

This section lists TCP load/init messages and FTP messages that are displayed on the station. Each message is followed by an explanation of its probable cause and a recommended recovery action.

Messages of each type are listed in ascending numerical order.

Message Format

The format of client TCP/IP messages is:

- NET####: message text
- FTP####: message text
- NMF####: message text

where #### is a four-digit number that identifies the message and message text is a short message that describes the error or status condition that generated the message.

Load/Init Errors

NET0100: Incorrect value for *<parm name>* detected in PROTOCOL.INI file by *<module name>*.

Cause: An incorrect value or incorrect number of values for a parameter was found in the PROTOCOL.INI file. *<module name>* is the name of the network module that encountered the incorrect value. *<parm name>* is the name of the parameter that has the incorrect value.

Action: Correct the value in the PROTOCOL.INI file.

NET0101: The value for *<parm name>* not found in PROTOCOL.INI file by *<module name>*.

Cause: Either a parameter is missing or the value for the parameter is missing from the PROTOCOL.INI file.

Action: The parameter and its value should be added to the PROTOCOL.INI file.

NET0102: Cannot load *<module name>* *<vers>*: incompatible DOS version.

Cause: The network could not be loaded because it cannot execute on the version of DOS that is currently on the PC netstation. The version of DOS must be 3.0 or greater. *<module name>* is the name of the network module that detected the incompatible DOS version. *<vers>* is the version number of the network module. In addition, you will get this error message if you try to load the network software in the OS/2 DOS-compatibility environment.

Action: On a DOS PC client, install a version of DOS that is 3.0 or greater. If you are in the OS/2 DOS-compatibility environment, restart your computer to run DOS, and try the command again.

NET0103: Insufficient memory to allocate *<value>* *<parm name>* by *<module name>*.

Cause: There was not enough memory for the network software to obtain internal resources that it needs, for example, internal buffers used by the network software. *<module name>* is the name of the network module that was unable to obtain the resource. *<value>* is the amount of the resource and *<parm name>* is the name of the parameter/resource.

Action: Lower the amount of the resource that was being requested.

NET0104: Insufficient memory to initialize *<module name>*.

Cause: There was not enough memory to obtain all the resources needed by a network module *<module name>*, for example, internal buffers used for sending messages.

Action: Lower the amount of resources needed by *<module name>* in order to fit in the amount of resources available.

NET0105: Bind failure: *<module name>* cannot bind to *<module name>*.

Cause: For the network to load successfully, each piece of the network software must load successfully. This error is displayed when it has been detected that not all network modules loaded successfully. The first *<module name>* is the name of the network module that is now failing to load. The second *<module name>* is the name of the network module that is not loaded.

This situation could arise from the following:

- Upon loading, a module detected an error and failed to load. In this case, an error message indicating the problem should have been displayed (prior to the current one).
- If the CONFIG.SYS or AUTOEXEC.BAT file have been modified, it is possible that one of the network module names may have been deleted and, as a result, that module did not load.

- If a secondary protocol stack is being used, it must be manually loaded before executing the service that requires it.

Action: Have the network administrator determine the cause of the problem and make any necessary corrections. If the CONFIG.SYS or AUTOEXEC.BAT file has been modified, use a backup copy of the CONFIG.SYS or AUTOEXEC.BAT file.

NET0106: Open failure on PROTOCOL.INI by <*module name*>.

Cause: An error occurred while trying to open the PROTOCOL.INI file. <*module name*> is the name of the network module that encountered the problem.

Action: Check CONFIG.SYS for the PROTMAN installation line:

```
DEVICE=PROTMAN.DOS/I: <PROTOCOL.INI path>
```

Verify that the PROTOCOL.INI file is present in the directory indicated in the CONFIG.SYS file. The DEVICE=PROTMAN.DOS line in the CONFIG.SYS file should contain a /I option followed by the path to the PROTOCOL.INI file. Verify there are no characters or spaces between the PROTOCOL.INI path and the end-of-line.

If the file is being read from a flexible disk, make sure the disk is inserted in the disk drive.

NET0107: Read failure on PROTOCOL.INI by <*module name*>.

Cause: An error occurred while trying to read the PROTOCOL.INI file. <*module name*> is the name of the network module that encountered the problem.

Action: If the file is being read from a flexible disk, make sure the disk is inserted in the disk drive. If the problem persists, try restoring a backup copy of the file.

NET0108: Close failure on PROTOCOL.INI by <*module name*>.

Cause: An error occurred while trying to close the PROTOCOL.INI file. <*module name*> is the name of the network module that encountered the error.

Action: If the file resides on a flexible disk, make sure the disk is inserted in the disk drive.

NET0109: TCP is not loaded—detected by <*module name*>.

Cause: A network module (named TCP) whose services are required by <*module name*> has not been loaded. This may be due to errors detected when the TCP module attempted to load, or because the TCP module has been deleted from the load process; that is, the TCP module was deleted from the CONFIG.SYS file.

Action: Check that the configuration file contains the line:

```
DEVICE=TCPDRV.DOS
```

If the configuration file contains the DEVICE=TCPDRV.DOS line, restart and look for error messages. The loading process pauses when an error is encountered.

NET0110: Insufficient memory to load <*module name*> <*vers*>.

Cause: As the network is loading, modules are "relocated" or moved to other areas in memory to make more efficient use of available memory. In this case, there was not enough memory to relocate a network module. <*module name*> is the name of the network module that could not be moved.

Action: Try to make more memory available. One way to do this when running DOS is to have the network administrator reduce the number of resident programs that are present in memory.

NET0111: Error accessing NEMM.DOS. <*module name*> <*vers*> not loaded.

Cause: NEMM.DOS (Network Expanded Memory Manager) is a network module whose presence is required by all other network modules, or they cannot load. Either NEMM.DOS has been corrupted on the disk or it has been accidentally deleted from the load process. <*module name*> is the name of the network module that is not loaded.

Action: Verify that NEMM.DOS has not been accidentally deleted from the load process: there should be a DEVICE=NEMM.DOS line in the CONFIG.SYS file. If CONFIG.SYS is correct, NEMM.DOS can be copied from the installation disks to the proper directory. If there are a number of corrupted files, rerun tcpsetup in order to reinstall the network software.

NET0112: Relocation failure. <*module name*> <*vers*> not loaded.

Cause: At load time, network modules are moved in memory to make the most efficient use of memory. In this case, a network module could not be moved to the desired location. This may be due to corruption of the network module as it resides on disk. <*module name*> is the name of the module that could not be relocated. <*vers*> is the module's version number.

Action: Reinstall the network by rerunning tcpsetup. If the load continues to file, contact your network administrator.

NET0113: Network context failure. <*module name*> <*vers*> not loaded.

Cause: A network module detected an error while accessing expanded memory. This may be due to corruption of the network's NEMM.DOS module, or it may be due to errors in the expanded memory software or hardware. <*module name*> is the name of the network module that failed to load; <*vers*> is the module's version number.

Action: Reinstall the network using tcpsetup. If the error persists, run the diagnostics provided with the expanded memory hardware.

NET0114: Warning: memory release failure in <*module name*> <*vers*>.

Cause: An error occurred when the network module <*module name*> attempted to release system memory it no longer requires. This is a diagnostic warning only; the module was able to load and should function properly; however, a small amount of system memory will not be accessible. <*module name*> is the name of the network module that detected the error. <*vers*> is the module's version number.

Action: None—this is only a warning. If you continue to get this message, restart to free memory not released.

NET0116: TCP access failure by <*module name*>.

Cause: The network module, <*module name*>, detected an error while accessing the network TCP module. This may be due to corruption of either <*module name*> or the network TCP module.

Action: Reinstall the network using tcpsetup.

NET0117: Incorrect PROTOCOL.INI format detected by <*module name*>.

Cause: Information in the PROTOCOL.INI file is incorrectly formatted, due to corruption of the file.

Action: Replace the PROTOCOL.INI file with a backup copy.

NET0118: Insufficient TCP resources to load <*module name*>.

Cause: The parameter configurations for the network TCP module do not contain enough resources to allow <*module name*> to load. This may be due to modifying PROTOCOL.INI and changing parameters for one or more services modules without changing the corresponding TCP resources.

Action: Remove and reinstall the client TCP software to build a new PROTOCOL.INI file and to establish a proper base configuration for network module resources at load time.

NET0119: PROTOCOL.INI file too large.

Cause: There is not enough memory to analyze the contents of the PROTOCOL.INI file. The PROTOCOL.INI file exceeds the 8 kilobytes maximum size allowed.

Action: Edit PROTOCOL.INI and remove unnecessary entries in order to decrease the size.

NET0120: Logical driver name <*name*> not found in PROTOCOL.INI.

Cause: The specified logical driver name was not found in PROTOCOL.INI.

Action: Rerun tcpsetup to create a new PROTOCOL.INI file.

NET0121: Insufficient TCP resources to load <*module name*>.

Cause: The parameter configurations for the network TCP module do not contain enough resources to allow <*module name*> to load. This may be due to modifying PROTOCOL.INI and changing parameters for one or more services modules without changing the corresponding TCP resources.

Action: Rerun tcpsetup to build a new PROTOCOL.INI file and to establish a proper base configuration for network module resources at load time.

NET0122: Exceptional error condition detected by <*module name*>.

Cause: An internal software error has occurred.

Action: Restart your PC client.

NET0123: Cannot access Protocol Manager.

Cause: An error occurred while trying to access the Protocol Manager. This error can occur if the Protocol Manager device driver has not been configured in CONFIG.SYS, or if Protocol Manager cannot be accessed due to an unexpected software error.

Action: Be sure that CONFIG.SYS contains the following line:

```
DEVICE=<path>PROTMAN.DOS/I: <PROTOCOL.INI  path>
```

Verify that the PROTOCOL.INI file is present in the directory indicated in the CONFIG.SYS file.

NET0124: TCP/IP module must be loaded before Windows/386.

Cause: An error occurred trying to load TCP TRS inside the Windows/386 environment. The TCP/IP module was not loaded. The loading process stops.

Action: First, load the TCP/IP module. Then, load Windows/386.

NET0125: NETBIND must be executed before TCP/IP TSR module is loaded.

Cause: An error occurred trying to load the TCP/IP TSR module. The NETBIND program was not executed.

Action: First, run NETBIND. Then, load the TCP/IP TSR module.

FTP Errors

FTP1000: Ambiguous command—does not contain enough characters to be uniquely identified.

Cause: The FTP command specified does not contain enough characters to uniquely identify the command you want to use. For example, RE is an ambiguous command because it could mean either REMOTEHELP or RENAME. In this example, a third letter must be used to uniquely specify the command.

Action: Reenter the desired command specifying the entire FTP command, or enter enough characters so that the command cannot be confused with another valid command.

FTP1001: Unrecognized FTP command.

Cause: FTP did not recognize the command. Either the command was misspelled or it is not supported by this implementation of FTP.

Action: Check the spelling of the command. Retry the operation using a valid FTP command. To invoke the FTP HELP facility, at the FTP prompt type:

```
help
```

FTP1002: Missing closing quotation mark—assumed at end of string.

Cause: FTP detected a missing quotation mark and will proceed as if the quotation mark was at the end of the input string.

Action: If FTP's assumption of the placement for the quotation mark is incorrect, you will need to reissue the command and the quoted data with the intended quotation placement.

FTP1003: String too long—must be no longer than <*length*> characters.

Cause: An invalid string has been entered in response to an FTP prompt. The valid length of a string depends on the state of FTP when the error occurred. <*length*> indicates the maximum length.

Action: Reenter a string that is less than or equal to <*length*> characters.

FTP1004: No match for <*filespec*>.

Cause: This error can occur if a local file (or files) is specified and a file matching the description does not exist. <*filespec*> may include wildcard characters.

Action: Check spelling and use of any wildcard syntax. Perform a local directory listing to see if the file(s) exist.

FTP1005: Unable to change local directory to <*directoryspec*>.

Cause: FTP could not change the current working directory to <*directoryspec*>. This could be caused by incorrect spelling or improper path specification.

Action: Check spelling and syntax of the desired pathname. Verify that the directory exists and reissue the command.

FTP1006: Ambiguous help command: <*command*>.

Cause: An FTP command specified in a HELP request does not contain enough characters to be uniquely identified.

Action: Reenter the HELP command specifying the entire FTP command, or enter enough characters so that the command cannot be confused with another valid command.

FTP1007: Unrecognized help command: <*command*>.

Cause: An FTP command specified in a HELP request is not recognized.

Action: Check spelling of the command. Also check to make sure that the command is supported by this FTP implementation. To invoke the FTP HELP facility, at the FTP prompt type:

```
help
```

FTP1008: Unrecognized option—<*option*> ignored.

Cause: This implementation of FTP does not recognize this option. This error only occurs when an invalid option is specified on the command line when starting FTP. All options that can be specified from the command line may also be set from within the FTP application by issuing the appropriate FTP commands.

Action: Make sure the option is supported, then retype the command.

FTP1009: The drive specification: <*drivespec*> cannot be located.

Cause: A drive specified in the DRIVE command cannot be located. This error occurs if the specified drive does not exist.

Action: Specify a valid drive. If the specified drive is a flexible disk drive, check that a disk is properly inserted into a specified flexible drive and that the door is closed.

FTP2000: Unable to open local file: <*filename*>.

Cause: A local file with the specified <*filename*> could not be opened as requested by FTP. This could be caused by improper spelling of <*filename*>, improper path specification, or by an attempt to open a read-only file for writing.

Action: Check spelling, pathname, syntax, and protections for the specified filename.

FTP2001: Unable to read from local file—file is locked.

Cause: A read was attempted on a locked file. This can happen if you attempt to access a file that another program may have open.

Action: Determine if another program has the file open. If the error persists, restart the computer to reset all of the open files.

FTP2002: Unable to write to local file.

Cause: A write was attempted to a read-only file, or the disk is full.

Action: Check file protections on the filename specified in the command and check to verify that the disk to which the file was being written is not full.

FTP2003: Error loading command interpreter.

Cause: FTP is unable to provide a temporary command line environment. The operating system cannot locate and execute COMMAND.COM for DOS.

Action: Make sure that the command interpreter is specified under COMSPEC. It must also be in a directory that is in the PATH statement.

FTP2004: Unable to establish pathname for current working directory.

Cause: Either there was insufficient memory available for allocation, or the pathname was too long. The maximum pathname length is 66 characters (including the two characters specifying the drive).

Action: Check available memory. Also verify that the pathname does not exceed 66 characters.

FTP3000: Network software not loaded.

Cause: The network transport or the sockets interface has not been loaded prior to attempting to run FTP.

Action: Load either the transport or sockets interface, and then try to run FTP again.

FTP3001: Internal networking error (*<errmsg>* - *<number>*).

Cause: An attempt to interact with the network has failed. *<errmsg>* is a text message describing the type of networking error that has occurred.

Action: The connection will be terminated, and in most cases the FTP application will also be terminated. Try restarting and reloading the network. If the error persists, contact your network administrator.

FTP3002: Time out expired on network service request.

Cause: Due to a lost connection, or an extreme delay in the network, a timer has expired and the connection is assumed lost.

Action: The connection was terminated, and in most cases the FTP application was also terminated. Restarting and reloading the network may solve the problem. If the error persists, contact your network administrator.

FTP3003: Invalid or unknown host: *<hostname>*.

Cause: FTP was unable to match *<hostname>* to an IP address. *<hostname>* may be spelled incorrectly. It may not be listed in a host file, or it may not be registered on the network.

Action: Check the spelling of the hostname and ensure that *<hostname>* is included in the host file if the host file is being used for name to IP address resolution. If the hostname does not work, try using the IP address in the command.

FTP3004: Unable to connect to *<host>* *(<reason>).*

Cause: FTP was unable to initiate a connection to the specified host. *<reason>* is a text message indicating the cause of the failed connection. The reason for the failed connection may be one of the following:

- The connection timed out. For example, a timeout expired prior to connection establishment.
- The connection is refused by the host.

- The host is unreachable. For example, the host is not running or IP addresses may be configured incorrectly.
- Insufficient resources on the network or local PC.

Action: Attempt the connection again at a later time. If the error persists, contact your network administrator.

FTP3005: Session lost—connection reset.

Cause: The session with the remote server has been lost unexpectedly. FTP has reset itself to a disconnected state.

Action: Use the OPEN command to try to reestablish a connection to the remote server.

FTP3006: Data connection closed unexpectedly—transfer failed.

Cause: During the process of data transfer between an FTP client and server, the data connection was closed by the remote host. This error occurs only when data is being transferred from the local machine to the remote host.

Action: Attempt the data transfer again. If the error persists, contact your network administrator.

FTP4000: Not connected to an FTP server—use OPEN first.

Cause: An FTP connection from the local FTP client to an FTP server was not established prior to issuing this command.

Action: After connecting to an FTP server with the OPEN command, try the command again.

FTP4001: Already connected—use CLOSE first.

Cause: An OPEN command was issued when the client is already connected to an FTP server. The OPEN command is only valid when FTP is not currently connected to an FTP server. Only one connection can be OPEN at a time.

Action: No action is needed. If you want to connect to a different server, issue the CLOSE command, then reissue an OPEN command to the desired server.

FTP4002: Server response not understood.

Cause: A response from the FTP server was not understood by the FTP client. It is possible that an error has caused a loss of synchronization between the server and client.

Action: If the error persists, exit FTP. Restart the application and reissue the desired commands. The DEBUG option may be valuable in determining the cause of this error.

FTP4003: Unrecognized transfer type.

Cause: An unsupported or unrecognized transfer type has been specified using the TYPE command.

Action: Be sure to correctly enter only the ASCII and Binary transfer types.

FTP4004: Connection not accepted by server.

Cause: The FTP server is currently unable to accept the connection. The cause of this error is dependent on the implementation of the FTP server to which a connection was attempted. A common cause is the lack of the necessary system or network resources on the FTP server host.

Action: Attempt the connection again at a later time. If the error persists, contact your network administrator.

FTP5000: File list overflow.

Cause: A wildcard expansion has caused an internal FTP buffer to overflow. This may happen if a very generic file specification (for example, *.*) has matched an extremely large number of files. This is possible only on the MGET, MPUT, and MDELETE commands.

Action: Be more specific about the files to be manipulated, or separate the files into smaller categories. For example, where the command MGET *.* may cause the capture buffer to overflow, the command MGET *.c *.h *.asm would probably work.

Network Maintenance Errors

NMF1000: Network driver error.

Cause: An internal network driver error has occurred. The error can be in the TCP driver or the network management driver (NMDRV or NMTSR).

Action: Restart system and try operation again.

NMF1001: Too many parameters.

Cause: Too many parameters are specified in the command line when running PING, ARP, or NETSTAT.

Action: Refer to the chapter TCP/IP Tools, or type PING, ARP, or NETSTAT without any parameters and a brief description on how to use these programs will appear on the screen.

NMF1002: Invalid parameter.

Cause: The parameter(s) specified for PING, ARP, or NETSTAT is invalid.

Action: Refer to the chapter TCP/IP Tools, or type PING, ARP, or NETSTAT without any parameters and a brief description on how to use these programs will appear on the screen.

NMF1005: Need to run NMTSR.EXE first.

Cause: The NMTSR.EXE program is not loaded. You must first run the nmtsr program before using any of the NMF functions.

Action: Run the NMTSR program. Make sure you see the message "NMTSR loaded successfully."

NMF1008: Insufficient memory.

Cause: This can happen in running NETSTAT.EXE and ARP.EXE. It means the system does not have enough memory to perform the operation.

Action: Close some active connections and try the operation again. If this does not solve the problem, restart the system.

NMF1009: Unknown host: <*hostname*>.

Cause: This happens when running PING or ARP with a host name. It means that the host name you enter was not found in the domain name server, and either you do not have a local host file or the name was not in your local host file.

Action: Check the name and make sure it is the name you are trying to resolve. If the name is correct, you can either ask the network administrator to add the name into the name server, or you can add it to the local host file. If you know the IP address of the host you are trying to use PING or ARP upon, you can also use its IP address instead of its host name.

NMF1010: Name server not responding.

Cause: This happens when running PING or ARP with a host name. It means the domain name server you specify in your PROTOCOL.INI file is not responding to the name request. The server may either be down or name service may not be available from that host. Furthermore, your system either does not have a local host file or the name is not found in that file.

Action: There are a number of actions you can consider. First, check the PROTOCOL.INI file to make sure that the IP address of your name server is correct. Second, check to be sure the name server is up and running. You can use PING with the server's IP address to do this. If you already know the IP address of the host you are trying to resolve, you may also bypass the name server by including the name in your local host file, or simply using the IP address instead of host name.

NMF1011: Name server error.

Cause: This happens when running PING or ARP with a host name. It means the name server you specify in your PROTOCOL.INI file encountered some error and was unable to resolve the name.

Action: Report problem to network administrator to see how the problem can be corrected at the name server end. Meanwhile, either use the local hosts file or IP address for PING and ARP.

NMF1012: Domain name server not loaded.

Cause: This happens when running PING or ARP with a host name. In order to resolve a name using the domain name server, you must load the domain name resolver first.

Action: In DOS you should run the DNRTSR.EXE program.

NMF2000: Internet address not available.

Cause: This happens when running NETSTAT -c or NETSTAT -a. The protocol stack is unable to return the internet (IP) address of this host.

Action: Check the PROTOCOL.INI file to make sure the IP address field is correct.

NMF2001: TCP connection table not available.

Cause: This happens when running NETSTAT -t or NETSTAT -a. The protocol stack is unable to retrieve information regarding current TCP connections.

Action: This error message usually is a result of internal TCP driver error. Restart system and try the operation again.

NMF3000: Invalid timeout value.

Cause: The timeout value specified in the PING command line is invalid. A valid timeout value must be between 1 and 300 seconds.

Action: Try the operation again with valid timeout value.

NMF4000: Failed to clear ARP table.

Cause: The ARP table is corrupted. This can be caused by TCP driver internal error or by other programs corrupting the memory.

Action: Restart the system and try the operation again.

NMF4001: Insufficient memory to get ARP table.

Cause: The ARP table is too big to fit in the memory allocated by the ARP.EXE program.

Action: Run ARP -c to clear the ARP table.

NMF4002: ARP table not available.

Cause: This happens when running ARP.EXE. The ARP table is probably corrupted.

Action: Restart the system and try the operation again.

Part 3

Local Area Transport (LAT)

7

Local Area Transport (LAT) Tools

This chapter provides an overview of tools that are available to assist in the configuration, management, and troubleshooting of a Local Area Transport (LAT) network.

Several tools described in this chapter are included with the LAT software components, and others are VMS layered products that must be purchased separately.

This chapter includes the following sections:

- LAT Control Program (LATCP)
- LAN Traffic Monitor (LTM)
- Terminal Server Manager (TSM)

LAT Control Program (LATCP)

The LAT Control Program (LATCP) helps you to configure LAT services to meet your network needs. Understanding LAT configuration options assists you in identifying configuration problems which may occur in setting up a LAT network.

LATCP enables you to see that LAT is loaded and running, to display and define the port and node characteristics, and to verify that the LAT service information is correct.

LATCP is distributed with system and application software as shown in Table 7–1.

Table 7–1 LAT Control Program

Software	Program Name
VMS	LATCP
ULTRIX	LCP
PATHWORKS for DOS	LATCP
PATHWORKS for OS/2	LATCP

Note

Each operating system offers a different user interface to the LAT Control Program. In some cases, different levels of capability are implemented because of differences in the LAT protocol functions available in each environment. LAT server nodes provide a richer set of functions than LAT client nodes.

On LAT servers you can use LATCP to:

- Start and stop LAT services on a LAT server
- Specify the operational characteristics for servers and their services

On all LAT nodes you can use LATCP to:

- Configure LAT services, group codes, and other characteristics
- Display the status for your LAT node
- Show and reset LAT counters

In addition, on DOS and OS/2 nodes, the Netsetup utility uses LATCP to configure LAT characteristics for the node.

LAN Traffic Monitor (LTM)

The LAN Traffic Monitor (LTM) is a VMS layered product consisting of software and hardware that captures and presents traffic data for an Ethernet.

You can use LTM to troubleshoot general LAN problems and determine the amount of LAT traffic on your network. The LTM allows you to actively monitor Ethernet usage by providing real-time data on Ethernet traffic and utilization.

LTM can collect data on all network protocols including LAT, DECnet, TCP/IP, and Systems Communication Architecture (SCA), as well as 802.3 packets.

Use LTM to display traffic rates for a device that is erroneously sending corrupted data on the network (also referred to as a babbling device). If the babbling device is transmitting corrupt information to an address other than its own address, the LTM display lists the babbling device as the top talker on the segment.

Generally, any node generating greater than 50 percent of the traffic could be a babbling device. In Example 7–1, NODEA (see ❶) is probably a babbling device because it is generating more than three-quarters of the network traffic.

Example 7–1 LAN Traffic Monitor Display

```
LAN Traffic Monitor V1.1.0  26-OCT-1990 16:14:58  Listener uptime 03 06:55:31

                     Current Top Ten Talkers Display

       Total Node Addresses : 125    Report Interval :   2.95

Address                Name          Count    Frames/Sec        % Total

AA-00-04-00-3F-12      NODEA           393          133.2         77.7 % ❶
08-00-2B-06-51-C9      LAT 1            25            8.5          4.9 %
AA-00-04-00-4E-13      NODED            23            7.8          4.5 %
08-00-2B-05-E2-63      LAT 2            19            6.4          3.7 %
AA-00-04-00-40-12      NODEM            18            6.1          3.6 %
AA-00-04-00-EE-11      NODEP            15            5.1          3.0 %
AA-00-04-00-7A-11      NODEB            10            3.4          2.0 %
<Other nodes>                            3            1.0          0.6 %

       <Total>              506         171.5        100.0 %
```

LTM Hardware and Software

The hardware portion of LTM consists of the following:

- A terminal capable of running Remote Graphics Instruction Set (ReGIS) software
- A LAN Bridge 100 (Rev. E or higher) or a LAN Bridge 150, attached to the Ethernet cable.

  The LAN bridge runs monitoring software and transmits information to a VMS layered application software program located on any VAX computer in the extended LAN.

  Before you run LTM, check the LAN bridge indicator lights to see if the bridge is set up to operate as a LAN Traffic Monitor. You can verify that the bridge is set up as a LAN Traffic Monitor by performing the following steps:

  1. Check that the SELF TEST, DC OK, and ONLINE lights are on.
  2. Check that the ACTIVITY lights are blinking approximately once per second in a pattern. This pattern indicates that the bridge is operating as a LAN Traffic Monitor.
  3. After you set up the bridge properly, downline load the LTM software to the bridge.

The software portion of the LAN Traffic Monitor consists of the following:

- LTM Listener software

  Using a LAN bridge as a monitoring device, the LTM Listener software counts and classifies Ethernet traffic and periodically reports traffic statistics to the LTM user interface. The LTM Listener can collect traffic data for time intervals from 1 to 48 hours. You can display LAN utilization data based on the traffic data collected for these periods.

- LTM user interface

  The LTM user interface collects and displays data received from the LTM Listener. The LTM user interface also performs data reduction and presents statistics such as the following:

  - Network traffic
  - Top 10 talkers (current, long term)
  - Throughput and utilization (current, long term, peak)
  - List of nodes on the extended Ethernet
  - List of multicast addresses on the extended Ethernet

- List of nodes using a particular protocol
- Node traffic by protocol type
- Multicast traffic by protocol type
- Protocol type traffic

To monitor multiple Ethernet segments, you can distribute multiple LTM Listeners throughout the network. You can also distribute multiple user interfaces throughout the extended LAN.

LTM Privilege Requirements

You need the following privileges on the VMS system used to run LTM:

- OPER
- NETMBX
- TMPMBX

Running LTM

To run LTM, enter the following command:

```
$ TRAFFIC_MONITOR/LAN
```

To get online help while using LTM, enter the following command:

```
TRAFFIC_MONITOR/LAN> HELP
```

To exit LTM, press the PF4 key:

```
TRAFFIC_MONITOR/LAN> PF4
```

Terminal Server Manager (TSM)

Terminal Server Manager (TSM) software is a VMS layered product that allows you to control and observe terminal servers anywhere within an extended local area network.

Terminal servers use the LAT protocol to communicate with other devices on the LAN. Terminal servers are sometimes used to provide modem and printing services on your network. You can use TSM to verify and reconfigure terminal server characteristics on your LAT network.

Note

> You can use TSM to manage terminal servers, but for a PC, you can only monitor the LAT packets transmitted by the PC. That is, you cannot manage LAT on a PC.

TSM runs from a central location on a VMS host system and allows you to do the following:

- Set up and manipulate a database of terminal servers
- Propagate server information from the TSM management directory to the DECnet database
- Set up and maintain terminal servers on the same local area network as the host system
- Perform troubleshooting on the terminal servers registered in the terminal servers database
- Define groups of terminal servers, each of which you can manage as a single entity
- Determine if all defined terminal servers are reachable

Use TSM to display group code definitions and port characteristics, and to define various parameters.

For example, if you receive the error message “Terminal Server Connection Failure”, you can use TSM to display and modify the port characteristics. In Example 7–2, information displayed for node ABC and port 4 shows that the required group code (group code 40) (see ❶) was not enabled on the user’s port (port 4 in this case). Enabling port 4 (see ❷) solves the problem.

To verify the solution, have the user attempt to connect to node ABC again.

Example 7–2 Terminal Server Manager Output

```
$ TERMINAL SERVER MANAGER
TERMINAL_SERVER_MANAGER> USE SERVER ABC
TERMINAL_SERVER_MANAGER> SET PRIVILEGE
password> xxxxxx
TERMINAL_SERVER_MANAGER> SHOW PORT 4
Port 3: r                              Server: ABC

Character Size:          8            Input Speed:       9600
Flow Control:          XON            Output Speed:      9600
Parity:               None            Modem Control: Disabled
Access:              Local            Local Switch:      None
Backwards Switch:     None            Name:            PORT_3
Break:               Local            Session Limit:        4
Forwards Switch:         \            Type:              Soft

Preferred Service: DELNI

Authorized Groups:  41- 44, 46- 49, 54, 56- 59, 79
(Current)  Groups:  41- 44, 46- 49, 54, 56- 59, 79 ❶

Enabled Characteristics:

Autobaud,  Autoprompt,  Broadcast,  Input Flow Control,  Loss Notification,
Message Codes,  Output Flow Control,  Verification

TSM> DEFINE PORT 4 GROUP 40 ENABLED
TSM> SET PORT 4 GROUP 40 ENABLED
TERMINAL_SERVER_MANAGER> SHOW PORT 4
Port 3: r                              Server: ABC

Character Size:          8            Input Speed:       9600
Flow Control:          XON            Output Speed:      9600
Parity:               None            Modem Control: Disabled
Access:              Local            Local Switch:      None
Backwards Switch:     None            Name:            PORT_3
Break:               Local            Session Limit:        4
Forwards Switch:         \            Type:              Soft

Preferred Service: DELNI

Authorized Groups:  40- 44, 46- 49, 54, 56- 59, 79
(Current)  Groups:  40- 44, 46- 49, 54, 56- 59, 79 ❷
TSM> EXIT
```

TSM Requirements

TSM requires the following:

- DECnet software
- Read access to the TSM management directory file
- OPER privilege

To set terminal server parameters with TSM also requires the following privileges and password:

- Privileges on the server
- Server access password
- OPER
- NETMBX
- TMPMBX

Running TSM

You can use the TSM software from the TSM prompt or directly from the DCL prompt.

To run TSM from the DCL prompt, use the following format:

```
$ TSM
```

To get online help for TSM, enter the following command:

```
TSM> HELP
```

To exit TSM, enter the following command:

```
TSM> EXIT
```

8

Isolating Local Area Transport (LAT) Problems

This chapter contains the LAT problem-isolation flowcharts and a series of troubleshooting procedures. The flowcharts help you isolate LAT network problems. After you have isolated a problem, a decision point leads you to a procedure or set of procedures. You can locate the starting page for each procedure in the Contents or in the index.

The master procedures are:

- VMS Server Master Procedure (LAT)
- ULTRIX Server Master Procedure
- DOS Client Master Procedure (LAT)
- DOS Client Master Procedure (LAT)
- OS/2 Client Master Procedure (LAT)
- Network Connection Procedure
- Network Segment Interface Procedure

LAT Problem-Isolation Flowcharts

To isolate a network problem, you must consider several key questions. The answer to each question determines which procedure you should perform. This section contains a table and a series of flowcharts, which ask the questions that guide you through the procedures.

In the flowcharts, the first key question asks if the network has ever carried traffic. If the answer is no, perform the VMS Server Master Procedure (LAT). This master procedure combines several procedures into one. You may not have to perform all of the subprocedures in the master procedure.

The remaining flowcharts ask questions specific to your network. The procedure you should use depends on your answer to questions. You may have to perform client, disk server, file server, or print server procedures.

Note

You should address each question in order. The answer to each question helps you rule out unlikely problems.

Table 8–1 lists the key questions in flowchart order and indicates the path you should take. For example, if your answer to key question 1 is No, go to Figure 8–1, Problem with Untried Network. If your answer is Yes, go to key question 2.

Table 8–1 Key Questions for LAT

	Key Question	If ...	Go to ...
1.	Has the network ever carried traffic?	No	Figure 8–1, Problems on an Untried Network (LAT Flowchart 1)
		Yes	Key Question 2
2.	Has hardware been added or changed?	Yes	Figure 8–2, When Hardware Has Changed (LAT Flowchart 2)
		No	Key Question 3
3.	Has software been modified?	No	Figure 8–3, When Software Is Unmodified (LAT Flowchart 3)
		Yes	Key Question 4
4.	Is there an error message? If not, is there a transport problem?	Yes	Figure 8–4, Problem with Transport (LAT Flowchart 4)
		No	Key Question 5
5.	Is there a problem with remote printing?	Yes	Figure 8–5, Printing Problems (LAT Flowchart 5)

Figure 8–1 Problems on an Untried Network (LAT Flowchart 1)

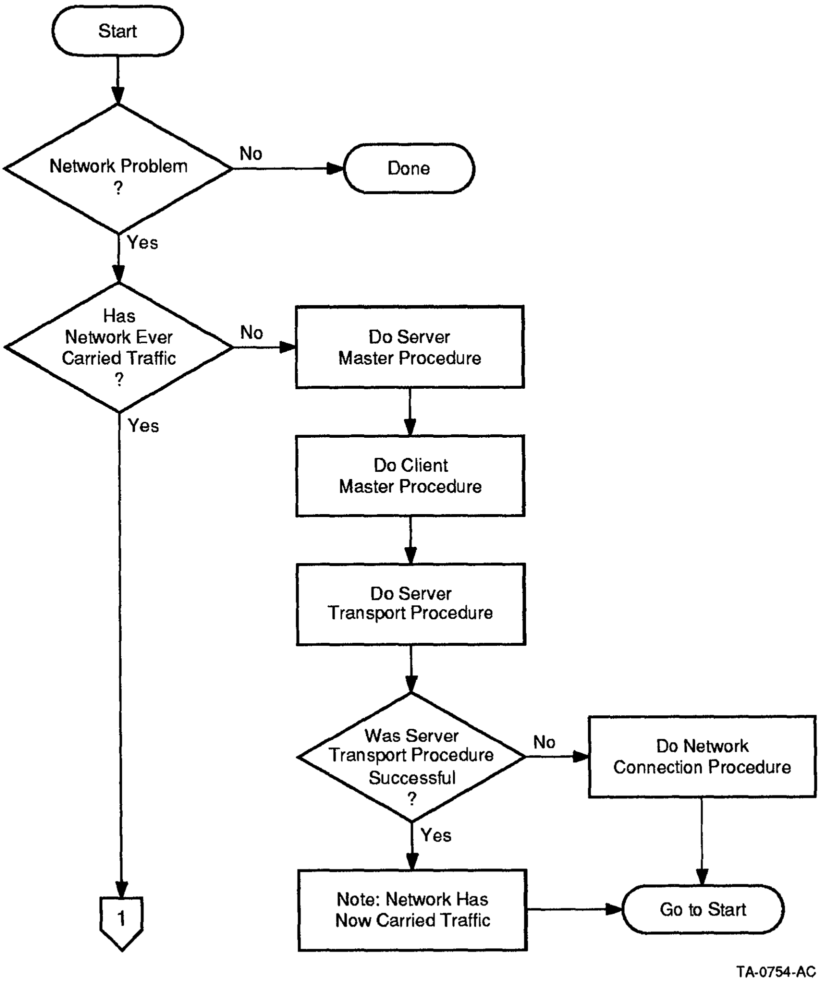

Start
Network Problem ?
No
Done
Yes
Has Network Ever Carried Traffic ?
No
Do Server Master Procedure
Yes
Do Client Master Procedure
Do Server Transport Procedure
Was Server Transport Procedure Successful ?
No
Do Network Connection Procedure
Yes
1
Note: Network Has Now Carried Traffic
Go to Start
TA-0754-AC

Figure 8–2 When Hardware Has Changed (LAT Flowchart 2)

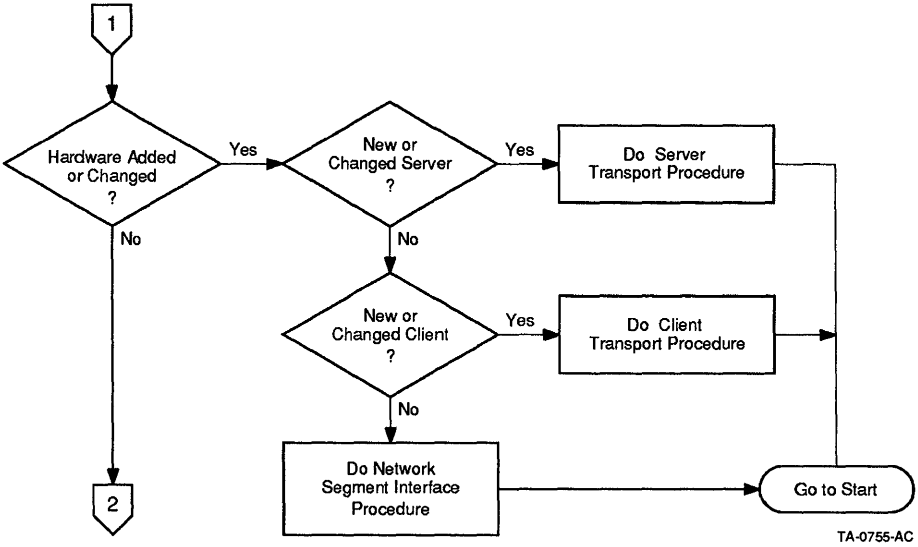

1
Hardware Added or Changed ?
Yes
No
New or Changed Server ?
Yes
No
Do Server Transport Procedure
New or Changed Client ?
Yes
No
Do Client Transport Procedure
Do Network Segment Interface Procedure
Go to Start
2
TA-0755-AC

Figure 8–3 When Software Is Unmodified (LAT Flowchart 3)

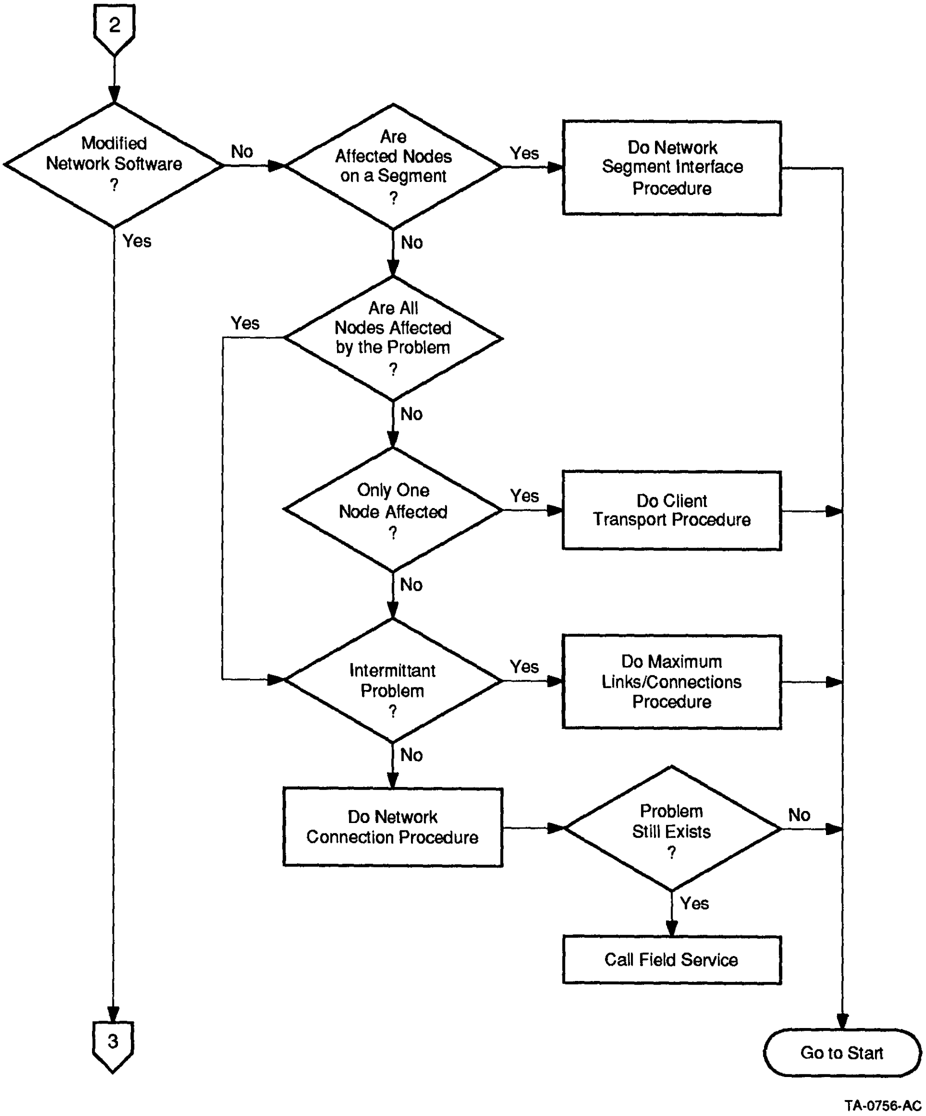

2
Modified Network Software ?
No
Are Affected Nodes on a Segment ?
Yes
Do Network Segment Interface Procedure
Yes
No
Are All Nodes Affected by the Problem ?
Yes
No
Only One Node Affected ?
Yes
Do Client Transport Procedure
No
Intermittant Problem ?
Yes
Do Maximum Links/Connections Procedure
No
Do Network Connection Procedure
Problem Still Exists ?
No
Yes
Call Field Service
3
Go to Start
TA-0756-AC

Figure 8–4 Problem with Transport (LAT Flowchart 4)

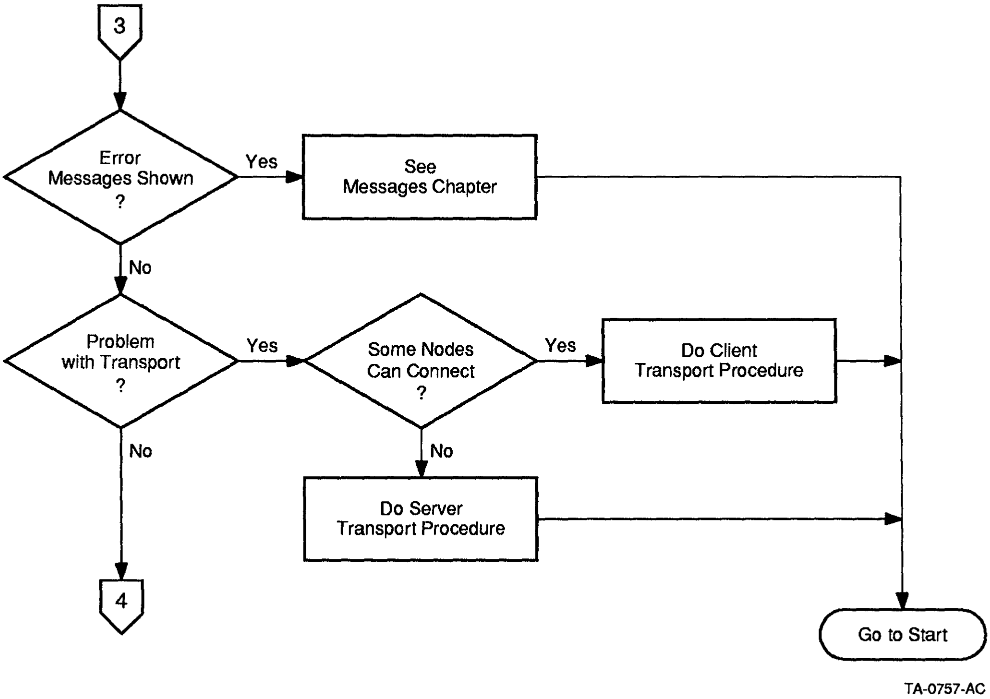
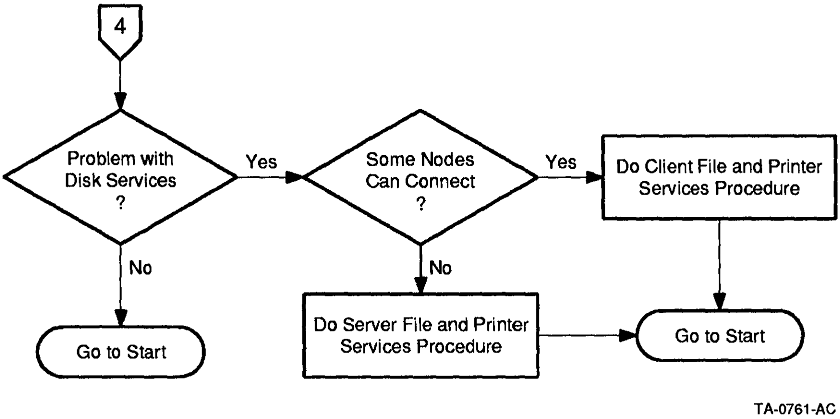


Figure 8–5 Printing Problems (LAT Flowchart 5)


4
Problem with Disk Services ?
Yes
No
Some Nodes Can Connect ?
Yes
No
Do Client File and Printer Services Procedure
Do Server File and Printer Services Procedure
Go to Start
Go to Start
TA-0761-AC

Troubleshooting Notes

Keep the following in mind as you begin troubleshooting network problems:

- Using privileged accounts

  Many of the troubleshooting procedures require the use of an account with system privileges. It is assumed that you have system management privileges for all nodes in the network.

- Troubleshooting LAT problems can require you to make changes to the LAT configuration.

- You should have a diagram showing the network topology. For each node on the network, you should have the following information:

  - The node name
  - The Ethernet address
  - The services offered
  - The queues, ports, and applications associated with the services
  - The services used (including preferred services)
  - The group code assignments

Having this information with you during the troubleshooting process assists in isolating and correcting network problems.

VMS Server Master Procedure (LAT)

The VMS Server Master Procedure (LAT) is a set of procedures that are used to verify the operational state of LAT on a VMS server. The VMS Server Master Procedure (LAT) has the following subprocedures:

- The VMS Server Transport Procedure
- The VMS Server LAT Services Procedure
- The VMS Server LAT Services Procedure
- The VMS Server Maximum Connections Procedure

Use these procedures to verify that your VMS server is operational. If you cannot successfully perform the VMS Server Transport Procedure, you will be required to perform hardware diagnostics procedures. These procedures are located in Isolating DECnet Problems in this manual.

VMS Server Transport Procedure

This procedure verifies that the LAT driver is operating correctly on a VMS server.

1. Log in to the system manager's account.
2. Verify the version number of the VMS operating system that is running on your server by entering:

```
$  SHOW SYSTEM
VAX/VMS V5.3  on node VVSRV  18-DEC-1990 00:02:08.24   Uptime  0 00:34:40
  Pid    Process Name     State  Pri      I/O       CPU       Page flts Ph.Mem
00000021 SWAPPER          HIB     16        0   0 00:00:01.65         0      0
00000044  LTA5:           CUR      7      243   0 00:00:04.88       790    246
00000026 ERRFMT           HIB      8       55   0 00:00:00.61        81    115
00000027 OPCOM            HIB      8       74   0 00:00:01.17       241    109
00000028 AUDIT_SERVER     HIB     10       27   0 00:00:01.57      1315    165
00000029 JOB_CONTROL      HIB      8      399   0 00:00:02.91       208    287
0000002A CONFIGURE        HIB      8        8   0 00:00:00.32        89    135
0000002B SYMBIONT_0001    HIB      6       30   0 00:00:01.00       239    182
0000002D NETBIOS          HIB      9       31   0 00:00:00.52       150    185
0000002E NETACP           HIB     10       41   0 00:00:01.49       292    322
0000002F REMACP           HIB      8       12   0 00:00:00.16        64     32
00000032 PCFS_SERVER      HIB     10     1227   0 00:00:23.44      1080   2199
00000033 LAD$KERNEL       HIB      9      108   0 00:00:01.79       182    253
0000003C SYSTEM           LEF      7      955   0 00:00:19.88      2982    174
```

   The first line of the response contains the version number of the VMS operating system that is running on your server. If the version number is less than 5.3, you must upgrade your VMS operating system.

3. Ensure that the LAT driver is running by entering:

```
$  RUN SYS$SYSTEM:LATCP
LCP>  SHOW CHARACTERISTICS

LCP Characteristics

Node name = \VVSRV\
Node Identification = \Welcome to VAX/VMS V5.3\
Groups = (0)  ❶
Multicast timer = 60 seconds
LAT Version = 5.1               LAT Protocol is active  ❷


Service Names and Ids:

Service name : \VVSRV\                    Dynamic rating : 81
          ID : \Welcome to VAX/VMS V5.3\


Node Links:

Link name = \LAT$LINK\
Link device = \XQA0:\
Groups = ()
Link-specific services:
Status = Active
LCP>
```

When reviewing the response, verify that the LAT protocol is active ❷. If the LAT protocol is inactive, you must restart the LAT driver with the command file SYS$SYSTEM:LTLOAD.COM.

When reviewing the response, verify that the correct group codes ❶ are enabled.

4. If the rating is not a dynamic rating, go to step 5.

   Ensure that the service is operating correctly by verifying that the rating is a nonzero value.

5. To confirm that the VMS server is able to send and receive LAT messages, enter:

```
LCP>  SHOW COUNTERS

LCP Node Counters

       566             Receive frames
         0             Receive errors
         0             Receive duplicates
    191549             Transmit frames
         3             Transmit errors
  00000334             Last transmit failure code
         0             Retransmissions
         4             Circuit timeouts
         0             Protocol errors
  00000000             Protocol bit mask
         0             Resource errors
         0             No transmit buffer
         0             Unit timeouts
         0             Solicitation failures
         0             Discarded output bytes
LCP>
```

   If the transmit frame count is nonzero and the transmit error count has the same or almost the same value as the transmit frame counter, it is likely that there is a network hardware problem.

   If the transmit frame count is nonzero and the receive frame count is zero, either no client has solicited for a service or no client can communicate on LAT.

6. Verify the activity on a VMS server node by setting the counters to zero and checking their values periodically.

```
LCP>  SET COUNTERS/ZERO
LCP>  SHOW COUNTERS

LCP Node Counters
```

```
            29              Receive frames
             0              Receive errors
             0              Receive duplicates
            31              Transmit frames
             0              Transmit errors
      00000000              Last transmit failure code
             0              Retransmissions
             0              Circuit timeouts
             0              Protocol errors
      00000000              Protocol bit mask
             0              Resource errors
             0              No transmit buffer
             0              Unit timeouts
             0              Solicitation failures
             0              Discarded output bytes
```

VMS Server Transport Procedure Completion

Successfully completing this procedure indicates that LAT is operational on the VMS server.

VMS Server LAT Service Procedure

This procedure verifies that LAT services are operating correctly on a VMS server.

1. Check the characteristics of LAT nodes that are known to a VMS server by entering:

   ```
   LCP>  SHOW SERVERS
   ```

   The following response indicates that no client nodes are known to the VMS server. If you receive this response, no client is communicating with the VMS server over LAT.

   ```
   %LAT-I-NOSERVERS, no known servers
   LCP>
   ```

   The following response indicates that a client has established a session with the VMS server.

   ```
   LCP Server Characteristics for LAT_AA0004000BF8

   Ethernet address = AA-00-04-00-0B-F8
   Server is active               Active users = 1
   Link name = LAT$LINK
   ```

2. Check the characteristics of LAT ports on a VMS server by entering:

   ```
   LCP>  SHOW PORTS
   ```

   The following response indicates that no client has logged on to the VMS server over LAT.

   ```
   %LAT-I-NOTERMS, no such terminal(s)
   LCP>
   ```

   The following response indicates that a client has established a session with the VMS server.

   ```
   Local Port Name = LTA4:   <interactive>

      Specified Remote Service Name = VVSRV
      Actual Remote Node Name = LAT_AA0004000BF8
      Link Name = LAT$LINK
   ```

VMS Server LAT Service Procedure Completion

Successfully completing this procedure indicates that a client is communicating with the VMS server over LAT.

VMS Server Maximum Links/Connections Procedure

This procedure verifies that the VMS server has sufficient resources for correct operation.

1. Use the LATCP SHOW COUNTERS command and verify that the resource error counter is 0.
2. Verify that the value for the transmit error counter is not above normal for your network.
3. Use the NCP SHOW LINE COUNTERS command and verify that the system buffer unavailable counter is in the normal range.
4. If necessary, reconfigure your server until these values are in acceptable limits.

VMS Server Maximum Connections Procedure Completion (LAT)

The VMS Server Maximum Connections Procedure is complete. Successfully completing this procedure indicates that the service connections are within the maximum limit on the VMS server.

VMS Server Remote Printer Services Procedure (LAT)

This procedure verifies that a VMS server printer service or a terminal server printer service is operating correctly on a VMS server.

Check the state of the queue on the VMS host system, and resolve any problems based on the print queue state. Ensure that parameters on the terminal server, VMS host system, and printer match appropriately, as follows:

- The server name on the terminal server matches the server name on the LTA device on the VMS host system.
- The port name on the terminal server matches the port name on the LAT device on the VMS host system.
- No duplicate server names exist.
- Printer characteristics on the printer match the printer characteristics on the terminal server port.

Note

To correct the LAT print queue problem, you can use TSM or NCP to enter commands on the terminal server, or you can go directly to the terminal server and enter the commands.

Whether you use TSM or NCP, or enter the commands directly on the server, the procedure is the same; only the prompts are different. The following shows how to log in to the terminal server using either TSM or NCP.

1. To use TSM to log in to the server, run TSM and use the following command:

```
TSM>  USE SERVER server-id
```

2. To use NCP to log in to the server, the server must be defined in the NCP database. If the server is defined in the NCP database, run NCP and use the following command to log in to the server:

```
NCP>  CONNECT NODE server-id
```

If the server is not defined, use the following NCP command:

```
NCP>  CONNECT VIA service-circuit PHYSICAL ADDRESS-
 _NCP>  ethernet-physical-address
Console connected press Cntrl D when finished.
<carriage return>
# <login password>
```

When you enter the following server commands, the system displays the Local> prompt rather than the TSM> prompt. To return to NCP from the Local> prompt, press Ctrl/D.

3. To enter commands directly on the server, go to the server and log in using your user name.

   ```
   Enter username> username
   ```

   When you enter the following server commands, the system displays the Local> prompt rather than the TSM> prompt.

   Note

   From this point on, the terminal server commands are the same regardless of how you access the server. However, the following procedures assume you use TSM to access the server.

Before you begin to solve this problem, do the following:

- Enable the display of all LAT error messages on your terminal using the following command:

  ```
  $ SET MESSAGE SYS$MESSAGE:NETWRKMSG
  ```

  To enable the display of LAT error messages for all users, put the SET MESSAGE command in the SYS$MANAGER:SYLOGIN.COM file.

- Determine the state of the queue on the VMS host system using the following command:

  ```
  $ SHOW QUEUE queue_name/FULL
  ```

Table 8–2 shows the queue states and conditions, their meanings, and the troubleshooting steps that solve the problem.

Table 8–2 Print Queue States and Conditions

State	Meaning	Solution
Stopped	Print queue has been stopped using the STOP/QUEUE/RESET command, or the queue manager has been stopped, or some other problem has occurred such as termination of the symbiont process.	Step A
Stalled	Printer is unable to complete the request due to a flow control problem, such as lack of paper.	Step B
Paused	Print queue has experienced an error or unexpected event when communicating with the server.	Step C
Printing Incorrectly	Printer is generating incorrect output.	Step D
Retained on Error	A job experienced an error during execution but remains in the queue.	Step E

A. **For a stopped queue, start the queue on the VMS host system using the following DCL command:**

```
$  START/QUEUE queue-name
```

A stopped queue usually indicates a problem on the VMS host system.

1. Check SYS$SYSTEM for LATSYM.DMP files.
2. If LATSYM.DMP files exist, check the OPERATOR.LOG file for jbc errors that explain why the files exist.

   For further help with LATSYM problems, call your local Digital service representative.

B. **For a stalled queue, do the following:**

1. Use the following TSM command to get information about the printer:

```
TSM>  USE SERVER server-name
TSM>  SHOW PORT port-id STATUS
```

a. If the Status field indicates your node is not connected to the terminal server, check the queue on the terminal server, using the following commands:

```
TSM>  USE SERVER server-name
TSM>  SHOW QUEUE
```

If the display shows entries in the queue for the VMS host system, and the port is connected to another system, the server is waiting for the port to become idle.

Also, font loading in some types of printers can take time. If the printer is not printing, check to see if the printer is loading fonts before you take any other action.

b. If signal check is enabled on the port, and the port status is signal wait, check the input signals. If they show no modem signals from the printer, the server is waiting for a modem signal from the printer.

   - Make sure no problem exists on the printer (such as a broken or disconnected cable) that might prevent the printer from sending signals.
   - After you resolve any problems which might prevent the printer from sending signals, turn the printer off, then on, to clear the problem.

c. If the flow control fields (Input and Output) indicate that output state is XOFF, the server is waiting for an XON character from the printer. Either the printer sent an XON character and the server lost it, or the printer never sent an XON character.

   - Make sure the printer is functioning properly. For example, be sure it is on, has paper, and is not displaying hardware errors.
   - Turn the printer off, then on, to clear the problem.
   - As a last resort, log out the port.

2. If the printer is not printing after a reasonable amount of time, and is not loading fonts, use the following command to log out the terminal server port and clear the problem:

```
TSM> LOGOUT PORT port-number
```

C. **For a paused queue, do the following:**

1. Use the following DCL command on the VMS host system to display the LAT device identification:

```
$ SHOW QUEUE queue-name/FULL
```

2. Use the following DCL command on the VMS host system to despool the LAT device:

```
$ SET DEVICE /NOSPOOL LTAn:
```

3. Copy a printable file to the LAT device to confirm whether the LAT device is working:

```
$ COPY/LOG file_name LTAn:
```

4. If the COPY command succeeds, go to step 8.

If the COPY command does not work, you get the error, data set hangup. The "data set hangup" error indicates that the VMS host cannot find the terminal server. This problem is due to any of the following:

- Incorrect or mismatched information on the terminal server and the VMS host
- Data transmission problem on the Ethernet segment
- Port configuration problems
- Terminal server problems

5. Be sure the server name and the port name on the VMS host system are correct and match the server name and the port name on the terminal server.

   a. Do the following on the VMS host system to display the port characteristics:

   ```
   $ MCR LATCP
   LCP> SHOW PORT LTAn:
   LCP> EXIT
   ```

   b. Do the following on the terminal server to display the server and port characteristics:

   ```
   $ TSM
   TSM> SHOW SERVER
   TSM> SHOW PORT xx
   TSM> EXIT
   ```

   c. If the host system definitions are wrong, use the following LATCP command to redefine them. Ensure that the LTA port on the VMS host system is defined to be an applications port, and that the QUEUE attribute is set.

   ```
   LCP> SET PORT LTAn:/APPLICATION/NODE=servername/PORT=portname
   ```

   d. If the server characteristics on the terminal server are wrong, use the following commands to redefine them:

   ```
   TSM> SET SERVER server-id characteristics
   TSM> DEFINE SERVER server-id characteristics
   ```

Note

The SET command causes the change to take effect immediately. The DEFINE command makes the change permanent, so when you reboot the server, the new characteristics are in place.

For the DECserver 500 and DECserver 550 terminal servers do not use a DEFINE command. Instead, use the SET command to make the changes. To cause the changes to take effect permanently, modify the load image.

---

e. If the port characteristics on the terminal server are wrong, use the following command to redefine them:

```
TSM> DEFINE PORT port-id characteristics
```

f. Log the port out to cause the port changes to take effect.

```
TSM> LOGOUT PORT port-number
```

6. Check to see if data transmission problems exist on the Ethernet segment.

   a. Run TSM and use the following command to display the terminal server counters:

   ```
   TSM> SHOW SERVER COUNTERS
   ```

   b. Check the Solicitations Accepted and Solicitations Rejected fields.

   c. Try the COPY command again.

   d. Display the terminal server counters again and check the Solicitations Accepted and Solicitations Rejected fields.

      - If the Solicitations Rejected field increments, the server is operating but is not accepting solicitations, probably because the port is misconfigured. Go to step 6.

      - If neither solicitations field increments when you issue the COPY command, the terminal server did not receive the copied file. A cabling or network problem could exist. Go to step 7.

      - If the Solicitations Accepted field increments, the COPY command worked. Go to step 8.

7. If the Solicitations Rejected field increments, ensure the terminal server port is properly configured.

   a. Run TSM and use the following command to display the current characteristics for the server port:

```
TSM> SHOW PORT
```

The terminal server port for the print queue must have the following characteristics defined:

- Unique name
- Access remote
- Autobaud disabled
- If group codes are enabled, the port's group code must match the VMS host group code definitions

b. If the terminal server characteristics are not correct, use the following TSM command to specify the correct characteristics, as required:

```
TSM> DEFINE PORT characteristics
```

c. Log the port out to cause the changes to take effect.

```
TSM> LOGOUT PORT port-number
```

d. Check the printer to ensure the printer's hardware is functional. For example, ensure the printer is connected, is on, has paper and so forth. Continue with step 9.

8. If neither the Solicitations Accepted nor the Solicitations Rejected field increments, check to see if cabling problems exist between the terminal server and the VMS host, or if a network problem exists.

   a. Use the following command to see if the terminal server knows about the VMS host system:

   ```
   TSM> SHOW NODE node-id
   ```

   b. If the terminal server displays the VMS host system, the COPY command should work.

   c. If the terminal server does not display the VMS host system, ensure that the terminal server cabling is intact and properly connected, and that the VMS host system cabling is properly connected to the Ethernet.

   d. Use NMCC/VAX ETHERnim to verify the path to the terminal server and the VMS host system.

   Use LAN Traffic Monitor data to see if a LAN segment problem or babbling device problem exists on the network.

   Use NCP loopback commands or NMCC/VAX ETHERnim to isolate network problems.

e. Try to reboot the terminal server to clear the problem.

Note

Rebooting the terminal server disconnects all connections to the terminal server. Use this step only as a last resort.

9. If the Solicitations Accepted field increments, and the COPY command succeeds, but still cannot print using the print queue, the queue could be using the wrong queue processor.

   Use the following DCL command to initialize the queue and define the correct queue processor:

   ```
   $ INITIALIZE QUEUE queue_name/PROCESSOR=LATSYM
   ```

10. Confirm that the port is working properly using the following command:

    ```
    TSM> TEST PORT
    ```

    The TEST PORT command allows the terminal server to communicate directly with the printer without VMS. It helps that confirm the connection between the terminal server and the printer is working.

    - If the test pattern prints correctly, the port is operating properly.
    - If the test pattern does not print correctly, check the connection between the terminal server and the printer. Also confirm that the characteristics of the terminal server and printer match, and the printer is operating properly, as shown in step 6a.

D. **For a queue that is printing incorrectly, do the following:**

Ensure the following parameters are the same on *both* the printer and the terminal server port:

- Port speed
- Flow control
- Character size
- Parity
- Baud rate

Autobaud is disabled on the terminal port

1. Use the following command to check the terminal server port:

   ```
   TSM> SHOW PORT port-id CHARACTERISTICS
   ```

2. If you need to change the terminal server characteristics, use the following command:

   ```
   TSM> DEFINE PORT port-id characteristics
   ```

3. Log the port out to cause the changes to take effect.

   ```
   TSM> LOGOUT PORT port-number
   ```

4. For instructions on setting printer characteristics, see the printer hardware documentation.

E. **For a queue displaying the "retained on error" message, do the following:**

1. Use the following command to display any additional messages:

   ```
   $ SHOW QUEUE queue_name/FULL
   ```

   Usually, the "retained on error" message results in a stalled or paused queue. Jobs that abort and are retained on error are usually the result of one of the following:

   - The port is logged out in the middle of a job
   - LAT shuts down on the VMS host system
   - The Ethernet device fails while transmitting
   - The job was deleted using the DELETE/ENTRY=nnn command

2. If the queue is stalled or paused, use the steps for solving stalled or paused queues.

3. After solving the stalled or paused problem, use the following DCL command to clear the queue of the job retained:

```
$ SET ENTRY/RELEASE job_entry_number
```

VMS Server Remote Printer Services Procedure Completion (LAT)

The VMS Server Remote Printer Services Procedure is complete. Successfully completing this procedure indicates that the remote printing services are operational on the VMS server.

VMS Server Master Procedure Completion (LAT)

The VMS Server Master Procedure (LAT) is complete.

ULTRIX Server Master Procedure

The LAT Control Program (**lcp**) executes the command you specify and returns to the default prompt in multiuser mode. Most of the procedures shown in this section consist of commands contained in your /etc/rc.local file where they run automatically when you boot your system.

1. The command option [-d] displays the characteristics of the LAT services on your system. Use the following command to confirm that the ULTRIX LAT server is running:

   ```
   #  /ect/lcp -d

   Node name/identification: ALARMS / ULTRIX
   Service name/identification: ALARMS / ULTRIX LAT SERVICE
   Groups:  40  44
   Multicast timer:  30 seconds
   LAT version: 5  eco: 1    LAT Protocol is active

   #
   ```

2. If an error message is displayed, start the LAT by entering the following command:

   ```
   #  /ect/lcp -s
   ```

   Note

   If the LAT does not start automatically on your system when it boots, add this line to your /etc/rc.local file.

3. To display the group code definitions on an ULTRIX system, enter the following command:

   ```
   # lcp -d
   ```

4. Compare the group code definitions displayed in **lcp** to those in the rc.local file. The definitions should be the same.
5. Compare the group code definitions on the ULTRIX system to those displayed on the client nodes that use the server.
   - If the group codes match on the ULTRIX server and on the client nodes which use the server, proceed to the Client Operation Verification Procedure.
   - If the group codes defined on the ULTRIX server are different from the group codes on the client nodes which use the server, change the group codes as needed on the appropriate node.

6. To change the group codes on the ULTRIX server, enter the commands shown, substituting the appropriate group numbers for group n:

```
# lcp -d
# lcp -g group_n, group_nn, group_nnn...
```

- Edit the /etc/rc.local file to reflect the same group codes you just specified or deleted in lcp.
- Ensure the configuration file contains the following lines:

  ```
  options         LAT
  pseudo-device   lat
  pseudo-device   lta n
  ```

  For non-RISC systems, the configuration file is /sys/conf/*hostname*. For RISC systems, the configuration file is /sys/conf/mips/*hostname*.

  For *lta n*, specify the number of terminals, using a multiple of 16.
- Check the \dev file to ensure the LAT devices are listed as LAT terminals.

ULTRIX Server Master Procedure Completion (LAT)

The ULTRIX Server Master Procedure is complete. Successfully completing this procedure indicates that the ULTRIX server on your network is set up correctly.

DOS Client Master Procedure (LAT)

The DOS Client Master Procedure (LAT) contains the following procedures:

- DOS Client Configuration Procedure
- DOS Client Transport Procedure
- DOS Client Maximum Connections Procedure
- DOS Client Printer Services Procedure

Use these procedures to verify that your DOS client is operational. To perform these tests, boot the DOS client with the key diskette. Then perform the indicated test.

If you cannot successfully perform the DOS Client Transport Procedure (LAT), you will be required to confirm that no server or client network hardware problems exist. The procedures used to isolate network hardware problems are located in Isolating DECnet Problems in this manual. When performing those procedures, load the network components into conventional memory. Doing so minimizes the opportunity for one problem to hide another problem.

DOS Client Configuration Procedure

This procedure verifies the proper information needed in your system files to start and use LAT protocol on your system. It verifies the contents of the following system files:

- CONFIG.SYS
- AUTOEXEC.BAT
- STARTNET.BAT

NOTE

> Any PATHWORKS Terminate and Stay Resident (TSR) software must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

To ensure that the network drivers required to load LAT are included, verify the contents of your CONFIG.SYS, AUTOEXEC.BAT, and STARTUP.BAT files as follows:

1. Verify that the contents of your CONFIG.SYS file to ensure the network card driver needed by the LAT protocol is loaded.

   ```
   files=40
   buffers=25
   device= c:\cache.exe 256 on /ext
   shell=\command.com /P /e:526
   device=\DECnet\PROTMAN.SYS /I:C:\DECNET
   device=\decnet\DEPCA.DOS
   ```

2. Verify the contents of your AUTOEXEC.BAT file to ensure that it includes the network startup files that start LAT.

   ```
   prompt $p$g
   path c:\;C:\DOS;c:\windows;C:\WINWORD;c:\mswinv30;c:\decnet\doc;
   REM Executing network startup procedure
   if not exist \DECNET\STARTNET.BAT Goto nostartup
   call \DECNET\STARTNET
   Goto end
   :nostartup
   echo ** WARNING ** STARTNET.BAT file not found. Network functions not performed
   :end
   ```

3. Verify that the command required to start LAT is in your STARTNET.BAT file.

   ```
   %_SYSD%\DECNET\LAT
   ```

DOS Client Configuration Procedure Completion (LAT)

The DOS Client Configuration Procedure is complete. Successfully completing this procedure indicates that LAT is configured correctly on the DOS client.

DOS Client Transport Procedure (LAT)

This procedure verifies the correct operation of the LAT transport on a DOS client.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Ensure the LAT driver is running by entering:

   ```
   C:\DECNET> LATCP
   LATCP 4.0.x

   LATCP> SHOW COUNTERS

   LAT counters as of 19-Jan-1991 23:59:18

   Seconds since last zeroed              = 5483
   Messages transmitted                   = 4455
   Messages received                      = 5092
   Messages retransmitted                 = 0
   Messages received out of sequence      = 3
   Illegal messages received              = 0
   Illegal slots received                 = 0
   Queue entry unavailable for receive    = 0
   Transmit buffers unavailable           = 0
   Invalid messages received              = 1
   Invalid slots received                 = 0
   Invalid multicast messages             = 0
   Invalid acknowledgements               = 0
   Solicit information messages received  = 0
   Solicit information messages sent      = 0
   Response information messages received = 0
   Response information messages sent     = 0
   Connection solicitations received      = 0
   Connection solicitations accepted      = 0
   DLL buffers owned                      = 3
   DLL buffers freed                      = 3
   Session transmit queue already full    = 0
   ```

   If the response is "LAT is not installed" the LAT driver is not running. To start the LAT driver, enter:

   ```
   C:\DECNET> LAT
   ```

2. Ensure a service is correctly defined in the LAT database by entering:

```
LATCP> SHOW SERVICES
Known LAT services as of 2-Oct-1990 9:05:22
3 services offered by 3 nodes

Service Name        Rating          Ethernet Address   Status

A                   42              AA-00-04-00-04-24  Available
B                   59              AA-00-04-00-07-24  Available
C                   94              AA-00-04-00-48-25  Available
```

   To automatically update the LAT service database you *must* enable multicasts using the LAT Control Program.

   You can define server nodes as preferred services by using LATCP to add a service. When you exit LATCP, this information is saved in a database file called DECLAT.DAT. At startup, the preferred services are immediately entered in the LAT service table.

   Note

   When upgrading from Version 3.x to Version 4.0, you must reconfigure LAT preferred services. The file DECNODE.DAT used in Version 3.x is no longer used to identify preferred services. For Version 4.0, this information is contained in the file DECLAT.DAT. Any information contained in the Version 3.x DECLAT.DAT file is ignored by the Version 4.0 software. Any preferred services configured under Version 3.x must be reconfigured for Version 4.0.

3. Verify the network services known by your node, and verify that they are active by checking for a service rating greater than zero.

   If the name of the server you want to connect to is not listed, you must add the server name and node to the LAT database by entering:

```
LATCP> ADD node_address node_name service_name
```

   node_address — The Ethernet address of the LAT server (for example, AA-00-04-00-1D-F8, or 9.123)

   node_name — For the node name of the LAT server (for example, SERVER1)

   service_name — The name of the preferred service you are adding (for example, POSTSCRIPT, or SERVER1)

For example:

```
LATCP> ADD AA-00-04-00-1D-F8 SERVER1 POSTSCRIPT
```

or

```
LATCP> ADD 9.123 SERVER1 SERVER1
```

4. Verify the circuit used to provide a service to your node by entering:

```
LATCP> SHOW CIRCUIT

LAT virtual circuits as of 20-Jan-1991 14:40:48

Node               Ethernet             Circuit   Circuit  Number of
Name               Address              State     Id       Sessions
-----------------------------------------------------------------
SERVER1            AA-00-04-00-1D-F8    Running   258      1
```

Run the program SETHOST to connect to the LAT service just added to ensure the node has been added to the LAT service table.

Note

The SETHOST command dynamically loads and unloads the LAT module. You do not have to load LAT explicitly, except to perform the tests described here, or to load the printer.

5. Use the LATCP SHOW CHARACTERISTICS command to verify the number of active sessions on your node. For example:

```
LATCP> SHOW CHARACTERISTICS

LAT characteristics as of 2-Oct-1990 8:55:17
```

```
Server name                                       = LAT_AA0004000BF8
Protocol version                                  = 5
Protocol ECO                                      = 1
Maximum number of circuits                        = 4
Number of circuits                                = 0
Maximum number of sessions                        = 32
Number of sessions                                = 0
Multicast                                         = Enabled
Fallback                                          = Disabled
Search                                            = Disabled
Port services                                     = 0
Service table size                                = 25
Number of services                                = 13
Number of nodes                                   = 12
Unused entries in service table                   = 0
Number of application SCBs                        = 3
Number of application SCBs in use                 = 0
Number of slot buffers in a application SCB       = 6
Maximum slot size when sending                    = 127 bytes
Group codes                                       = 0 - 255
Number of ticks per second                        = 18
Retransmit timer                                  = 6 ticks
Retransmit limit                                  = 99
Multicast timer                                   = 540 ticks
Keepalive timer                                   = 360 ticks
Cmd retry timer                                   = 4 ticks
Cmd retry limit                                   = 4
Response timer                                    = 36 ticks
LPT throttle                                     = 255 bytes
```

6. Perform steps a through c for problems using LAT with Microsoft Windows.

   a. If LAT is still not working, ensure LAT has at least one Session Control Block (SCB) allocated for each LAT session you plan to use.

   b. Verify that at least one less application SCB is in use than the number of application SCBs defined for your node.

Note

The VT320 and SETHOST programs use one SCB for each host session established. In the example shown above, LAT has three SCBs defined.

   c. If necessary, increase the number of application SCBs.

   You can increase or decrease the number of SCBs allocated to LAT by using the DEFINE SCB command.

   The SCB value in the SHOW CHARACTERISTICS example above was set using the following command in LATCP:

   ```
   LATCP> DEFINE SCB 3
   ```

   This value ensures you can run three simultaneous LAT sessions.

7. Verify that the number of sessions is less than the maximum number of sessions.

8. Verify that the number of circuits is less than the maximum number of circuits.

9. If necessary, increase the number of circuits.

   Note

   This step is required only if you are trying to connect to more than four nodes.

   You can increase or decrease the number of virtual circuits supported on your node by using the DEFINE MAXIMUM CIRCUITS command.

   Set the maximum number of circuits to match the example by using the following command in LATCP:

   ```
   LATCP> DEFINE MAX CIRCUITS 6
   ```

   This value ensures you can run six simultaneous virtual circuits. You need at least one virtual circuit available for each LAT session you are using.

10. If you offer a LAT printer service on your node, verify that the number of local services shown is equal to the number of printer services you are offering on your node.

11. If any changes are made to your LAT parameters, you must exit LATCP and restart the LAT for the changes to take effect. After restarting the LAT, use the LATCP SHOW command to verify that changes took place when the LAT was reloaded.

12. If you still have problems, verify your system configuration by using the DOS Client Configuration Procedure. If necessary, reconfigure your system and retry these procedures until the system and the LAT configuration are correct.

You should be able to log in to a LAT service with SETHOST to verify any services you add. Use LATCP to verify that your other changes took place.

DOS Client Transport Procedure Completion (LAT)

The DOS Client Transport Procedure is complete. Successfully completing this procedure indicates that the local area system transport is set up correctly on the DOS client.

DOS Client Printer Services Procedure (LAT)

This section contains the procedure for troubleshooting printer services offered by DOS clients.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

Note

If you have configured a LAT printer service on your DOS node, it is initialized when LAT is loaded on your PC. When a printer is initialized by LAT, it is "hidden" from DOS and cannot be used as a normal DOS printer without first unloading LAT.

1. Verify that the service exists on the DOS server by using the SHOW PORTS command.

```
LATCP>  SHOW PORTS

LAT ports as of 19-Jan-1991 23:58:32

Service            Service            Service   Queue
Name               Password           Rating    Depth    LPT#
---------------------------------------------------------------
A                                     26        0        1
B                                     0         0        2
```

   You should see an entry for each printer configured on your DOS server.

2. If no services are shown, add the printer service to your LAT configuration.

   a. You can do this by entering the following command in LATCP:

   ```
   LATCP> ADD LPTn service_name [/rating=n] [/password=string]
   ```

   or

   ```
   LATCP> ADD LPTn service_name [/rating=n] [/nopassword]
   ```

Note

If you are using a password to access the printer service, it will be displayed.

b. Exit LATCP and restart LAT. You can do this by typing:

```
C:> LAT
```

3. If the appropriate number of local printer services are displayed and you are still having problems printing, for each printer, ensure that:

   - The printer is connected and powered on.
   - The printer is connected to the proper LPT port.
   - The printer has an adequate supply of paper.
   - The paper is not jammed and passes through the printer correctly.
   - The printer is on line.

4. If you are still unable to print, unload LAT and see if the printer will print directly from DOS. You can do this by entering the following:

   ```
   C:>  LAT  /u
   LAT unloaded
   ```

5. Print a text file from the DOS command processor using the DOS COPY command. The following example shows the commands to copy your AUTOEXEC.BAT file to the printer port.

   ```
   C:> COPY AUTOEXEC.BAT LPT[n]:
   ```

   If the file does not print from DOS with LAT unloaded, ensure that:

   - The printer is connected and powered on.
   - The printer is connected to the proper LPT port.
   - The printer is on line.

   If you have verified all of the steps above and the printer still will not print, call field service.

   If the file prints correctly directly from DOS, the problem must be related to the LAT configuration on your PC.

6. Use the following procedure to ensure that your LAT configuration is correct.

   a. Use the LATCP command SHOW PORTS to determine whether the node offers a printer service. If the node does not offer a printer service, go to step 7.

   b. Use the LATCP SHOW CHARACTERISTICS to verify the information listed for active sessions on your node.

```
LATCP> SHOW CHARACTERISTICS

LAT characteristics as of 2-Oct-1990 8:55:17

Server name                                  = LAT_AA0004000BF8
Protocol version                             = 5
Protocol ECO                                 = 1
Maximum number of circuits                   = 4
Number of circuits                           = 0  ❶
Maximum number of sessions                   = 32
Number of sessions                           = 0  ❷
Multicast                                    = Enabled
Fallback                                     = Disabled
Search                                       = Disabled
Local services                               = 0  ❸
Service table size                           = 25
Number of services                           = 13
Number of nodes                              = 12
Unused entries in service table              = 12
Number of application SCBs                   = 1
Number of application SCBs in use            = 1
Number of slot buffers in a application SCB  = 6
Maximum slot size when sending               = 127 bytes
Group codes                                  = 0 - 255 (all groups enabled)
Number of ticks per second                   = 32
Retransmit timer                             = 6 ticks
Retransmit limit                             = 24
Multicast timer                              = 960 ticks
Keepalive timer                              = 640 ticks
Cmd retry timer                              = 4 ticks
Cmd retry limit                              = 4
Response timer                               = 64 ticks
LPT throttle                                 = 255 bytes ❹
```

c. Check the number of circuits in use on your node and ensure that the number is less than the maximum number of circuits available. Check the value displayed in ❶.

d. Check the number of sessions in use on your node and ensure that the number is less than the maximum number of sessions available. Check the value displayed in ❷.

e. Check the number of local services in use on your node and ensure that the number is less than the maximum number of circuits and sessions available. Check the value displayed in ❸.

f. Check the value displayed in ❹ if you experience printer problems.

   - If your printer appears to stall when printing, set this to a lower value.
   - If your printer is printing more slowly than normal, set this to a higher value.

7. Make the appropriate changes to modify the configuration so it passes the tests listed above.

8. Reload LAT and ensure that the printer resets when LAT is loaded.

DOS Client Printer Services Procedure Completion (LAT)

The DOS Client Printer Services Procedure is complete. Successfully completing this procedure indicates that the printer service is set up correctly on the DOS client.

DOS Client Maximum Links/Connections Procedure

This procedure ensures that the LAT node has not exhausted the resources (connections or sessions) specified for the node when it was configured.

> **NOTE**
>
> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

Use this procedure to ensure that sufficient resources are available on the DOS client that is offering a printer service.

1. Check the number of circuits in use on your node and ensure that it is less than the maximum number of circuits available.
2. Check the number of sessions in use on your node and ensure that it is less than the maximum number of sessions available.
3. Check the number of local services in use on your node and ensure that it is less than the maximum number of circuits and sessions available.
4. If you experience a problem accessing services on the DOS LAT server, use the SHOW SESSIONS command in LATCP to ensure that the service is not being used by another user.

DOS Client Maximum Links/Connections Procedure Completion (LAT)

The DOS Client Maximum Connections Procedure is complete. Successfully completing this procedure indicates that the service connections are within the maximum limit on the DOS client.

DOS Client Master Procedure Completion (LAT)

The DOS Client Master Procedure (LAT) is complete.

OS/2 Client Master Procedure (LAT)

The OS/2 Client Master Procedure (LAT) contains the following procedures:

- OS/2 Client Configuration Procedure
- OS/2 Client Transport Procedure

Use these procedures to verify that your OS/2 client is operational.

OS/2 Client Configuration Procedure

This procedure verifies that your OS/2 system is properly configured and that your system contains the files it needs to use the LAT protocol.

The procedures verify the following system files:

- CONFIG.SYS
- STARTUP.CMD
- PCSAOS2.CMD

Introduction to OS/2 Configuration Files

When troubleshooting OS/2 systems, it is important to know whether your client is set up with DUALBOOT software. DUALBOOT allows a client to boot using OS/2 or DOS. Understanding the dualboot utility is important because you can experience network problems that are the result of using inappropriate system files. The following brief description of DUALBOOT provides some insight into potential problems with client configurations when you use DUALBOOT.

DUALBOOT works by automatically renaming files and by pointing the system to the appropriate load modules which start the selected operating system (DOS or OS/2). Renaming files is necessary since both operating systems use CONFIG.SYS and AUTOEXEC.BAT files, but the two files are very different.

DOS can normally boot without a CONFIG.SYS file, but OS/2 requires the file. In addition, if the DOS session is enabled, duplicate COMMAND.COM and AUTOEXEC.BAT files must be avoided when renaming files. To minimize this possibility, be aware of the file sizes you use in your DOS and OS/2 environments. The following table shows the file names that exist after DOS and OS/2 are booted.

After OS/2 Boots:	After DOS Boots:
CONFIG.DOS	CONFIG.SYS
CONFIG.SYS	CONFIG.OS2
COMMAND.DOS	COMMAND.COM
COMMAND.COM	COMMAND.OS2
AUTOEXEC.BAT	AUTOEXEC.OS2
AUTOEXEC.DOS	AUTOEXEC.BAT

Caution

If you use DUALBOOT:

1. Do *not* change either the names or extensions of files with the extension .SYS, .OS2, or .DOS.
2. While booting, do *not* interrupt or reset the PC by:
   - Simultaneously pressing the Ctrl, Alt, and Del keys.
   - Pressing the Reset button.
   - Turning the power off.

If file extensions are either incorrectly or partially renamed, the system will not start. You then have to boot from a diskette and manually rename the files.

The following table lists files required for OS/2.

File	Type	Purpose
CONFIG.SYS	ASCII	The primary startup for the Presentation Manager. Sets up the OS/2 environment variables and installs drivers.
OS2SYS.INI	Binary	Initialization file. Contains Print Spooler information.
OS2.INI	Binary	Initialization file. Contains program names, group names, and additional information used by the Presentation Manager.
STARTUP.CMD	ASCII	Optional batch file (required for PCSA for OS/2). Starts the first CMD (command interpreter) session.

Sample Configuration Files for OS/2

Verify the contents of your CONFIG.SYS, STARTUP.CMD, and PCSAOS2.CMD files to ensure that the network drivers required to load LAT are included. The following are examples of the commands required to start the network drivers and LAT.

Sample OS/2 CONFIG.SYS File

```
PROTSHELL=C:\OS2\PMSHELL.EXE C:\OS2\OS2.INI C:\OS2\OS2SYS.INI C:\OS2\CMD.EXE
SET COMSPEC=C:\OS2\CMD.EXE
LIBPATH=C:\PCSAOS2\DLL;C:\LANMAN\NETLIB;C:\OS2\DLL;C:\;
SET
PATH=C:\PCSAOS2\PBIN;C:\LANMAN\NETPROG;C:\OS2;C:\OS2\SYSTEM;C:\OS2\INSTALL;C:\
;
SET
DPATH=C:\PCSAOS2\DECNET;C:\PCSAOS2\PBIN;C:\LANMAN\NETLIB;C:\PCSAOS2\CS
;C:\OS2;C:\OS2\SYSTEM;C:\OS2\INSTALL;C:\;
SET PROMPT=$i[$p]
SET HELP=C:\OS2\HELP
BUFFERS=30
DISKCACHE=64
MAXWAIT=3
MEMMAN=SWAP,MOVE
PROTECTONLY=NO
SWAPPATH=C:\OS2\SYSTEM 512
THREADS=128
SHELL=C:\OS2\COMMAND.COM /P
BREAK=OFF
FCBS=16,8
RMSIZE=640
DEVICE=C:\OS2\DOS.SYS
COUNTRY=001,C:\OS2\SYSTEM\COUNTRY.SYS
DEVINFO=SCR,VGA,C:\OS2\VIOTBL.DCP
SET VIDEO_DEVICES=VIO_IBMVGA
SET VIO_IBMVGA=DEVICE(BVHVGA)
DEVICE=C:\OS2\POINTDD.SYS
DEVICE=C:\OS2\PDIMOU01.SYS
DEVICE=C:\OS2\MOUSE.SYS TYPE=PDIMOU$
DEVICE=C:\OS2\PMDD.SYS
DEVICE=C:\OS2\EGA.SYS
SET KEYS=ON
DEVICE=C:\OS2\COM01.SYS
IOPL=YES
REM *************** PCSA for OS/2 1.1 BL2 *****************
REM *************** Do not modify this block *****************
SET DECNET=C:\PCSAOS2\DECNET
SET DNETPATH=C:\PCSAOS2\DECNET
SET DNETMAIL=C:\PCSAOS2\MAIL
DEVICE=C:\PCSAOS2\DEV\PROTMAN.OS2 /I:C:\PCSAOS2\DEV
DEVICE=C:\PCSAOS2\DEV\DEPCA.OS2
DEVICE=C:\PCSAOS2\DEV\DLLMAC.SYS
DEVICE=C:\PCSAOS2\DEV\NETDRV.SYS
DEVICE=C:\PCSAOS2\DEV\LASTDD.SYS
DEVICE=C:\PCSAOS2\DEV\LADDRV.SYS /D:4
DEVICE=C:\LANMAN\NETPROG\RDRHELP.SYS
IFS=C:\LANMAN\NETPROG\NETWKSTA.SYS /I:C:\LANMAN
REM *************** PCSA for OS/2 1.1 BL2 *****************
```

Sample OS/2 STARTUP.CMD File

```
@echo off
call C:\PCSAOS2\PCSAOS2.CMD
```

Sample OS/2 PCSAOS2.CMD File

PCSAOS2.CMD is the main batch file involved in client startup. It contains the contents of the LAT startup files:

```
@echo off

:INSTALL
if not exist C:\PCSAOS2\INSTALL.CMD goto INITIATE
echo Installing PCSA for OS/2 1.1 BL2
call C:\PCSAOS2\INSTALL.CMD
del  C:\PCSAOS2\INSTALL.CMD

:INITIATE
echo Initiating PCSA for OS/2 1.1 BL2
detach C:\PCSAOS2\PBIN\MOP
detach C:\PCSAOS2\PBIN\DNP /NOMSG

:SETUP
if not exist C:\PCSAOS2\SETUP.CMD goto PROCESS
echo Setting up PCSA for OS/2 1.1 BL2
call C:\PCSAOS2\SETUP.CMD
del  C:\PCSAOS2\SETUP.CMD

:PROCESS
echo Starting DECnet for OS/2
detach C:\PCSAOS2\PBIN\SPAWNER
if exist C:\PCSAOS2\NVDPRO.CMD call C:\PCSAOS2\NVDPRO.CMD
echo Starting LAT for OS/2
detach C:\PCSAOS2\PBIN\LATCP /D:20
echo Starting LAD for OS/2
detach C:\PCSAOS2\PBIN\LASTCP /N=CUPPC0
if exist C:\PCSAOS2\LADPRO.CMD call C:\PCSAOS2\LADPRO.CMD
echo Starting LAN Manager 2.0 Workstation
NET START WORKSTATION
NET LOGON CUPPC0
if exist C:\LANMAN\NETPRO.CMD call C:\LANMAN\NETPRO.CMD

:VERIFY
if not exist C:\PCSAOS2\VERIFY.CMD goto COMPLETED
echo Verifying PCSA for OS/2 Installation
call C:\PCSAOS2\VERIFY.CMD
del  C:\PCSAOS2\VERIFY.CMD

:COMPLETED
echo PCSA for OS/2 1.1 Started
```

OS/2 Client Configuration Procedure Completion (LAT)

The OS/2 Client Configuration Procedure is complete. Successfully completing this procedure indicates that LAT is configured correctly on the OS/2 client.

OS/2 Client Transport Procedure (LAT)

1. Ensure the LAT driver is running by entering:

   ```
   [C:\] LATCP /SHOW
   Local Area Transport Control Program 1.01
   Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.
   VAX1
   ULTRIX2
   ```

   If the LAT driver is not running, the following screen is displayed:

   ```
   Local Area Transport Control Program 1.01
   Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.
   To install, please type:
    DETACH LATCP [/D:#] [/R:#] [/NOMULTICAST] [/GROUP]

           Where:  /D:# - Number of service table entries, default 50.
                   /R:# - Retransmit limit, default 8.
                   /NOMULTICAST- Disable reception of service announcements.
                   /GROUP:#,#  - Enable only specific groups of services.
   ```

   To start the LAT driver, enter:

   ```
   [C:\] DETACH LATCP /d:50 /r:8/multicast/group:xx,xx
   ```

   The following table lists the parameters that you can use on the LATCP command line. For example:

   ```
   DETACH LATCP /D:20
   ```

   Starting LAT with this command string enables a LAT service table with 20 entries.

Parameter	Description
/D:nn	Specifies the number of entries in the LAT service table. The table lists LAT services as announced to the network.
/B:nn	Specifies the maximum number of buffers available for LAT processes.
/S:nn	Specifies the maximum number of sessions allowed through the LAT driver.
/R:nn	Specifies the retransmit limit.
/G:n,n...	Specifies the group codes to enable within the LATCP process. The parameters passed must be separated by a comma (with no spaces).

If the LAT installation is successful, the following screen is displayed:

```
Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.
LATCP is currently running.
To shutdown or obtain information type:
        LATCP  [/SHUTDOWN] [/SHOW] [/COUNTERS] [/ZERO] [/[NO]MULTICAST]

        Where: /SHUTDOWN    - Shutdown the LAT driver.
               /SHOW        - List all known services.
               /COUNTERS    - Display LAT counters.
               /ZERO        - Display, then zero LAT counters.
               /MULTICAST   - Enable reception of service announcements, default.
               /NOMULTICAST - Disable reception of service announcements.
```

If the installation is not successful, an error message appears.

2. To verify that your node is able to receive LAT service announcements and to display the services available on the LAT network, use the LATCP /SHOW command. You can display the services known by your node by entering:

```
LATCP> /SHOW

Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.

SERVICE A
SERVICE B
SERVICE C
```

   Allow no less than two minutes for LAT to listen for service announcements troubleshooting LAT problems.

3. Verify that the services you wish to use are listed. If no services are listed, enable multicasts on your client by entering:

```
LATCP> /MULTICAST

Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.

Lat Multicast reception has been enabled.
```

4. If you want to disable multicast and use only preferred services on your client, you can disable multicast by entering:

```
LATCP> /NOMULTICAST

Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.

Lat Multicast reception has been disabled.
```

5. If you are unable to verify that LAT is working on your client by using the LATCP/SHOW command, you can determine if your client is able to send or receive LAT messages by using the LATCP /COUNTERS command. Check the LAT counters to see the number of messages sent or received by your client and the number of invalid multicast messages you have received.

Verify the LAT counters by entering:

```
LATCP> /COUNTERS

Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.

Seconds Since Zeroed                    438201
Messages Transmitted                    0
Messages Received                       0
Messages Retransmitted                  0
Out of Sequence Messages                0
Illegal Messages Received               0
Illegal Slots Received                  0
Queue Entry Unavailable                 0
Transmit Buffer Unavailable             0
Invalid Messages Received               0
Invalid Slots Received                  0
Invalid Multicast Received              908
```

In the example shown above, LAT has received no valid multicast. Check the group codes and verify that the services you want to use are active.

6. If you still have not received a service announcement, verify your LAT configuration to ensure that you are properly configured for LAT. Verify that you have the proper group codes configured.

   Reset the LAT counters after checking your configuration and cabling. Do so by entering:

```
LATCP> /ZERO

Local Area Transport Control Program 1.01
Copyright (c) 1987, 1988, 1989, 1990 by Digital Equipment Corporation.

Seconds Since Zeroed                    438201
Messages Transmitted                    0
Messages Received                       0
Messages Retransmitted                  0
Out of Sequence Messages                0
Illegal Messages Received               0
Illegal Slots Received                  0
Queue Entry Unavailable                 0
Transmit Buffer Unavailable             0
Invalid Messages Received               0
Invalid Slots Received                  0
Invalid Multicast Received              908
Counters have been zeroed.
```

7. If your system is still having problems, use the LAT Configuration Verification Procedure to verify the network files needed are properly installed on your system.

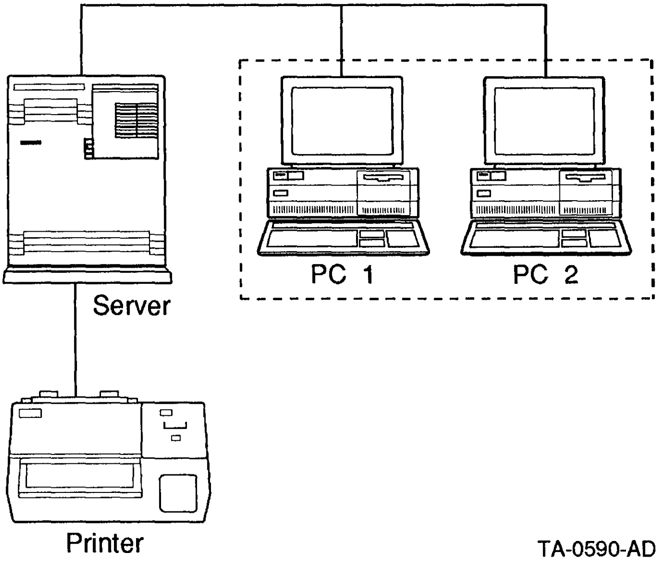
OS/2 Client Transport Procedure Completion (LAT)

The OS/2 Client Transport Procedure is complete. Successfully completing this procedure indicates that the local area system transport is set up correctly on the OS/2 client.

OS/2 Client Master Procedure Completion (LAT)

The OS/2 Client Master Procedure (LAT) is complete. If successful, you know that the OS/2 client on your network, shown in Figure 8–6, is set up correctly.

Figure 8–6 VMS Server Set Up Correctly



Network Connection Procedure

This procedure must be performed using DECnet tools. If you have not installed DECnet on the client, you should perform the appropriate Client Master Procedure for DECnet. Then perform the Network Connection Procedure for DECnet.

Network Segment Interface Procedure

This procedure must be performed using DECnet tools. If you have not installed DECnet on the client, you should perform the appropriate Client Master Procedure for DECnet. Then perform the Network Segment Interface Procedure for DECnet.

Common Network Problems Using LAT

This section describes some common problems encountered when you use LAT in your network environment. Most of the examples use DOS clients to illustrate the problem resolution procedure; however, the same approach can be used on other platforms.

The following LAT client problems are covered in this section:

- Unable to connect to LAT server (service).
- LAT cannot connect to a particular service.
- LAT connects to the wrong service.
- LAT will not load.
- LAT loses connections.
- LAT loses characters when using SETHOST or VT320.
- LAT uses too much memory.
- LAT does not work under an operating environment.

Terminal server connection failures are also covered.

LAT Client Problems

Unable to connect to LAT server node

Symptoms

```
Unable to connect to LAT Server Node
```

Explanation

This problem can be the result of several things, including hardware, software, and configuration problems. To troubleshoot this problem, follow the recommendations to isolate the cause; then perform the steps in the troubleshooting procedure.

Recommendations

Ensure that the LAT server is loaded and running.

Ensure that the LAT client software is running. Use the LATCP SHOW SERVICES command to determine if your node is getting service announcements from the server.

Verify that the appropriate network connections exist between the client and the server.

Ensure that the service and configuration information is consistent between the client and the server.

Troubleshooting Procedure

If the server and client are both running and appear to be properly configured, do the following:

1. Ensure that the client's LAT group codes match those for the service you want to access.
2. Use the LATCP command SHOW SERVICES to ensure that the service is listed in the service table. If it is not, add the service as a preferred service.
3. Ensure that multicasts are enabled on the client and that the client has received a service announcement from the server. You may want to set the server's MULTICAST_TIMER value to the minimum; doing so minimizes the time a client must wait to receive a service announcement.
4. Verify that both the server and client have valid LAT node names.

5. Verify that another node has heard the service announcement. If the service is not shown on any other nodes, the service may have been disabled or may no longer be offered.
6. Verify that there is not a physical network problem such as a wiring problem, repeater not working, or a bridge preventing packets from being forwarded.

Cannot connect to a particular LAT service

Symptoms

```
Can not connect to a particular service
The service you want to use does not appear in your LAT Service Table
```

Explanation

This problem occurs when a service is either unavailable on the LAT network or when a preferred service has not been properly configured on the client.

Recommendations

Use the LATCP command SHOW SERVICES to ensure that the service is listed in the service table. If it is not, add the service as a preferred service.

Troubleshooting Procedure

If the server and client are both running and appear to be properly configured, do the following:

1. Determine whether the service is known by any node on the LAT network. If the service is available to other nodes but not your node, ensure that the client has been properly configured and that the LAT service table is large enough.
2. Ensure that the client has the group code required to access the service.
3. Ensure that the service node is still offering the service.
4. Check the number of retransmissions that are listed under the LAT Control Program SHOW COUNTERS Command.

   If there are more retransmissions than the number configured in the retransmission limit parameter, LAT could be timing out before a service can be established. Increase the retransmission limit to a value higher than the number of retransmissions shown. If this fixes the problem, it may indicate problems with the LAN media or connections which should be investigated.

LAT connects to the wrong service

Symptoms

```
LAT connects to the wrong server node
LAT print jobs go to the wrong printer
```

Explanation

This occurs when the LAT network has multiple services with identical service names. Unless a preferred service is specified using both the node name and service name, LAT always connects to the highest rated service with that name.

Recommendations

Verify that the service node has been configured with the correct node name and address.

Ensure that the LAT configuration information is consistent between the client and server.

Verify that the appropriate network connections exist between your client and server.

Troubleshooting Procedure

If the server and client are both running and appear to be properly configured, do the following:

1. Use the LAT Control Program SHOW SERVICES command to find who is offering the service you want to connect to. If more than one service appears with the same service name, use the LAT Control Program SHOW SESSIONS/CIRCUITS command to find which node you are connected to.
2. If the service is the highest rated service shown, you need to reconfigure LAT on your PC to exclude that server node entry by using group codes or by configuring a preferred service for the node you wish to use.
3. If there is no service for that node in the service table, add it as a preferred service.
4. Ensure that the group codes match between the Service Node and your client and that the service is enabled and has a nonzero service rating.

LAT will not load

Symptoms

```
LAT will not load on your PC.
```

Explanation

This problem is typically the result of an error in the configuration or installation of network software components on your client. You may also encounter problems loading LAT if there is insufficient memory available to load the terminate and stay resident (TSR) portion of LAT. This typically occurs because of memory conflicts between TSRs, or because there is not enough memory left to load the network software after other TSR programs (network or mouse drivers, software applications, and so on).

Recommendations

Check that the LAT client software has been properly installed.

Troubleshooting Procedure

1. Verify that the network drivers have been loaded by using the MEMMAN utility to verify that they have been loaded into memory.
2. Remove all TSR programs, except for your network drivers, from your CONFIG.SYS and AUTOEXEC.BAT files. Try loading LAT without the other TSR programs in memory. Try loading only LAT without other network components to see if it can load by itself. If this works, examine your network drivers and other TSR programs to determine how to reduce the memory enough to get LAT to load.
3. Examine your system memory to determine whether the LAT driver is loaded into conventional or EMS memory. If the LAT driver is loaded into EMS, try loading it into conventional memory to see if the problem disappears. If the driver loads into conventional memory and LAT works normally, your EMS memory is either improperly configured or incompatible.
4. If the preceding steps show that you have insufficient memory to load LAT, use the default service table size.

5. If the LAT Control Program cannot add or change service information, or if your preferred services and other configuration information does not show up when you run the LAT Control Program, you have mismatched versions of LAT and the LAT Control Program. Reinstall the network software and ensure that the client is properly configured.

LAT loses connections

Symptoms

```
LAT loses connections
```

Explanation

The LAT protocol is intended to provide a reliable communications transport for character based data in LAN environments where routing functions are not required. Generally, LAT functions are intended to operate over typical conditions in IEEE 802.3/Ethernet environments. With the LAN networking technology that may exist in your network (multiport repeaters, LAN bridges, and hybrid bridge/router technology), you may encounter situations where the default LAT parameters are inappropriate. The technical complexity in your LAN topology may require you to understand and investigate the configuration parameters of the LAN components to optimize network performance. This is especially true if LAN usage is heavy on a particular LAN segment or if you have bridges and repeaters on your LAN.

Recommendations

Check that the LAT server you are connecting to is loaded and running.

Ensure that the service you are using is still enabled. The service node operator may have disabled it.

Verify that the appropriate network connections exist between your client and server. Ensure that all components existing between your client and the service node are appropriately configured. Ensure that there are no routers between the client and server nodes. Confirm that LAT multicast messages are not being filtered by LAN bridges.

Troubleshooting Procedure

1. Check VMS or ULTRIX security settings to ensure that auto logoff is not enabled or, if it is enabled, that it is not set to an inappropriately low value.
2. Check the number of retransmissions on your client by using the LAT Control Program. If this number is greater than the default, increase LAT retransmission limits on your client.

3. If the problem is seen on more than one client, or is happening with other protocols also, check and if necessary, increase the retransmission limits on the LAT server and other nodes.
4. Ensure that any hardware between your client and the server node is appropriately configured to support your LAT connection. Some network equipment filters packets based upon packet size, protocol, address, or LAN activity level. This is especially important with LAN bridges and remote LAN bridges.

LAT loses characters when using SETHOST or VT320

Symptoms

```
LAT loses characters
LAT printing becomes garbled
```

Explanation

In some situations LAT may appear to lose characters when using SETHOST or VT320 emulation. This occurs when the client cannot process all the information being received from the network. This is caused by the use of expanded memory managers, which increase the system overhead at the expense of system I/O performance. This problem is usually limited to computers with 8088 or 8086 processors. Also see LAT loses connections in this section.

Recommendations

Verify that the appropriate network connections exist between the client and server.

Ensure that all components existing between the client and the service node are appropriately configured.

Verify that the client hardware and software are appropriate for the amount of network traffic they must process.

Troubleshooting Procedure

1. Verify that the expanded memory manager is in use on your system. An expanded memory manager increases the overhead of each network interrupt call. This may cause problems on slow systems with heavy network activity.
2. Verify that LAT was loaded before using a task switcher, such as DOS V5.0 DOSSHELL. Also, you cannot switch out of a LAT session by using DOS V5.0 DOSSHELL.
3. Verify that there are enough SCBs.

LAT uses too much memory

Symptoms

```
LAT uses too much memory
```

Explanation

The amount of memory LAT uses is directly affected by the number of entries configured in the LAT service table. Each entry in the LAT service table uses 47 bytes of memory, so configure only the number of entries needed if memory constraints are an issue on your client. SCBs and printing also take up lots of memory. The use of EMS, if it is available, to load LAT can alleviate a shortage of conventional memory on DOS clients.

Recommendations

Reduce the service table size and use preferred services.

Configure FALLBACK and SEARCH on your LAT node.

Configure group codes to filter service announcements added to your service table. Try loading LAT into EMS memory.

Troubleshooting Procedure

1. Use the LAT Control Program to reconfigure your client using the minimum number of service table entries possible. If the default number of entries is 10, you only need to increase the number of entries in the LAT service table if you use more than 10 LAT services.
2. If it is possible to define all the services used as preferred services, do so.
3. Configure FALLBACK and SEARCH in LATCP to maximize the use of Service Table entries defined. Configuring FALLBACK causes LAT to try all known addresses for a LAT service. This is an efficient way to ensure connection to a service of your choice. Configuring SEARCH causes LAT to solicit LAT service nodes for a specific service. If the service is found, it enters the service in the LAT service table and discards any unused entries. The use of preferred services, FALLBACK and SEARCH, allows for the most efficient use of a small LAT service table.

LAT uses too much memory

4. If unable to configure all your LAT services as preferred services, the use of group codes allows you to filter any service announcements which do not match the group codes configured on your client. This keeps the LAT service table from making entries of services not used.
5. If your LAT service table is large and cannot be reduced through the techniques described above, try loading LAT into EMS memory if it is available. This frees up conventional memory and may reduce your memory constraints.

LAT does not work under an operating environment

Symptoms

```
LAT does not work under an operating environment (Microsoft Windows).
```

Explanation

Problems with different operating environments (Microsoft Windows) may be the result of how operating environments allocate memory and manage system resources (display, disk, network, and system I/O). The only applications supported at this point are SETHOST and the VT320 terminal emulator. However, the following information provides guidelines in troubleshooting LAT problems under your operating environment.

Recommendations

Ensure that LAT is loaded into conventional memory before starting the operating environment.

Troubleshooting Procedure

1. Verify that LAT works with SETHOST in a DOS environment before loading the operating environment.
2. Verify that LAT is loaded in conventional memory before starting the operating environment.
3. Verify that LAT has at least one application SCB shown for each LAT session you use. One application SCB is needed for each VT320 or SETHOST session you will use on your PC. Ensure that the client has sufficient LAT SCBs.
4. Ensure that the line SET NVTWIN=1 is added in your STARTNET.BAT file. This parameter is not installed by the NETSETUP program and must be done manually. This prevents the SCB from being swapped out of memory when you change windows.

Note

SETHOST and the VT320 terminal emulator have been enhanced so that SCBs are not swapped under Microsoft Windows.

LAT Terminal Server Problems

Terminal server connection failures

Symptoms

A user cannot connect to a service, VMS node, or ULTRIX host from a terminal server.

Explanation

This symptom indicates a LAN problem involving the LAT protocol. The terminal server cannot connect to the requested service, node, or host for one of the following reasons:

- The group code is undefined, or the group codes between the terminal server and the requested service, node, or host do not match.
- The terminal server node limit may be exceeded.
- The LAT protocol may not be started on the requested service, node, or host.
- Resources are insufficient on the requested service, node, or host.

Troubleshooting Strategy

Note

You can correct this problem using TSM or NCP to enter commands on the terminal server, or you can go directly to the terminal server and enter the commands.

Whether you use TSM or NCP, or enter the commands directly on the terminal server, the procedure is the same. Only the prompts change, depending on the method you use. For the purposes of illustration, TSM> is the prompt for the server commands in the following steps.

Troubleshooting Procedure

To troubleshoot this problem, do the following:

1. Make sure the group code definitions on the user's terminal server port match those on the requested service, VMS or ULTRIX system.

   A. Log in to the terminal server, using one of the following methods:

   - To use TSM to log in to the terminal server, run TSM and use the following command:

     ```
     TSM> USE SERVER server-id
     ```

   - To use NCP to log in to the terminal server, the terminal server must be defined in the NCP database. If the terminal server is defined in the NCP database, run NCP and use the following command to log in to it:

     ```
     NCP> CONNECT NODE server-id
     ```

     If the terminal server is not defined, you can use the following NCP command:

     ```
     NCP> CONNECT VIA PHYSICAL ADDRESS ethernet-physical-address
     ```

     When you enter the following terminal server commands, the system displays the Local> prompt rather than the TSM> prompt. To return to NCP from the Local> prompt, press Ctrl/D.

   - To enter commands directly on the terminal server, go to the terminal server and log in using your user name.

     ```
     Enter username> username
     ```

     When you enter the following terminal server commands, the system displays the Local> prompt rather than the TSM> prompt.

   Note

   From this point on, the commands are the same regardless of how you access the terminal server. However, the following prompts assume you use TSM to access the terminal server.

   B. For DECserver 100 terminal servers, use the following command to display the group codes defined on the terminal server:

   ```
   TSM> SHOW SERVER
   ```

For DECserver 200 terminal servers, use the following commands to display the group codes defined on the terminal server:

```
TSM>  SHOW SERVER server-id
TSM>  SHOW PORT port-id
```

C. If the requested service is a VMS system, do the following to display the group code definitions on that system:

   a. Run LATCP on the user's requested service, and use the following command to check the group codes:

      ```
      LCP>  SHOW CHARACTERISTICS
      ```

   b. Compare the group code definitions displayed in LATCP to those in the LTLOAD.COM file. The definitions should be the same.

   c. Compare the group code definitions on the VMS system to those you displayed in step 2 on the terminal server.

      - If the definitions are not the same for the VMS system and the terminal server, go to step 5.
      - If the definitions are the same for the VMS system and the terminal server, go to step B.

D. If the requested service is an ULTRIX system, do the following to display the group code definitions on that system:

   a. Use the following LAT control program (lcp) command to display the host characteristics:

      ```
      #  lcp -d
      ```

   b. Compare the group code definitions displayed in **lcp** to those in the rc.local file. The definitions should be the same.

   c. Compare the group code definitions on the ULTRIX system to those you displayed in step 2 on the terminal server.

      - If the definitions are not the same for the ULTRIX system and the terminal server, go to step 5.
      - If the definitions are the same for the ULTRIX system and the terminal server, go to step B.

E. Determine whether the group code definitions are correct on the terminal server or the service node (VMS or ULTRIX system), and correct as necessary.

   Step a explains how to redefine the group code definitions on the terminal server.

Step b explains how to redefine the group code definitions on the service node (VMS or ULTRIX system).

a. If the service node (VMS or ULTRIX system) definitions are correct, redefine the terminal server definitions to match the service node definitions as follows:

   i Use the following commands to redefine the group codes on the terminal server to match the group codes on the VMS or ULTRIX service node:

Note

These commands require that you use the SET PRIVILEGED command on the terminal server to enable privileges for these operations.

```
TSM> SET SERVER/ENABLE=group-list
TSM> DEFINE SERVER/ENABLE=group-list
```

   ii Use the following commands to define the port characteristics:

```
TSM> SET PORT AUTHORIZE GROUP group-id
TSM> DEFINE PORT AUTHORIZE GROUP group-id
TSM> SET PORT GROUP group-id
TSM> DEFINE PORT GROUP group-id
```

b. If the terminal server definitions are correct, then redefine the service node (VMS or ULTRIX) definitions to match the terminal server definitions, as follows:

   For VMS systems:

   i Run LATCP, and use the following commands to redefine the group codes on the service node:

```
LCP> SHOW CHARACTERISTICS
LCP> SET NODE/ENABLE=GROUPLIST
LCP> SET NODE/DISABLE=GROUPLIST
```

   ii Edit the SYS$MANAGER:LTLOAD.COM file to reflect the same group codes you just specified or deleted in LATCP.

For ULTRIX systems:

i Use the following **lcp** commands to redefine the group codes on the service node, substituting the appropriate group numbers for group_n:

```
# lcp -d
# lcp -g group_n, group_nn, group_nnn...
```

ii Edit the /etc/rc.local file to reflect the same group codes you just specified or deleted in lcp.

2. **If the group codes are properly defined and the problem persists, the number of systems defined in the group codes may be greater than the server node limit on the terminal server. Do the following:**

   1. Use the following command to display the server node limit on the terminal server:

      ```
      TSM>  SHOW SERVER
      ```

   2. If the server node limit on the terminal server is too small to accommodate the number of systems the terminal server needs to access, increase it using the following commands:

      ```
      TSM>  SET SERVER NODE LIMIT n
      TSM>  DEFINE SERVER NODE LIMIT n
      ```

3. **Be sure the LAT protocol is started on the requested VMS or ULTRIX system.**

   For VMS systems:

   Use the following command to start the LAT protocol:

   ```
   $  @LTLOAD.COM
   ```

   For ULTRIX systems:

   1. Be sure the configuration file contains the following lines:

      ```
      options          LAT
      pseudo-device    lat
      pseudo-device    lta n
      ```

      For non-RISC systems, the configuration file is /sys/conf/*hostname*. For RISC systems, the configuration file is /sys/conf/mips/*hostname*.

      For lta N, specify the number of terminals, using a multiple of 16.

   2. Add the following lines to the /etc/ttys file to define the tty devices:

```
tty08  "/etc/getty std.9600"  vt100  on nomodem #LAT
.
.
.
tty24  "/etc/getty std.9600"  vt100  on nomodem #LAT
```

3. Use the following **lcp** command to ensure the LAT protocol starts with the appropriate group code designations:

   ```
   #  lcp -s -G groupn, groupn...
   ```

4. Be sure the /etc/rc.local file contains the following line so that the LAT protocol starts and has the appropriate group codes defined:

   ```
   lcp -s
   ```

5. Be sure the DECnet or IP is running before you try to start LAT on an ULTRIX system.

   ULTRIX requires DECnet or IP to be running before LAT can start.

9
LAT Messages

This chapter contains LAT messages displayed on PCs using DOS or OS/2. The DOS messages section is first, with messages listed in alphabetical order. The OS/2 messages section is second, with messages listed in alphabetical order, and then in numerical order.

DOS Client Messages

This section contains messages that can be displayed on your DOS PC while you are using LAT. The message is shown first, followed by an explanation and advice on how to respond to the problem.

Cannot initialize the window system

Explanation: You tried to use the LATCP ADD or LATCP DELETE command on a video adapter that is not recognized by LAT. The window system could not display the information for the operation you specified.

User Action: Make sure you have sufficient memory available. If you have sufficient memory, test the video configuration by running another utility that uses video extensively.

You may also have a video problem that requires you to set your VGA card to emulate CGA. Set the VGA card using the utility supplied with the card.

Cannot open "filename.ext"

Explanation: LATCP HELP or DECLAT.DAT could not be opened.

User Action: Do any, or all, of the following:

- Make sure your path is valid for these files.
- Make sure you have sufficient storage space on your disk.
- Make sure you are not using a read-only disk. The LATCP ADD and DELETE commands modify DECLAT.DAT. Therefore, you need a disk with write privileges.

DLL not loaded.

Explanation: You cannot start LATCP until you load the Scheduler (SCH) and the data link.

User Action: Ensure that the Scheduler and the data link (DLLDEPCA) have been installed. If you are using NDIS, ensure that DLLNDIS is loaded.

Incompatible version of LAT

Explanation: You tried to use an earlier version of LAT with LATCP.

User Action: Use the version of LAT supplied with your PCSA Version 4.0 software. Reenter the command.

Insufficient memory (LATCP)

Explanation: You specified the LATCP ADD, DELETE, or one of the SHOW commands.

User Action: Because these commands use temporary buffers, you must have enough space for these buffers.

Insufficient space for the requested module.

Explanation: The allocated EMS memory is not big enough to load the specified module.

User Action: You need 128K bytes of memory to load network components. To achieve this, you may need to free some expanded memory by allocating less space to RAM disks or caches.

Invalid address

Explanation: You specified the LATCP ADD or DELETE command and entered an invalid node address or Ethernet address.

User Action: Reenter the command with a valid address.

Invalid service name

Explanation: You used an invalid service or print queue name.

User Action: Reenter the service name. Do not use special characters.

Initialization failed, Invalid printer, LPT x

Explanation: You tried to specify either of the following:

- A printer with an invalid LPT number (for example,LPT 5).

- An invalid printer because it was already defined as a LAT service or unavailable.

User Action: Make sure that the printer port you are initializing is not already initialized as a LAT service or that is available (not reserved by some other program).

Initialization failed, No printer LPT x

Explanation: You specified either of the following:

- A printer port that does not have a printer connected to it.
- A printer port that is not available to DOS.

User Action: Make sure that the printer port you are initializing is available from DOS before loading LAT and that the hardware needed (for example, printer and port) is properly configured and connected to the proper port.

initialization failed, No paper LPT x

Explanation: Check the paper supply in the printer to ensure that:

- There is paper in the printer.
- The paper is not jammed, causing an out of paper indication.

User Action: Make sure that the printer has paper and that it is not jammed.

Initialization failed, I/O error LPT x

Explanation: Check the printer to ensure that:

- The printer cable is connected properly to both the system and printer ports. Check the cable for damage.
- The printer control panel is not indicating any I/O errors and it is powered on.

User Action: Make sure that the printer is working by doing a self- test. If the self-test passes, verify that the cable is properly connected at both ends. If you think that the cable may be damaged, replace it. If the I/O error cannot be cleared through restarting the service, call your Digital service representative.

Initialization failed, Printer offline LPT x

Explanation: Check the printer to ensure that it is on line.

LAT.EXE has an invalid file format

Explanation: You specified the LATCP ADD command and tried either to load or unload LAT.EXE.

User Action: LAT.EXE could be corrupted. Obtain another copy of LAT.EXE and reenter your command.

LAT is not installed

Explanation: You specified one of the LATCP SHOW commands, but LAT.EXE is not loaded. The LATCP SHOW commands require that LAT.EXE be loaded first.

User Action: Load LAT.EXE and reenter the SHOW command.

LAT was not installed

Explanation: You used the LAT /u command to unload LAT when LAT hadn't been started.

User Action: Load LAT.EXE before you use LAT /u.

Scheduler has not been installed.

Explanation: You tried a file or printer service function, but the Scheduler has not been started.

User Action: Do all of the following:

- With the USE/STATUS command, find out if the Scheduler is installed.
- If not, install the Scheduler, using Netsetup.
- Make sure STARTNET.BAT has been executed by entering the STARTNET command.

Service name cannot exceed 16 characters

Explanation: You specified either the LATCP ADD or LATCP DELETE command and entered a service name that is longer than 16 characters.

User Action: Reenter the ADD or DELETE command and specify a service name that is no longer than 16 characters.

Service name too long

Explanation: You specified a service name that was too long.

User Action: Specify a service name with a maximum of 31 characters.

Service not offered

Explanation: You tried to connect to a service that may not be currently offered by any server.

User Action: Do any or all of the following:

- Try to reconnect to the service. Check that you have correctly spelled the service name.
- Use the LAT Control Program SHOW SERVICES to display the services that are listed in your LAT service table.

Service "string" not offered

Explanation: Either of the following occurred:

- You tried to connect to a service that is not currently offered.
- No server offering the service responded within the timeout period.

User Action: Use LATCP SHOW SERVICES to determine whether the service is available.

Syntax error

Explanation: You entered a command that LATCP could not recognize.

User Action: Reenter your LATCP command, using the correct syntax. For more information, see the LATCP commands.

The preferred service already exists

Explanation: You tried to add a preferred service that already exists.

User Action: No action necessary. The preferred service has already been added.

The preferred service does not exist

Explanation: You tried to delete a preferred service that does not exist.

User Action: No action necessary.

Unable to find the file LAT.EXE

Explanation: You specified either the LATCP ADD or the LATCP DELETE command, but LATCP could not find LAT.EXE.

User Action: Make sure your path is correct for the LAT.EXE file. Reenter your command.

Warning: Service table full Some sessions may be missing

Explanation: The service table is full. Certain services were probably not stored in the service table.

Explanation: Use the LATCP DEFINE SERVICE TABLE command to increase the number of services you can store in the service table. Then restart the LAT.

OS/2 Client Messages

This section contains messages that may be displayed on your PC while you are using the network. The message is shown first, followed by an explanation and advice on how to respond to the problem.

Unable to obtain information about current process.

Explanation: LATCP is unable to obtain process information by means of OS/2 system calls.

User Action: Check the SPD and ensure that you are running a supported version of OS/2.

Value "string" for /"string" switch is out of range

Explanation: The value specified is out of range.

User Action: Refer to the documentation for the allowed values and reenter the command.

LAT0003: LATCP is already running.

Explanation: You attempted to restart LATCP, while LATCP was running.

User Action: You must enter the command LATCP /SHUTDOWN to terminate LAT before restarting it.

LAT0004: LAT driver initialization error. Error code: "nn".

Explanation: The LAT driver attempted to initialize, and could not. This is typically caused by an improperly installed network, or because NETBIND has not been executed.

User Action: Verify that the network software (data link, Ethernet driver, and NETBIND) have all been started. Enter NETBIND at the OS/2 prompt. If NETBIND has executed, you receive a message stating that NETBIND has executed. If you receive a message stating that NETBIND has not started, you must reinstall the network by running Netsetup.

LAT0006: Could not open file LATCP.MSG

Explanation: The file specified cannot be found. This file is the message file for LATCP, LATCP.MSG. If this file is not found, then all messages printed by LAT are in English.

User Action: In your CONFIG.SYS file, place LATCP.MSG in a directory on the DPATH.

LAT0009: Could not change the state of the LAT Multicast.

Explanation: You requested an enable/disable of multicast addresses. This message is displayed when you cause an error in attempting to change the state of multicast. For example, you may have tried to turn on the LAT multicast when it is already on.

User Action: Reenter the request.

Part 4

Local Area System Transport (LAST)

10

Local Area System Transport (LAST) Tools

This chapter provides an overview of the LAST Control Program (LASTCP), which is used to control the Local Area System Transport (LAST) driver, and to display information about LAST.

LASTCP exists for two environments, VMS and OS/2, and the commands are different for each. Also, LASTCP on VMS offers an interactive mode, while LASTCP on OS/2 does not.

One of the reasons for these differences is that LAST on VMS supports both the server and client sides of the protocol. LAST on OS/2 supports only the client side of the protocol.

On DOS, the LAST driver is used to change the characteristics of LAST. The DOS LAST driver does not support an interactive mode.

This chapter includes the following sections:

- LASTCP on VMS
- LASTCP on OS/2
- LAST on DOS

LASTCP on VMS

To start LASTCP on VMS, type the following command:

```
$ RUN SYS$SYSTEM:ESS$LASTCP
%LASTCP-I-VERSION, LASTDRIVER X1.5 is running
LASTCP>
```

The LASTCP command syntax has four parts:

- A command verb
- A component
- One or more parameters
- One or more qualifiers

LASTCP has the following command verbs:

- EXIT
- HELP
- SHOW
- START
- STOP
- ZERO

Some command verbs act on a component. Those components can have parameters and the parameters can have qualifiers.

EXIT

The EXIT command returns you from LASTCP to the VMS prompt.

HELP

The HELP command activates the LASTCP help facility. HELP displays a list of keywords and topics. It then presents a TOPIC> prompt and allows you to enter the keyword or topic, on which you would like information.

SHOW

The SHOW command displays information about LASTDRIVER or its environment. The SHOW command can display information about the following:

- NODE
- COUNTERS
- STATUS

- CLIENTS
- SERVERS

Showing Information About Nodes

The SHOW NODE commands display the counters or characteristics of the indicated node. The displayed counter or characteristic information was counted or gathered by the node on which you are running LASTCP.

Showing Network Counters

The SHOW COUNTERS command displays the counters for line, circuit, or transport. The qualifier /ALL_CONTROLLER displays the counters for all active Ethernet controllers. The qualifier /CONTROLLERS displays the counters for the specified Ethernet controllers. By default, only the counters for the first controller are displayed.

The controller letter used in the /CONTROLLERS qualifier is one of A, B, C, or D (the maximum number of controllers is four). The controller letter is taken from the device name, which has the form DDCU:, where:

DD is the device type
 C is the controller field
 U is the unit number

For example, XQA0: indicates controller A and XEB0: indicates controller B.

Showing the LASTDRIVER Status

The SHOW STATUS command displays the current status and operational characteristics of LASTDRIVER.

Showing Known Servers

The SHOW SERVERS command displays a list of the LAST server nodes that are known to be on the network.

START TRANSPORT

The START TRANSPORT command starts LASTDRIVER.

First, LASTCP will try to start the device specified in the /DEVICE qualifier. If /DEVICE is not specified, LASTCP will start the device specified in the LAST$DEVICE logical name. Finally, if neither /DEVICE nor LAST$DEVICE are specified, LASTCP will attempt to start all Ethernet devices based on an internal table.

The LAST transport should not be started until DECnet has been started. If the LAST transport is started before DECnet, DECnet will not start properly.

START TRANSPORT /ALL_CONTROLLERS

The /ALL_CONTROLLERS qualifier instructs LASTCP to start LAST on all available Ethernet adapters.

If the /CONTROLLERS qualifier is used, the /ALL_CONTROLLERS qualifier cannot be used.

The default is to start all Ethernet controllers.

START TRANSPORT /CHECKSUM

The /CHECKSUM qualifier establishes mandatory data checksums for all messages exchanged between the current node and any remote node. LASTDRIVER computes a checksum for all messages and verifies the checksum on all received messages.

START TRANSPORT /CIRCUIT_MAXIMUM

The /CIRCUIT_MAXIMUM qualifier sets the maximum number of nodes that can be simultaneously connected.

The default maximum circuits is 80.

START TRANSPORT /CONTROLLERS

The /CONTROLLERS qualifier specifies the Ethernet controllers to initialize for LASTDRIVER. The default is to initialize all Ethernet controllers.

If the /ALL_CONTROLLERS qualifier is used, the /CONTROLLERS qualifier cannot be used.

The controller letter used in the /CONTROLLERS qualifier is one of A, B, C, or D (the maximum number of controllers is four). The controller letter is taken from the device name, which has the form DDCU:, where:

DD is the device type
C is the controller field
U is the unit number

For example, XQA0: indicates controller A and XEB0: indicates controller B.

START TRANSPORT /DEVICE

The /DEVICE qualifier starts the LAST on the specified device(s). This qualifier overrides the LASTCP default device table and the LAST$DEVICE logical name.

START TRANSPORT /GROUP

The /GROUP qualifier specifies the LAST group code.

Group codes are a method of segmenting a LAN so that services associated with certain nodes are not seen by other nodes. An example of such an environment is an extended LAN. A network manager may want to restrict nodes to services offered on their own LAN segment.

When specifying a group code, enter a number between 0 and 1023 inclusive. The default group code is zero.

START TRANSPORT /NODE_NAME

The /NODE_NAME qualifier specifies the node name that LASTCP should use to initialize LASTDRIVER.

By default, LASTCP uses the DECnet node name.

START TRANSPORT /SLOW_MODE

The /SLOW_MODE qualifier instructs LASTDRIVER to require remote transmitters to use a TRANSMIT_QUOTA of one when communicating with this node. This introduces a transmit delay for slow recipients.

This qualifier is not normally used.

START TRANSPORT /TIMEOUT

The /TIMEOUT qualifier specifies the minimum timeout interval (in seconds) to be used by LAST. The timeout interval determines when inactive clients should be disconnected. An inactive client is one that has been turned off or otherwise isolated from the server.

By default, the server's timer is specified by the client transport. The /TIMEOUT qualifier allows a minimum value to be enforced on all connections.

The value n represents an integer in the range of 60 to 65534.

START TRANSPORT /TRANSMIT_QUOTA

The /TRANSMIT_QUOTA qualifier specifies the number of transmit buffers LASTDRIVER can use to communicate with a remote node.

The default value is five.

STOP

The STOP command stops LASTDRIVER. After stopping LASTDRIVER, this node can not communicate over LAST.

ZERO

This command sets all of the specified component's counters to zero.

LASTCP on OS/2

There are two different methods of invoking LASTCP on OS/2. The first method is used for installing the LAST device driver. The second method is used to change the characteristics of the LAST driver or to display information about LAST.

Installing and Starting LAST

LASTCP has the following format for installing and starting LAST:

Format

```
                 ┌ /N:name  ┐
                 │ /M:D | E │
DETACH LASTCP    │ /C:D | E │
                 │ /R:n     │
                 │ /W:n     │
                 └ /G:n     ┘
```

Qualifier	Value	Usage
/N:	name	The DECnet node name
/M:	D	Disables reception of multicast traffic (default mode)
	E	Enables reception of multicast traffic
/C:	D	Disables checksumming (default mode)
	E	Enables checksumming
/R:	n	The quota of read buffers for a single transaction (the range is 1 to 15 and the default is 4)
/W:	n	The quota of write buffers for single transaction (the range is 1 to 15 and the default is 4)
/G:	n	The group code number (the range is 1 to 1023 and the default is 0)

Changing the Characteristics or Displaying Information

LASTCP has the following format for changing the characteristics of LAST or displaying information about LAST.

Format

```
        ┌ /SHUTDOWN  ┐
        │ /COUNTERS  │
LASTCP  │ /VERSION   │
        │ /ZERO      │
        │ /R:n       │
        └ /W:n       ┘
```

Qualifier	Value	Usage
/SHUTDOWN		Stops the LAST background process
/COUNTERS		Displays the LAST counters
/VERSION		Displays the LAST version number and status
/ZERO		Sets the LAST counters to zero
/R:	n	The quota of read buffers for a single transaction (the range is 1 to 15)
/W:	n	The quota of write buffers for single transaction (the range is 1 to 15)

LAST on DOS

LAST has the following format for installing and starting LAST and for changing the characteristics of LAST:

Format

```
               ┌ /N:name  ┐
DETACH LASTCP  │ /M:D | E │
               │ /C:D | E │
               └ /G:n     ┘
```

Qualifier	Value	Usage
/N:	name	The DECnet node name (When LAST is installed before DECnet DNP, this switch must be used.)
/M:	D	Disables reception of multicast traffic (default mode)
	E	Enables reception of multicast traffic
/C:	D	Disables checksumming (default mode)
	E	Enables checksumming
/G:	n	The group code number (the range is 1 to 1023 and the default is 0)

11

Isolating Local Area System Transport (LAST) Problems

This chapter contains the LAST problem-isolation flowchart and a series of troubleshooting procedures. The flowcharts help you isolate LAST network problems. After you have isolated a problem, a decision point leads you to a procedure or a set of procedures. You can locate the starting page for each procedure in the Contents or in the index.

The master procedures are:

- VMS Server Master Procedure (LAST)
- DOS Client Master Procedure (LAST)
- OS/2 Client Master Procedure (LAST)
- Network Connection Procedure
- Network Segment Interface Procedure

LAST Problem-Isolation Flowcharts

To isolate a network problem, you must consider several key questions. The answer to each question determines which procedure you should perform. This section contains a table and a series of flowcharts, which ask the questions that guide you through the procedures.

In the flowcharts, the first key question asks if the network has ever carried traffic. If the answer is no, perform the VMS Server Master Procedure (LAST). This master procedure combines several procedures into one. You may not have to perform all of the subprocedures in the master procedure.

The remaining flowcharts ask questions specific to your network. The procedure you should use depends on your answer to questions. You may have to perform client, disk server, file server, or print server procedures.

Note

You should address each question in order. The answer to each question helps you rule out unlikely problems.

Table 11–1 lists the key questions in flowchart order and indicates the path you should take. For example, if your answer to key question 1 is No, go to Figure 11–1, Problem with Untried Network. If your answer is Yes, go to key question 2.

Table 11–1 Key Questions for LAST

	Key Question	If ...	Go to ...
1.	Has the network ever carried traffic?	No	Figure 11–1, Problem with Untried Network (LAST Flowchart 1)
		Yes	Key Question 2
2.	Has hardware been added or changed?	Yes	Figure 11–2, When Hardware Has Changed (LAST Flowchart 2)
		No	Key Question 3
3.	Has the network been modified?	No	Figure 11–3, When Software Is Unmodified (LAST Flowchart 3)
		Yes	Key Question 4
4.	Is there an error message? If not, is there a transport problem?	Yes	Figure 11–4, Problem with Transport (LAST Flowchart 4)
		No	Key Question 5
5.	Is there a problem with disk services?	Yes	Figure 11–5, Problem with Disk Services (LAST Flowchart 5)
		No	Key Question 6
6.	Is there a problem with file services?	Yes	Figure 11–6, Problem with File Services (LAST Flowchart 6)
		No	Key Question 7
7.	Is there a problem with print services?	Yes	Figure 11–7, Problem with Print Services (LAST Flowchart 7)

Figure 11–1 Problem with Untried Network (LAST Flowchart 1)

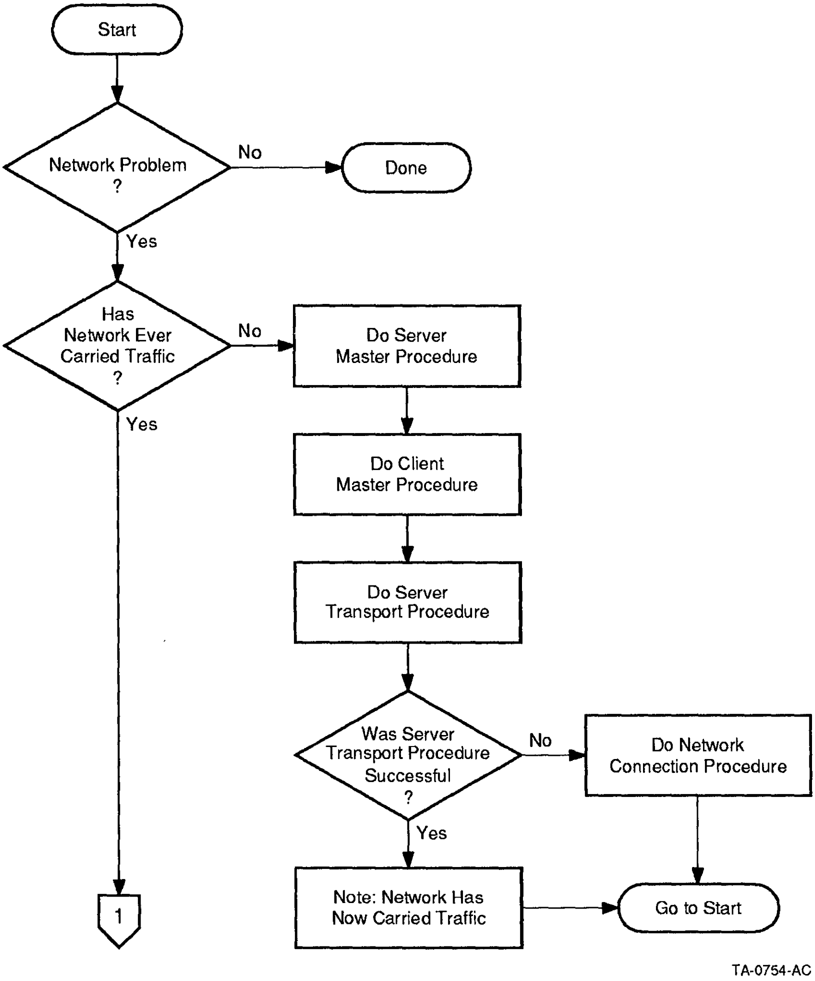

Start
Network Problem ?
No
Done
Yes
Has Network Ever Carried Traffic ?
No
Do Server Master Procedure
Do Client Master Procedure
Do Server Transport Procedure
Was Server Transport Procedure Successful ?
No
Do Network Connection Procedure
Yes
Note: Network Has Now Carried Traffic
Go to Start
Yes
1
TA-0754-AC

Figure 11–2 When Hardware Has Changed (LAST Flowchart 2)

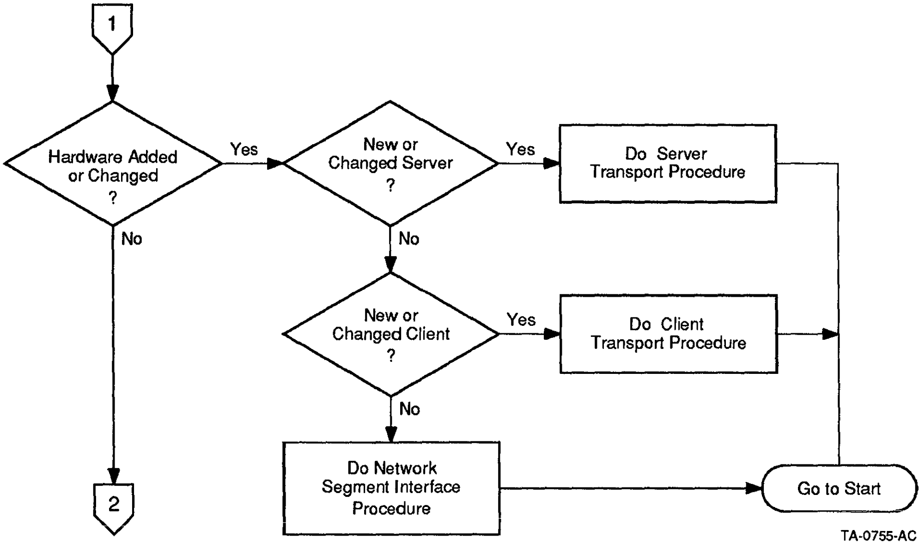

1
Hardware Added or Changed ?
Yes
No
New or Changed Server ?
Yes
Do Server Transport Procedure
No
New or Changed Client ?
Yes
Do Client Transport Procedure
No
Do Network Segment Interface Procedure
Go to Start
2
TA-0755-AC

Figure 11–3 When Software Is Unmodified (LAST Flowchart 3)

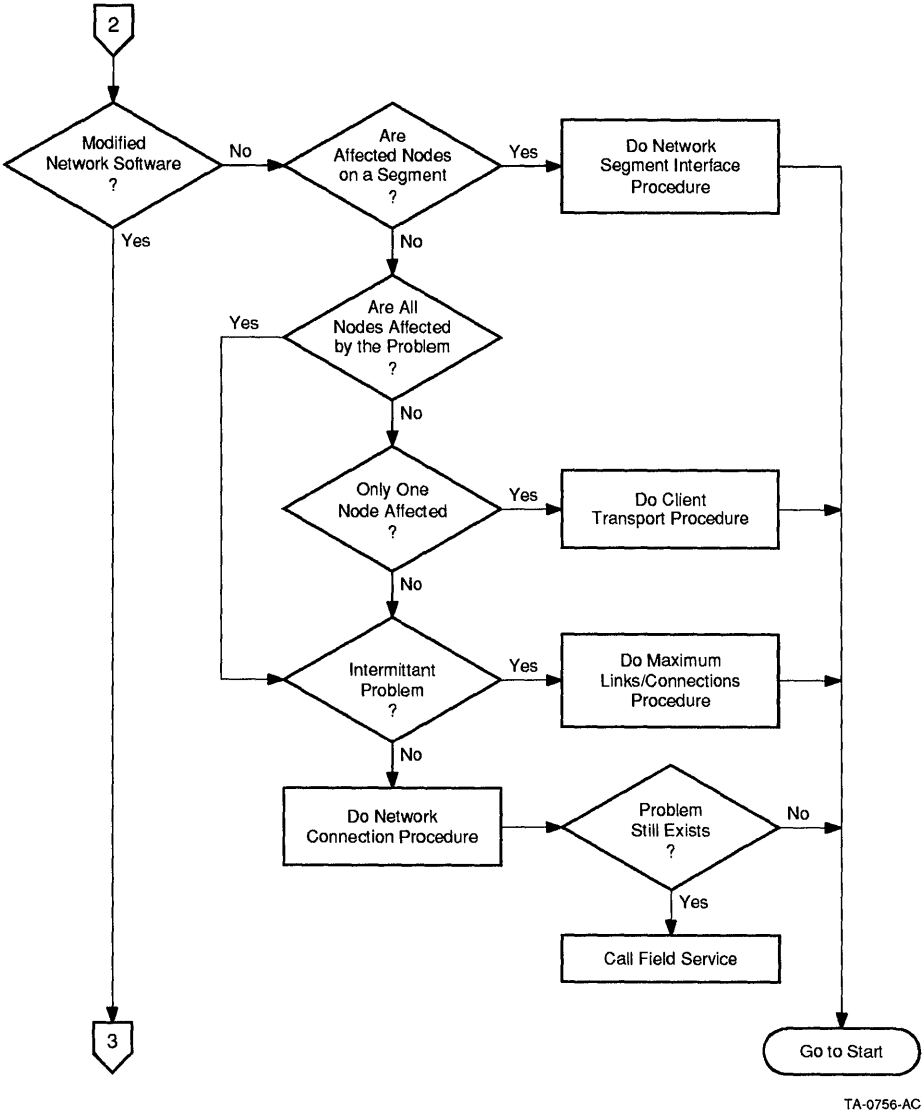
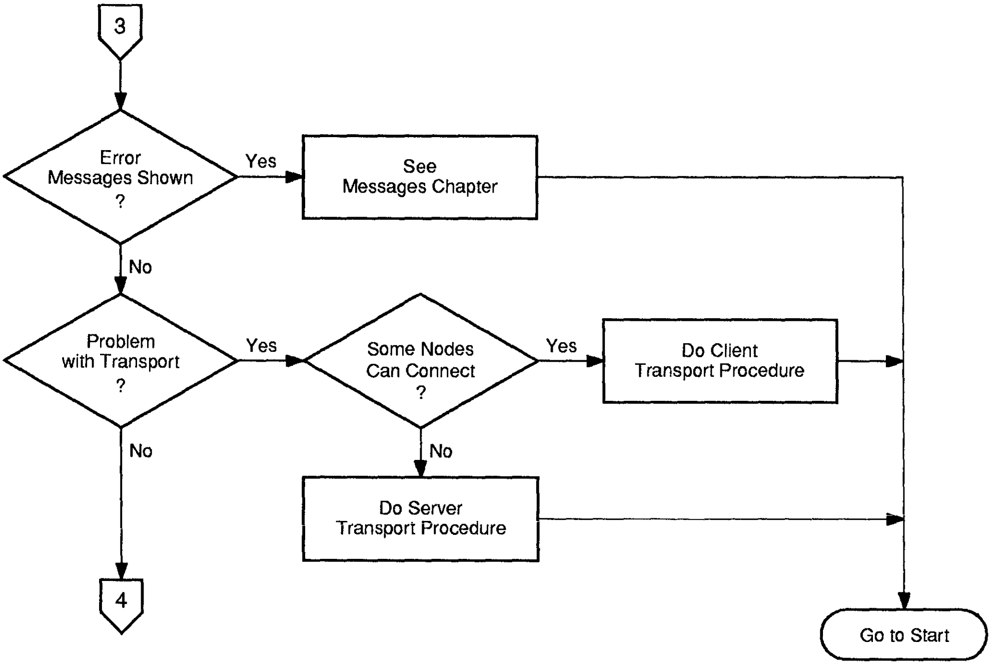

2
Modified Network Software ?
No
Yes
Are Affected Nodes on a Segment ?
Yes
No
Do Network Segment Interface Procedure
Are All Nodes Affected by the Problem ?
Yes
No
Only One Node Affected ?
Yes
No
Do Client Transport Procedure
Intermittant Problem ?
Yes
No
Do Maximum Links/Connections Procedure
Do Network Connection Procedure
Problem Still Exists ?
No
Yes
Call Field Service
3
Go to Start
TA-0756-AC

Figure 11–4 Problem with Transport (LAST Flowchart 4)



TA-0757-AC

Figure 11–5 Problem with Disk Services (LAST Flowchart 5)

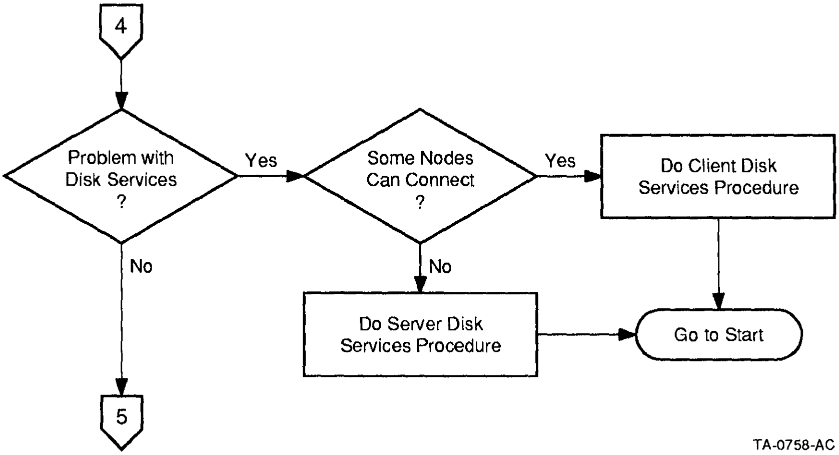

4
Problem with Disk Services ?
Yes
Some Nodes Can Connect ?
Yes
Do Client Disk Services Procedure
No
No
Do Server Disk Services Procedure
Go to Start
5
TA-0758-AC

Figure 11–6 Problem with File Services (LAST Flowchart 6)

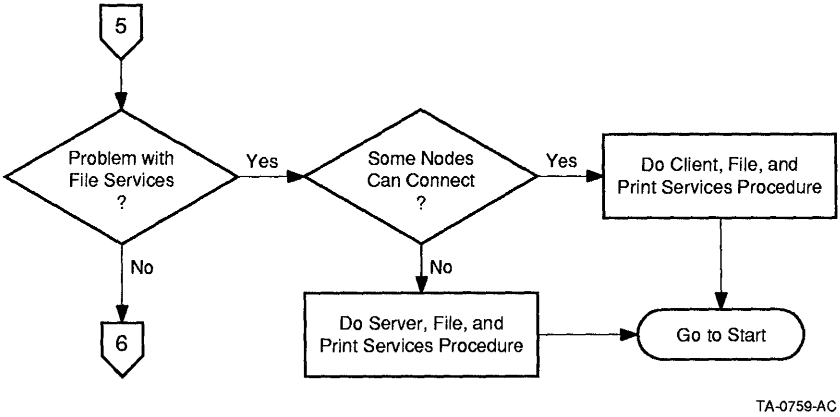
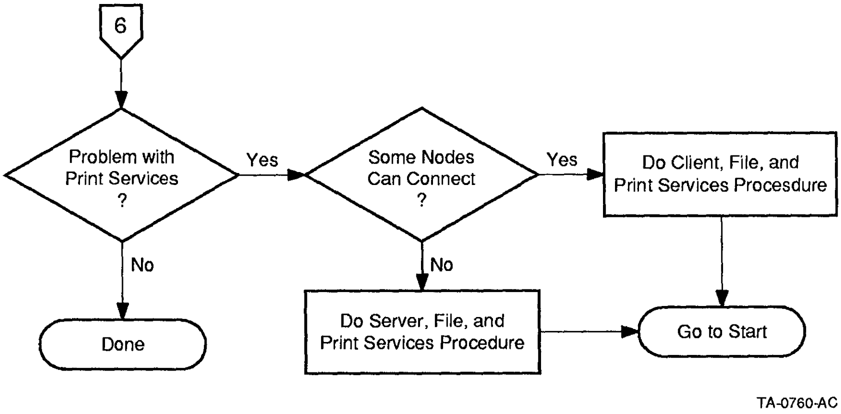

5
Problem with File Services ?
Yes
Some Nodes Can Connect ?
Yes
Do Client, File, and Print Services Procedure
No
No
6
Do Server, File, and Print Services Procedure
Go to Start
TA-0759-AC

Figure 11–7 Problem with Print Services (LAST Flowchart 7)


6
Problem with Print Services ?
Yes
Some Nodes Can Connect ?
Yes
Do Client, File, and Print Services Procesdure
No
No
Done
Do Server, File, and Print Services Procedure
Go to Start
TA-0760-AC

VMS Server Master Procedure (LAST)

The VMS Server Master Procedure (LAST) is a set of procedures that are used to verify the operational state of LAST on a VMS server. The VMS Server Master Procedure (LAST) has the following subprocedures:

- The VMS Server Transport Procedure
- The VMS Server Disk Services Procedure
- The VMS Server File and Print Services Procedure
- The VMS Server Maximum Connections Procedure

Use these procedures to verify that your VMS server is operational. If you cannot successfully perform the VMS Server Transport Procedure (LAST), you will be required to perform hardware diagnostics procedures. These procedures are located in Isolating DECnet Problems in this manual.

VMS Server Transport Procedure (LAST)

This procedure verifies that the LAST driver is operating correctly on a VMS server.

Note

LAST should always be started after DECnet has started.

When DECnet starts, it changes the Ethernet adapter's physical address from the Ethernet hardware address to the Ethernet address used by DECnet. If LAST has been started before DECnet, then DECnet cannot change the physical address and will not start correctly.

You can verify the startup sequence by examining the contents of the file SYS$STARTUP:SYSTARTUP_V5.COM.

1. Log in to the system manager's account.
2. Verify the version number of the VMS operating system that is running on your server by entering:

```
$  SHOW SYSTEM
VAX/VMS V5.3  on node VVSRV  18-DEC-1990 00:02:08.24   Uptime  0 00:34:40
  Pid     Process Name    State  Pri      I/O       CPU       Page flts Ph.Mem
00000021 SWAPPER          HIB     16        0   0 00:00:01.65         0      0
00000044  LTA5:           CUR      7      243   0 00:00:04.88       790    246
00000026 ERRFMT           HIB      8       55   0 00:00:00.61        81    115
00000027 OPCOM            HIB      8       74   0 00:00:01.17       241    109
00000028 AUDIT_SERVER     HIB     10       27   0 00:00:01.57      1315    165
00000029 JOB_CONTROL      HIB      8      399   0 00:00:02.91       208    287
0000002A CONFIGURE        HIB      8        8   0 00:00:00.32        89    135
0000002B SYMBIONT_0001    HIB      6       30   0 00:00:01.00       239    182
0000002D NETBIOS          HIB      9       31   0 00:00:00.52       150    185
0000002E NETACP           HIB     10       41   0 00:00:01.49       292    322
0000002F REMACP           HIB      8       12   0 00:00:00.16        64     32
00000032 PCFS_SERVER      HIB     10     1227   0 00:00:23.44      1080   2199
00000033 LAD$KERNEL       HIB      9      108   0 00:00:01.79       182    253
0000003C SYSTEM           LEF      7      955   0 00:00:19.88      2982    174
```

   The first line of the response contains the version number of the VMS operating system that is running on your server. If the version number is less than 5.3, you must upgrade your VMS operating system.

3. Ensure that the LAST driver is running by entering:

```
$  RUN SYS$SYSTEM:ESS$LASTCP
%LASTCP-I-VERSION, LASTDRIVER V1.5 is running
LASTCP>
```

   When starting LASTCP, notice the state of the LASTDRIVER in the version message. If the state is stopped, you must restart the LASTDRIVER with the command file LAD_STARTUP.COM.

4. Determine the nodes that are reachable over LAST by entering:

```
LASTCP> SHOW KNOWN NODES
 Node                 Node            Physical       Active     Start
 Name                  Id             Address         Links     Time

VVSRV            08002B0D2F8C-76E0  AA-00-04-00-48-25    0         -
WRKONE           08002B07BC4F-5D07  AA-00-04-00-D6-24    0         -
WRKTWO           08002B14CB75-78E8  AA-00-04-00-84-27    0         -

Total of 3 known nodes
LASTCP> EXIT
$
```

At a minimum, the server node on which you are operating LASTCP should be listed as a known node. If the response is the message "Total of 0 known nodes", then the LAST driver is not running. Restart the LAST driver with the command file LAD_STARTUP.COM.

If the server node is listed, but no other nodes are listed, then one of the following problems exists:

- LAST is not running on any other node on the network.
- Between the server and the client, there is a physical connection problem in the Ethernet.

Use the appropriate client procedure (DOS or OS/2) to ensure that LAST is running on a client that is on the same Ethernet segment.

After ensuring that LAST is running on a client, repeat the LASTCP command SHOW KNOWN NODES. If only the server node is listed, it is likely that a physical connection problem exists. Use the procedures in the Isolating DECnet Problems chapter to find and correct the connection problem. Then, repeat this procedure to confirm that LAST is working correctly.

VMS Server Transport Procedure Completion (LAST)

The VMS Server Transport Procedure (LAST) is complete. If successful, you know that LAST is running correctly on the VMS server.

VMS Server Disk Services Procedure (LAST)

This procedure verifies that the disk server is operating correctly on a VMS server. The disk server's process name is LAD$KERNEL.

To successfully complete this procedure, it is assumed that you have successfully completed the VMS Server Transport Procedure (LAST).

1. Ensure that the disk server is running:

```
$ ADMINISTER /PCSA
PCSA_MANAGER> SHOW DISK_SERVER SERVICES /TYPE=ALL


Disk server services:
Service name Type  Server  Limit  Users  Acc  Rating  Status
------------ ----  ------  -----  -----  ---  ------  -------------
MSWINV21     USER  VVSRV      30      0  RO        1  MNT PERM
PCSA$DOS_SYSTEM_V22
             SYST  VVSRV    NONE      0  RO        1  MNT PERM
PCSA$DOS_SYSTEM_V30
             SYST  VVSRV    NONE      0  RO        1  MNT PERM
```

The previous example contains a normal response, which indicates that the disk server is running and has three disk services mounted. If this is a new installation (not an upgrade) and no disk services have been created and mounted, then the response appears as follows.

Note

For PATHWORKS for VMS Version 4.1, the DOS system files are stored in the file service PCSAV40 and will not appear in the list of disk services.

If PATHWORKS for VMS Version 4.1 is the first version of disk services that has been installed on this server and no disk services have been created, then the message "%PCSA-E-NOACTSERVICES, no active services" is displayed. In that case, the disk server is running, but no disk services are available.

If PCSA Manager returns the following error messages, the disk server is not running:

```
%PCSA-E-NODSRVLINK, unable to establish link to Disk Server
%PCSA-E-DISKSRVNOTAVAIL, Disk Server is not available
```

The disk server must be started as follows:

```
PCSA_MANAGER> EXIT
$ @SYS$STARTUP:LAD_STARTUP
```

2. Ensure that the service you are trying to connect to exists and is mounted. In the following example, the service name is TESTER.

```
$  ADMINISTER /PCSA
PCSA_MANAGER> SHOW DISK_SERVER SERVICES /SERVICE=service_name


Disk server services:


Service name  Type  Server  Limit  Users  Acc  Rating  Status
------------  ----  ------  -----  -----  ---  ------  -------------
TESTER        USER  VVSRV      30      0   RW       1  MNT PERM
```

In the previous example, service_name is the name used at the client in the USE command to connect to the disk service. In the following example, TESTER is the service:

```
A:\> USE E: TESTER /V
```

If the PCSA Manager shows the following response, the disk service was not mounted or it was dismounted with the /PERMANENT switch.

```
%PCSA-E-NOACTSERMATCH, no active services match user constraints
```

If a container file exists and you know the location of the container file, you can mount the disk service as follows:

```
PCSA_MANAGER>  MOUNT DISK file_name service_name -
_PCSA_MANAGER>  /ACCESS=access_type -
_PCSA_MANAGER>  /CONNECTIONS=connections -
_PCSA_MANAGER>  /TYPE=mount_type /PASSWORD=password -
_PCSA_MANAGER>  /PERMANENT
```

file_name
Is a valid VMS file name and is the name of the container file created using PCSA Manager (for example, DUA0:[PCSA.LAD]TESTER.DSK).

service_name
Is the service name used at the client to connect to the service (for example, TESTER).

connections
Is the number of users allowed to connect to a service at one time. If the access_type is WRITE, connections cannot be specified.

access_type
Is READ or WRITE. Write access implies read access. If the optional switch, /ACCESS, is omitted, access defaults to read only.

password
Is the password that must be used at the client to allow connections to the service. If the optional switch, /PASSWORD, is omitted, a password is not assigned and a password is not required at the client.

If a container file does not exist, you can create a container file using the following command line:

```
PCSA_MANAGER> CREATE DISK file_name -
_PCSA_MANAGER> /CONTIGUOUS /SIZE=size /TYPE=type
```

file_name — Is a valid VMS file name and is the name of the container file created using PCSA Manager (for example, SYS$SYSDEVICE:[PCSA.LAD]TESTER.DSK).

size — Is one of 360KB, 720KB, 1.2MB, 1.44MB, 5MB, 10MB, 20MB, 32MB, 64MB, 128MB, 256MB or 512MB. If the TYPE is boot, 360KB, 720KB, 1.2MB, and 1.44MB are valid sizes. If the optional switch, /SIZE, is omitted, size defaults to 1.2MB.

type — Is one of APPLICATION, BOOT, SYSTEM, or USER. If the optional switch, /TYPE, is omitted, the type defaults to USER.

For consistency in the troubleshooting procedures, confirm the existence of the disk service TESTER by entering:

```
$ ADMINISTER /PCSA
PCSA_MANAGER> SHOW DISK_SERVER SERVICES /TYPE=ALL
%PCSA-E-NOACTSERMATCH, no active services match user constraints
```

If the disk service does not exist, create and mount the disk service TESTER by entering:

```
PCSA_MANAGER> CREATE DISK TESTER /SIZE=1.2MB /TYPE=SYSTEM
%PCSA-I-CREATEDISK, creating SYS$SYSDEVICE:[PCSA.LAD]TESTER.DSK
%PCSA-I-FORMATDISK, formatting disk, Size = 1.2MB, Allocation = 2400/2400
%PCSA-I-DISKCREATED, SYS$SYSDEVICE:[PCSA.LAD]TESTER.DSK created

PCSA_MANAGER> MOUNT DISK SYS$SYSDEVICE:[PCSA.LAD]TESTER.DSK TESTER -
_PCSA_MANAGER> /TYPE=SYSTEM /ACCESS=WRITE /PERMANENT
%PCSA-I-DISKMOUNTED, SYS$SYSDEVICE:[PCSA.LAD]TESTER.DSK;1 mounted
%PCSA-I-MOUNTINFO, service name = TESTER, server node = MATHBX

PCSA_MANAGER> SHOW DISK_SERVER SERVICES /TYPE=ALL

Disk server services:

Service name  Type  Server           Limit  Users  Acc  Rating  Status
------------  ----  ---------------  -----  -----  ---  ------  -------------
TESTER        SYST  MATHBX               1      0  RW        1  MNT PERM

PCSA_MANAGER>
```

VMS Server Disk Services Procedure Completion (LAST)

The VMS Server Disk Services Procedure is complete. Successfully completing this procedure indicates that the disk server is set up correctly on the VMS server.

VMS Server File and Print Services Procedure (LAST)

This procedure verifies that LANSDRIVER is operating correctly on a VMS server.

To successfully complete this procedure, it is assumed that you have successfully completed the VMS Server Transport Procedure (LAST).

PATHWORKS for VMS Version 4.1 provides file and print services over LAST. LANSDRIVER provides the interface between LAST and PCFS_SERVER (the file and print services process).

- Perform VMS Server Master Procedure (DECnet) and DOS Client Master Procedure (DECnet) to ensure that file and print services are operating correctly.
- Ensure that LANSDRIVER is loaded by entering:

```
$  RUN SYS$SYSTEM:SYSGEN
SYSGEN>   SHOW /DRIVER

  Driver      Start    End
IKDRIVER    8037A610 8037B540
IMDRIVER    80379AF0 8037A400
INDRIVER    80377180 80379AF0
GWDRIVER    80373830 80374140
PSDRIVER    8035A1C0 8035A8C0
LADCDRIVER  80358030 80358F80
LADDRIVER   803155B0 803171C0
LANSDRIVER  803127B0 803146C0
LTDRIVER    8030DD60 803124E0
LASTDRIVER  80309760 8030DA10
RTTDRIVER   803084B0 80309010
CTDRIVER    80305F70 803084B0
NDDRIVER    802F9A80 802FA510
NETDRIVER   802F4E20 802F9A80
YFDRIVER    802F1420 802F22D0
XQDRIVER    802E9EB0 802F0380
TUDRIVER    802E6440 802E9EB0
PYDRIVER    802E3AC0 802E41C0
TWDRIVER    8044AA30 8044AEB0
WSDRIVER    802E3350 802E3750
DUDRIVER    803A2F10 803A76A9
PUDRIVER    803A0890 803A2F06
TTDRIVER    8039A9B0 803A0889
OPERATOR    80201400 80201914
NLDRIVER    801A7483 801A7602
MBDRIVER    801A7400 801A7D8B
SYSGEN>   EXIT
```

If LANSDRIVER appears in the list, it is loaded. If LANSDRIVER does not appear in the list, restart the file server with the command file SYS$STARTUP:PCFS_STARTUP.COM. After restarting the file server if LANSDRIVER does not appear in the list, it is likely that PATHWORKS for VMS Version 4.1 was installed incorrectly.

VMS Server File and Print Services Procedure Completion (LAST)

The VMS Server File and Print Services Procedure (LAST) is complete. Successfully completing this procedure indicates that file and print services are set up correctly on the VMS server.

VMS Server Maximum Connections Procedure (LAST)

This procedure verifies that the problem with making a connection is not due to reaching the maximum number of connections for a service.

If you are trying to connect to a disk service, use the Disk Services Maximum Connection Procedure. Otherwise, use the File and Print Services Maximum Connection Procedure.

Disk Services Maximum Connection Procedure

Ensure that the maximum number of connections has not been reached:

```
$  ADMINISTER /PCSA
PCSA_MANAGER>  SHOW DISK_SERVER SERVICES /TYPE=ALL


Disk server services:
Service name  Type  Server  Limit  Users  Acc  Rating  Status
------------  ----  ------  -----  -----  ---  ------  -------------
MSWINV21      USER  VVSRV      30      0  RO        1  MNT PERM
PCSA$DOS_SYSTEM_V22
              SYST  VVSRV    NONE      0  RO        1  MNT PERM
PCSA$DOS_SYSTEM_V30
              SYST  VVSRV    NONE      0  RO        1  MNT PERM
```

The previous example contains a normal response, which indicates that MSWINV21 has a limit of 30 and that no one is connected to the service.

If the maximum number of connections has been reached, then you must determine if this is the normal number of connections. If this is the normal number of connections, you can either increase the number of allowed connections or create the same service on another server.

File and Printer Services Maximum Connection Procedure

Ensure that the maximum number of connections has not been reached:

```
$  ADMINISTER /PCSA
PCSA_MANAGER>  SHOW FILE_SERVER SERVICE /ACTIVE

File Server active services:

Service name  Service type  Att/Len  Limit  Users
------------  ------------  -------  -----  -----
LN03AF11$ANSI
              PRINTER       STR/EST   NONE      1
THOMAS        USER          STR/EST      1      1

PCSA_MANAGER>
```

The previous example contains a normal response, which indicates that THOMAS has a limit of one and that one connection is currently active.

If the maximum number of connections has been reached, then you must determine if this is the normal number of connections. If this is the normal number of connections, you can either increase the number of allowed connections or create the same service on another server.

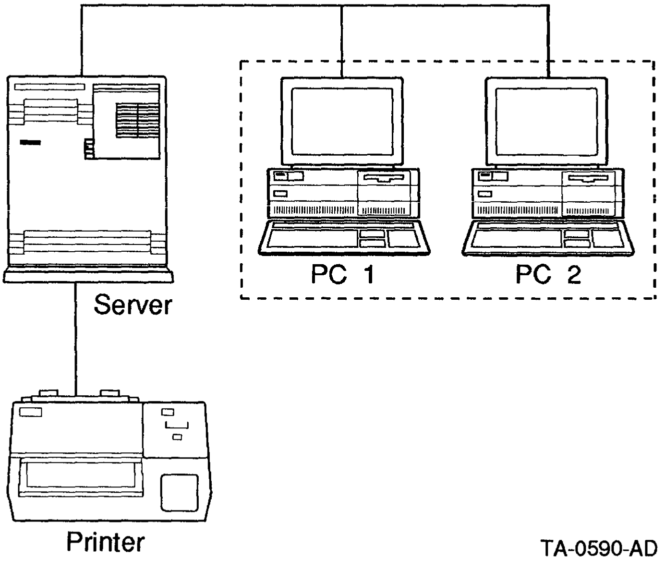
VMS Server Maximum Connections Procedure Completion (LAST)

The VMS Server Maximum Connections Procedure is complete. Successfully completing this procedure indicates that the service connections are within the maximum limit on the VMS server.

VMS Server Master Procedure Completion (LAST)

The VMS Server Master Procedure (LAST) is complete. If successful, you know that the VMS server on your network, shown in Figure 11–8, is set up correctly.

Figure 11–8 VMS Server Set Up Correctly



DOS Client Master Procedure (LAST)

The DOS Client Master Procedure (LAST) contains the following procedures:

- DOS Client Required Components Procedure
- DOS Client Memory Interaction Procedure
- DOS Client Transport Procedure
- DOS Client Disk Services Procedure
- DOS Client File and Print Services Procedure

Use these procedures to verify that your DOS client is operational. To perform these tests, boot the DOS client with the key diskette. Then perform the indicated test.

If you cannot successfully perform the DOS Client Transport Procedure (LAST), you will be required to confirm that no server or client network hardware problems exist. The procedures used to isolate network hardware problems are located in Isolating DECnet Problems. When performing those procedures, load the network components into conventional memory. Doing so minimizes the opportunity for one problem to hide another problem. The section DOS Client Memory Interaction Procedure (LAST) discusses loading network components into conventional memory.

Troubleshooting Considerations

Note

> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

PATHWORKS for DOS Version 4.1 includes a wider variety of options for configuration of network software than previous versions. The DOS client user can choose to load selected network components into extended memory or into expanded memory and can choose not to load certain components at all or to load and unload them as needed. This introduces two considerations into troubleshooting DOS client network problems:

- The first consideration involves the use of extended or expanded memory. When components of PCSA network software occupy extended or expanded memory, problems may arise due to conflicts with other software. For example, if any part of the network software is in expanded memory, TSR applications that use hot keys may hang. Because of this potential for conflicts, we recommend that you remove all network components from extended and expanded memory and reload them into conventional memory before performing the tests in the DOS client procedures. The DOS client memory interaction procedure explains how to do this.

- The second consideration involves the loading of the appropriate components. In general, the procedures include steps to ensure that the components required for correct operation of each type of service are present.

When you are troubleshooting disk services (LAD.EXE) or file services (LANSESS.EXE), always set the read (/R:1) and write (/W:1) transaction size to 1. Doing so precludes packet congestion (data overrun) at the client adapter. If you are troubleshooting a new network, it also precludes packet congestion at the server adapter until multiple clients are operating on the network.

Remember the following troubleshooting tip for file and print services over LAST. If a DOS client can connect to a disk service on a particular server, then the network hardware and LAST have been proven to work between that server and that client. Thus, between that server and client, any problem with file and print services over LAST is a configuration or version problem.

Between a PATHWORKS for DOS Version 4.1 DOS client and a PATHWORKS for VMS Version 4.1 VMS server, a DOS client first attempts to make file service connections over LAST. Only on failing to make the connection over LAST will the DOS client attempt to make the connect over DECnet. To determine which transport (LAST or DECnet) was used to make a connection, at the DOS client, use the following steps:

1. Use the NCP command SHOW KNOWN LINKS to ensure that the DOS client is not currently connected over DECnet to any server.

   ```
   C:\> NCP SHOW KNOWN LINKS
   No known links
   Active Volatile Nodes as of 3-Jan-1991 1:44:15
   ```

2. Make the connection to the file or print service.

3. Again use the NCP command SHOW KNOWN LINKS. If a known link is listed for a server, the connection was made over DECnet. Otherwise, the connection was made over LAST. You can ignore any remote name other than "64". Only "64" names indicate a file or print service connection.

   ```
   C:\> NCP SHOW KNOWN LINKS

   Known Links Status as of 20-Jan-1991 19:27:09

   State        Socket  Node     Local   Remote  Local          Remote
                                 Addr    Addr    #   Name        #   Name

   Running      1       8.200    18304   8195    0   WKSONE      64
   ```

DOS Client Required Components Procedure (LAST)

The network components required for a DOS client depends on the following configuration criteria:

- The services that the client must use
- The connection method
- The data link used
- The client memory configuration

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

In addition to the network components, you need the troubleshooting diskette and the netsetup diskette. Verify that you have the following PATHWORKS for DOS Version 4.1 network components available locally, either on diskettes or on your hard disk:

- CONFIG.SYS
- SCH.EXE
- Data link components

  The required data link components can be either of two models:

  - The Digital-specific data link DLLDEPCA.EXE for the EtherWORKS family of network adapters
  - The Digital-specific data link interface DLLNDIS.EXE for Network Driver Interface Specification (NDIS) drivers, such as:

    a. DEPCA.DOS

    b. ELNKII.SYS

    c. ELNKMC.SYS

    d. Other certified, third-party NDIS data links

    In addition to the NDIS driver, PROTOMAN.SYS is required to manage the protocols and NETBIND.EXE is required to bind the protocol layers.
- LAST.EXE

- For disk services, the following are required:
  - LADDRV.SYS
  - LAD.EXE
- For file and print services, the following are required:
  - LANSESS.EXE
  - REDIR.EXE

    There are three versions of the redirector, REDIR.320, REDIR.330, and REDIR.400. Ensure that the version of the redirector matches the version of DOS on the client. Copy the correct version of the redirector, REDIR.320, REDIR.330, or REDIR.400 to REDIR.EXE.

  Although it is not required for LAST, you should also have the DECnet Network Process (DNP) component for your DOS client named DNNETH.

  If you want to load network components into nonconventional memory, you also need EMSLOAD.EXE.

- Ensure that all components are PATHWORKS for DOS Version 4.1 components by checking the dates on the files. The dates should be later than June, 1991.

Component Load Order

The order in which the components are loaded depends on the data link model that you have selected (DLLDEPCA.EXE or DLLNDIS.EXE).

Using DLLDEPCA.EXE

If you are using DLLDEPCA.EXE, the first executable component loaded must be SCH.EXE; the second executable component loaded must be DLLDEPCA.EXE. LAST must be loaded before LAD or LANSESS. LANSESS or DNNETH must be loaded before REDIR. Table 11–2 lists the CONFIG.SYS driver components and when they are required for this model.

Table 11–2 CONFIG.SYS Components Required With DLLDEPCA.EXE

Driver Component	Requirement
LASTDRIVE=Z	Required for file services over LAST or DECnet. This example indicates that all remaining logical drives up to Z are available. You may wish to set LASTDRIVE at a lower value (for example, M or S).
DEVICE=\HIMEM.SYS	Required if you want to load the redirector into expanded memory. This is not recommended during troubleshooting.
DEVICE=\LADDRV.SYS /D:4	Required for disk services. This example provides for four virtual disk drive letters. You may want to change the number of drive letters allocated to virtual disks.
SHELL=\COMMAND.COM /E:526 /P	Required for all configurations. The size of the environment that you require may be more or less than the 526 indicated in the example.

Using DLLNDIS.EXE

If you are using DLLNDIS.EXE, the first executable component loaded must be DLLNDIS. Then you must execute NETBIND.EXE. The second executable component loaded must be SCH.EXE. LAST must be loaded before LAD or LANSESS. LANSESS or DNNETH must be loaded before REDIR. Table 11–3 lists the CONFIG.SYS driver components and when they are required for this model.

Table 11–3 CONFIG.SYS Components Required with DLLNDIS.EXE

Driver Component	Requirement
LASTDRIVE=Z	Required for file services over LAST or DECnet. This example indicates that all remaining logical drives up to Z are available. You may wish to set LASTDRIVE at a lower value (for example, M or S).
DEVICE=\HIMEM.SYS	Required if you want to load the redirector into expanded memory. This is not recommended during troubleshooting.

(continued on next page)

Table 11–3 (Cont.) CONFIG.SYS Components Required with DLLNDIS.EXE

Driver Component	Requirement
DEVICE=\LADDRV.SYS /D:4	Required for disk services. This example provides for four virtual disk drive letters. You may want to change the number of drive letters allocated to virtual disks.
SHELL=\COMMAND.COM /E:526 /P	Required for all configurations. The size of the environment that you require may be more or less than the 526 indicated in the example.
DEVICE=\DECNET\PROTMAN.SYS /I:A:\DECNET\	Always required.
DEVICE=\DECNET\ELNKII.SYS	Always required.
	Only one of the following NDIS drivers, or another certified driver, is required.
DEVICE=\DECNET\DEPCA.DOS	NDIS driver for DEPCA and EtherWORKS Ethernet adapters.
DEVICE=\DECNET\ELNKII.SYS	NDIS driver for 3COM 3C503 Ethernet adapters.
DEVICE=\DECNET\ELNKMC.SYS	NDIS driver for 3COM 3C523 Ethernet adapters.

DOS Client Required Components Procedure Completion (LAST)

The DOS Client Required Components Procedure is complete. Successfully completing this procedure indicates that you have all of the network components required for network operation and troubleshooting on the DOS client.

DOS Client Memory Interaction Procedure (LAST)

This procedure provides a minimal checkout of LAST, disk services, and LAST file services. Use this procedure to identify problems caused by having some network components operating in nonconventional memory. Nonconventional memory can mean either expanded memory or extended memory.

Note

Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

The strategy in this procedure is to load client network components one at a time into conventional memory. After each component or set of components, the operation of the component or set of components is verified.

After the operation of the required components is proven in conventional memory, reboot the DOS client. Repeat the procedure with individual components loaded one-by-one into nonconventional memory.

Before performing this procedure, you should:

- Perform the steps in the VMS Server Master Procedure or otherwise verify that your server is configured and operating correctly.
- Be aware of the different types of memory available on your DOS client and where in memory your network components should be loaded. These concepts are covered in *Memory Solutions for Client Administrators*.
- Have access to a server account that has management privileges.
- Run Netsetup to create a STARTNET.BAT file and a DECNODE.TXT file.

The following is the DOS Client Memory Interaction Procedure. The command examples assume that you have loaded the required components into the subdirectory C:\ DECNET.

1. If your DOS client has been set up to use the high memory area (HMA) extended memory (XMS), reconfigure it to not do so. To do this, edit your CONFIG.SYS file and delete or comment out the line "device=himem.sys." Also delete or comment out any lines that enable the use of expanded memory.

2. Prevent your STARTNET.BAT file from automatically loading network components by renaming that file:

   ```
   C:\> CD C:\DECNET
   C:\DECNET> RENAME STARTNET.BAT STARTNET.BAK
   ```

3. Perform the DOS Client Transport Procedure (LAST).
4. Perform the DOS Client Disk Services Procedure (LAST).
5. Perform the DOS Client File and Printer Services Procedure (LAST).

At this point, you have verified the operation of the network with all DOS client's LAST components running in conventional memory. If you do not want to run any DOS client network component in extended or expanded memory, you are finished with this procedure.

If you want to run LAST.EXE, LAD.EXE, or REDIR.EXE in nonconventional memory, reenable the desired nonconventional memory model. Then:

1. Reboot the client.
2. Perform the previous numbered steps, but load one more components into nonconventional memory than was loaded in the previous repetition.

To load LAST.EXE into expanded memory, enter:

```
C:\DECNET> EMSLOAD LAST /N:node_name /M:E
```

To load LAD.EXE into expanded memory, enter:

```
C:\DECNET> EMSLOAD LAD /R:1 /W:1
```

To load REDIR.EXE into high memory, enter:

```
C:\DECNET> REDIR /L:10 /HIMEM:YES
```

Repeat this process until all of the desired components are loaded into nonconventional memory. For example, in repetition number 1, load all of the components except LAST.EXE into conventional memory and load LAST.EXE into nonconventional memory. For repetition number 2, load all of the components except LAST.EXE and LAD.EXE into conventional memory and load LAST.EXE and LAD.EXE into nonconventional memory.

If you discover a problem running a component in nonconventional memory, eliminate any nonessential drivers from CONFIG.SYS and eliminate any non-network related programs from AUTOEXEC.BAT. If that resolves the conflict, reenable one of the eliminated drivers and/or programs and reboot the DOS client. Repeat the process of reenabling a driver or program and rebooting until the conflict reappears. The last driver or program that was reenabled causes the conflict. You must then decide whether you want to leave the driver or program disabled or whether you want to run the affected network component in conventional memory.

DOS Client Memory Interaction Procedure Completion (LAST)

The DOS Client Memory Interaction Procedure is complete. Successfully completing this procedure indicates that you have eliminated any memory interactions that affected network operation on the DOS client.

DOS Client Transport Procedure (LAST)

This procedure verifies that LAST is operating correctly on a DOS client.

Note

> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

To confirm the operation of LAST:

1. Using the information in DOS Client Required Components Procedure (LAST), confirm that CONFIG.SYS contains the required lines for the DOS client's data link model.
2. Reboot your DOS client.
3. Load data link and scheduler according to the data link model for this DOS client. All components loaded in this step must always be loaded into conventional memory.

   If the DOS client uses DLLDEPCA.EXE, load the scheduler and the data link as follows:

   ```
   C:\DECNET> SCH /A
   C:\DECNET> DLLDEPCA /FAST
   ```

   If the DOS client uses DLLNDIS.EXE, load the data link , bind the protocols, and then load the scheduler as follows:

   ```
   C:\DECNET> DLLNDIS
   C:\DECNET> NETBIND
   C:\DECNET> SCH /A
   ```

4. Load the DOS client LAST component:

   ```
   C:\DECNET> LAST /N:node_name
   ```

   In the previous example, node_name is the DECnet node name of the DOS client.

5. To see a list of servers on the network that offer the service TESTER, enter:

   ```
   C:\DECNET> USE TESTER
   ```

   If a list of services is displayed, then the network is operating correctly, the servers listed are configured correctly, and the servers are offering the system service. Also, the client Ethernet hardware, data link layer, and transport layer are running.

If no list of services is displayed, isolate the network hardware problem using the procedures located in Isolating DECnet Problems.

DOS Client Transport Procedure Completion (LAST)

The DOS Client Transport Procedure is complete. Successfully completing this procedure indicates that the local area system transport is set up correctly on the DOS client.

DOS Client Disk Services Procedure (LAST)

This procedure confirms the operation of disk services on a DOS client.

> **Note**
>
> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

1. Load the DOS client virtual disk components:

   ```
   C:\DECNET> LAD /R:1 /W:1
   ```

2. Confirm that the required components are loaded:

   ```
   C:\DECNET> USE /STATUS
   ```

   If the DOS client response does not contain a "Virtual drives:" line, it is likely that CONFIG.SYS does not contain a "DEVICE = LADDRV.SYS" entry or that the location of LADDRV.SYS is incorrectly specified.

3. Use the first available virtual drive letter to connect to the service TESTER.

   ```
   C:\DECNET> USE drive_letter: TESTER
   ```

   If you cannot connect to the service, either LAD.EXE was not loaded or the disk server is not operating correctly on the server.

DOS Client Disk Services Procedure Completion (LAST)

The DOS Client Virtual Disk Procedure is complete. Successfully completing this procedure indicates that the virtual disk components are set up correctly on the DOS client.

DOS Client File and Printer Services Procedure (LAST)

This procedure confirms the operation of file services on LAST.

Note

> Any PATHWORKS terminate and stay resident (TSR) program must be loaded first before you can invoke a task switcher, such as the DOS Version 5 DOSSHELL program, or any shell program, such as Microsoft Windows.

- Load LANSESS and the redirector. Enter:

  ```
  C:\DECNET> LANSESS /R:1 /W:1
  C:\DECNET> REDIR /L:10
  ```

- Connect to the system service PCSAV40 by entering:

  ```
  C:\DECNET> USE M: \\host_name\PCSAV40
  ```

  In the previous example, *host_name* is the DECnet node name of the server. In the previous example, *host_name* would be replaced by the example server VVSRV.

- Confirm the connection to the service as follows:

  ```
  C:\DECNET> USE
  ```

  If you cannot connect to the file service PCSAV40, ensure that the file server is operating correctly on the server.

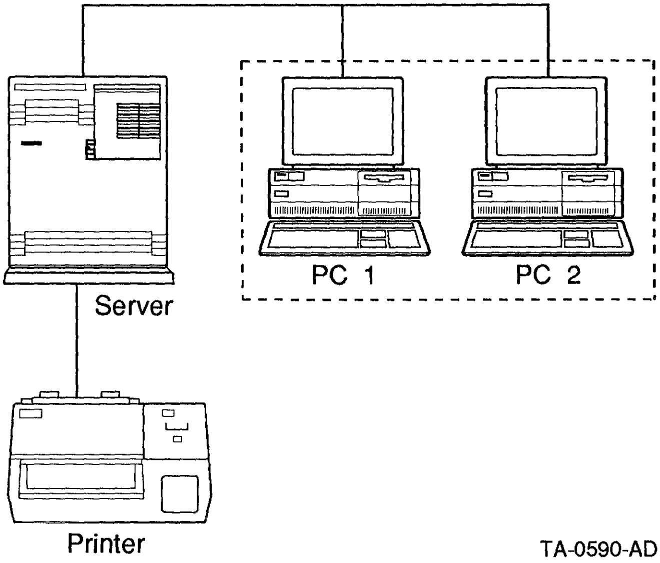
DOS Client File and Print Services Procedure Completion (LAST)

The DOS Client File and Printer Services Procedure is complete. Successfully completing this procedure indicates that the file and printer services over LAST are set up correctly on the DOS client.

DOS Client Master Procedure Completion (LAST)

The DOS Client Master Procedure is complete. If successful, you know that the DOS client on your network, shown in Figure 11–9, is set up correctly.

Figure 11–9 DOS Client Set Up Correctly



OS/2 Client Master Procedure (LAST)

The OS/2 Client Master Procedure (LAST) contains the following procedures:

- OS/2 Client Required Components Procedure
- OS/2 Client Transport Procedure
- OS/2 Client Disk Services Procedure
- OS/2 Client File and Printer Services Procedure

Use these procedures to verify that your OS/2 client is operational. To perform these tests, boot the OS/2 client with the key diskette. Then perform the indicated test.

If you cannot successfully perform the OS/2 Client Transport Procedure (LAST), you will be required to confirm that no server or client network hardware problems exist. The procedures used to isolate network hardware problems are located in Isolating DECnet Problems.

Troubleshooting Considerations

PATHWORKS for OS/2 Version 1.1 includes a wider variety of options for configuration of network software than previous versions. The OS/2 client user can choose not to load certain components at all or to load and unload them as needed. In general, the procedures include steps to ensure that the components required for correct operation of each type of service are present.

When you are troubleshooting LAST, always set the read (/R:1) and write (/W:1) transaction size to 1. Doing so precludes packet congestion (data overrun) at the client adapter. If you are troubleshooting a new network, it also precludes packet congestion at the server adapter until multiple clients are operating on the network.

OS/2 Client Required Components Procedure (LAST)

Verify that you have the following PATHWORKS for OS/2 Version 1.1 network components available locally on your hard disk:

- CONFIG.SYS
- PROTMAN.OS2
- DEPCA.OS2
- DLLMAC.SYS
- LASTDD.SYS
- LADDRV.SYS
- Network Driver Interface Specification (NDIS) drivers like:
  - DEPCA.OS/2
  - ELNKII.SYS
  - ELNKMC.SYS
  - Other certified, third-party NDIS data link
- NETBIND.EXE
- LASTCP.EXE

Although it is not required for LAST, you should also have the following DECnet Network Process (DNP) and Local Area Transport (LAT) components for your OS/2 client:

- NETDRV.SYS
- RDRHELP.SYS

- NETWKSTA.SYS
- MOP.EXE
- DNP.EXE
- SPAWNER.EXE
- LATCP.EXE
- NET.EXE
- DNETDLL.DLL
- MOPCALLS.DLL
- LATCALLS.DLL

Ensure that all components are PATHWORKS for OS/2 Version 1.1 components by checking the dates on the files. The dates should be later than October 1990.

Component Load Order

The order in which the components are loaded is important.

Within CONFIG.SYS, the network driver components should be listed in the following order:

- PROTMAN.OS2
- DEPCA.OS2
- DLLMAC.SYS
- NETDRV.SYS
- LASTDD.SYS
- LADDRV.SYS
- RDRHELP.SYS
- NETWKSTA.SYS

Note

> If LAN Manager is started, NETWKSTA.SYS binds the protocol layers and NETBIND.EXE does not appear in PCSAOS2.CMD. Otherwise, NETBIND.EXE binds the protocol layers and does appear in PCSAOS2.CMD.

The executable network components should be loaded in the following order:

- NETBIND.EXE
- MOP.EXE
- DNP.EXE
- SPAWNER.EXE
- LATCP.EXE
- LASTCP.EXE
- NET START WORKSTATION (NET.EXE)

OS/2 Client Required Components Procedure Completion (LAST)

The OS/2 Client Required Components Procedure is complete. Successfully completing this procedure indicates that you have all of the network components required for network operation and troubleshooting on the OS/2 client.

OS/2 Client Transport Procedure (LAST)

To confirm the operation of LAST:

1. Using the information in OS/2 Client Required Components Procedure (LAST), confirm that CONFIG.SYS contains the required lines for the OS/2 client as follows:

   ```
   DEVICE=C:\PCSAOS2\DEV\PROTMAN.OS2 /I:C:\PCSAOS2\DEV
   DEVICE=C:\PCSAOS2\DEV\DEPCA.OS2
   DEVICE=C:\PCSAOS2\DEV\DLLMAC.SYS
   DEVICE=C:\PCSAOS2\DEV\LASTDD.SYS
   DEVICE=C:\PCSAOS2\DEV\LADDRV.SYS /D:4
   ```

2. Confirm that the CONFIG.SYS LIBPATH, PATH, and DPATH point to the network components. For example, LIBPATH should point to C:\PCSAOS2\DLL and PATH and DPATH should both point to C:\PCSAOS2\PBIN.

3. Using the OS/2 System Editor, edit the file STARTUP.CMD. Place a REM statement at the beginning of the line that calls PCSAOS2.CMD.

   ```
   REM call C:\PCSAOS2\PCSAOS2.CMD
   ```

4. Reboot your OS/2 client.

5. Bind the network protocols as follows:

   ```
   [C:\] NETBIND
   ```

6. Start LAST as follows:

   ```
   [C:\] DETACH C:\PCSAOS2\PBIN\LASTCP /N=node_name
   ```

   In the previous example, *node_name* is the DECnet node name of the OS/2 client.

7. To see a list of servers on the network that offer the service TESTER, enter:

   ```
   [C:\] USE TESTER

   USE Version V1.1.04 PCSA Network Connection Manager

   Service information for TESTER

                Service  Password  Access   Maximum   Current
   Node Name    Rating   Required  Mode     Connects  Connects  Network Address
   ---------    -------  --------  -------  --------  --------  -----------------
   VVSRV              1     No        RW          1         0   AA-00-04-00-48-25
   ```

   If a list of services is displayed, then the network is operating correctly, the servers listed are configured correctly and are offering the system service. Also, the client Ethernet hardware, data link layer, and transport layer are running.

   If no list of services is displayed, isolate the network hardware problem using the procedures located in Isolating DECnet Problems in this manual.

OS/2 Client Transport Procedure Completion (LAST)

The OS/2 Client Transport Procedure is complete. Successfully completing this procedure indicates that the local area system transport is set up correctly on the OS/2 client.

OS/2 Client Disk Services Procedure (LAST)

To confirm the operation of disk services, perform the following steps:

1. Confirm that the OS/2 client virtual disk components are loaded:

```
[C:\] USE /STATUS

USE Version V1.1.04 PCSA Network Connection Manager
Copyright (c) 1989, 1990 by Digital Equipment Corporation

Component Information

    Datalink version 1.2.2 is installed
    LAST version 1.11 is installed
    LAD version 1.10 is installed

Client Information

    Station address:   AA-00-04-00-84-27
    Hardware address:  08-00-2B-14-CB-75
    Ethernet hardware: OS/2 NDIS Driver

    Physical drives:    8 (A:-H:)
    Logical drives:    26 (A:-Z:)
    Virtual drives:     4 (E:-H:)
```

   In the previous example, the first available virtual drive letter is E. If the OS/2 client response does not contain a "Virtual drives:" line, it is likely that CONFIG.SYS does not contain a "DEVICE = LADDRV.SYS" entry or that the location of LADDRV.SYS is incorrectly specified.

2. Use the first available virtual drive letter to connect to the service TESTER.

```
[C:\] USE E: TESTER

[C:\] USE
USE Version V1.1.04  PCSA Network Connection Manager     [Virtual drives E:-H:]

Status  Dev   Type  Connection name                       Mode     Size
------  ---   ----  ------------------------------------  -------  -------
        E:    DISK  \\VVSRV\TESTER                        RW FAST  1.20 MB
```

   If you cannot connect to the service, the disk server is not operating correctly on the server.

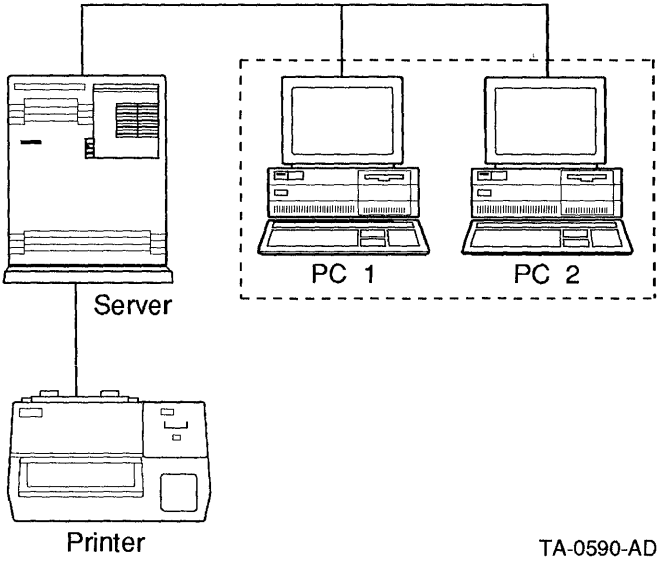
OS/2 Client Disk Services Procedure Completion (LAST)

The OS/2 client Disk Services Procedure is complete. Successfully completing this procedure indicates that the virtual disk components are set up correctly on the OS/2 client.

OS/2 Client Master Procedure Completion (LAST)

The OS/2 Client Master Procedure is complete. If successful, you know that the OS/2 client on your network, shown in Figure 11–10, is set up correctly.

Figure 11–10 OS/2 Client Set Up Correctly



Network Connection Procedure

This procedure must be performed using DECnet tools. If you have not installed DECnet on the client, you should perform the Client Master Procedure for DECnet. Then perform the Network Connection Procedure for DECnet.

Network Segment Interface Procedure

This procedure must be performed using DECnet tools. If you have not installed DECnet on the client, you should perform the Client Master Procedure for DECnet. Then perform the Network Segment Interface Procedure for DECnet.

12 LAST Messages

This chapter contains LAST-related messages and local area disk (LAD) messages. Although VMS and DOS support file and print services over LAST, this chapter does not contain file and printer services related messages. File and printer services related messages can be found in Chapter 3 and *Server Messages*.

This chapter is divided into three hardware/operating system sections:

- LAST-Related Messages on VMS
- LAST-Related Messages on DOS
- LAST-Related Messages on OS/2

Each operating system section is further divided by software component.

LAST-Related Messages on VMS

This section contains messages generated:

- By the LAST Control Program (LASTCP). These messages are listed alphabetically and followed by an explanation and advice.
- By LAD$KERNEL. These messages are displayed in the disk server's log file, which is in the directory represented by LAD$LOG_FILES. These messages can also be displayed with PCSA MANAGER messages.

LASTCP Messages

The following messages are generated by LASTCP.

%LASTCP-E-ASSIGNERR, Error assigning unit 'ddcu'

Severity: Error

Explanation: LASTCP was unable to assign the specified device. The reason LASTCP could not assign it is described in the VMS error message also displayed.

User Action: Check the VMS error message also displayed.

%LASTCP-E-DRVRALRSTRT, LASTDRIVER is already started

Severity: Error

Explanation: You attempted to start LASTDRIVER when it was already started.

User Action: None

%LASTCP-E-ERRSETQUO, Error setting process quotas

Severity: Error

Explanation: LASTDRIVER could not set process quotas. You must have CMKRNL (change mode to kernel) privilege to set process quotas.

User Action: Ensure that you have this privilege, and enter the command again.

%LASTCP-E-INVQUOTA, Invalid transmit quota 'x'

Severity: Error

Explanation: The value you specified for the transmit quota is not correct.

User Action: Use a valid quota in the range 1 to 255.

%LASTCP-E-IVCMD, Invalid command

Severity: Error

Explanation: The command you entered is not a valid LASTCP command.

User Action: Check the command syntax and enter it again.

%LASTCP-E-IVQUAL, Value for qualifier 'name' is invalid as 'x'

Severity: Error

Explanation: The value you specified for a qualifier or parameter is invalid.

User Action: Check the command's description and enter the command again.

%LASTCP-E-NOCONTROL, Controller ‘letter’ is not active

Severity: Error

Explanation: The Ethernet controller that you specified is not running or does not exist.

User Action: If the Ethernet controller is not running, initialize it and enter the command again. The default controller is A.

%LASTCP-E-NODEVFOUND, No Ethernet device found - use LAST$DEVICE

Severity: Error

Explanation: The Ethernet device is not defined to LASTCP.

User Action: You must specify the Ethernet device using the logical LAST$DEVICE.

%LASTCP-E-NONODNAM, Node name required to start transport

Severity: Error

Explanation: LASTDRIVER could not determine the VAX computer’s DECnet node name.

User Action: If DECnet is not running, specify the /NODENAME qualifier with the LASTCP START TRANSPORT command.

%LASTCP-E-NOSUCHNODE, Node ‘name’ not found

Severity: Error

Explanation: The specified node name is not known to LASTDRIVER.

User Action: Enter a valid node name.

%LASTCP-E-NOTINITED, LASTDRIVER controller init not called

Severity: Error

Explanation: The transport is loaded, but the controller did not initialize.

User Action: Restart the driver by running the LAD_STARTUP.COM file.

%LASTCP-E-NOTLOADED, LASTDRIVER is not loaded

Severity: Error

Explanation: The transport is not loaded.

User Action: Run the LAD_STARTUP.COM file to load the transport.

%LASTCP-E-NOTSTARTED, LASTDRIVER not started

Severity: Error

Explanation: To use the command you entered, LASTDRIVER must be started.

User Action: Start LASTDRIVER with the LASTCP START TRANSPORT command.

%LASTCP-E-NOTSTOPPED, LASTDRIVER not stopped

Severity: Error

Explanation: LASTCP could not stop the transport.

User Action: You may not have the correct privileges, or the device may be off line. Check the VMS error messages also displayed.

%LASTCP-E-STRTERR, Error initializing 'ddcu' for LASTDRIVER

Severity: Error

Explanation: LASTDRIVER could not initialize the port for the specified controller.

User Action: The controller may be unplugged, or another hardware problem may exist. Check the controller and enter the command again.

%LASTCP-E-VERSERR, LASTDRIVER version mismatch

Severity: Error

Explanation: The version of LASTDRIVER does not match the version of LASTCP.

User Action: Determine which component is running the latest version, and use the new version of the other component.

LAD$KERNEL Messages

The following messages are generated by LAD$KERNEL. Some messages are displayed individually, but are actually one of a pair of messages. The other message may come from PCSA Manager or VMS. For more information on the PCSA Manager message, see the PCSA Manager messages in *Server Messages*. For more information on the VMS message, see the VMS documentation set.

%LAD-E-DISMOUNTFAILED Dismount request failed

Severity: Error

Explanation: The service that you tried to dismount was not dismounted.

User Action: Check the other message displayed.

%LAD-E-DUPSERVNAM Duplicate service name detected

Severity: Error

Explanation: The service name that you specified already exists.

User Action: Enter the command again using another service name.

%LAD-E-INVACCMODE Invalid access mode specified

Severity: Error

Explanation: An invalid access mode was specified.

User Action: Access modes can be either READ or WRITE. Other access modes are not allowed. Enter the command again and specify the correct mode.

%LAD-E-INVPASS Invalid password specified

Severity: Error

Explanation: The password that you specified is incorrect.

User Action: Enter the command again using the correct password.

%LAD-E-MOUNTFAILED Mount request failed

Severity: Error

Explanation: LAD$KERNEL could not mount the requested virtual disk.

User Action: Check the other message displayed and try the command again.

%LAD-E-NOCACHE Server cache not set

Severity: Error

Explanation: The disk server's cache is not set because the driver is not started.

User Action: Set the cache to start the driver.

%LAD-E-NOSERVERDATAB Couldn't find server database file

Severity: Error

Explanation: LAD$KERNEL could not find the disk server's service database, SYS$COMMON:[PCSA]LAD$SERVICE_DATABASE.DAT.

User Action: Ensure that the database, SYS$COMMON:[PCSA]LAD$SERVICE_DATABASE.DAT exists. Then, enter the command again.

%LAD-E-NOSUCHSERVICE Service name not found

Severity: Error

Explanation: The service name that you specified is not in the disk server's service database.

User Action: Either add a service with that name, or enter the correct service name.

%LAD-E-NOTMOUNTED Service is not mounted

Severity: Error

Explanation: The service you tried to dismount is not mounted.

User Action: Check the name of the service and enter the command again. Also, check the VMS message displayed.

%LAD-E-REMOUNTFAILED Cannot remount permanent services

Severity: Error

Explanation: LAD$KERNEL could not remount the permanent services.

User Action: Check the other message displayed.

%LAD-E-SETFAILED Set request failed

Severity: Error

Explanation: The PCSA SET DISK_SERVER SERVICE command failed to set the requested characteristic.

User Action: Check the other message displayed.

%LAD-E-SHOWFAILED Show request failed

Severity: Error

Explanation: The PCSA SHOW DISK_SERVER command failed to display the requested information.

User Action: Check the other message displayed.

%LAD-E-SPURIOUSDISMOUNT Spurious dismount request

Severity: Warning

Explanation: You attempted to dismount a virtual disk that is currently being dismounted. The disk is dismounted correctly.

User Action: None

%LAD-E-WAITING Waiting for DECnet/VAX

Severity: Error

Explanation: You tried to start the disk server, but DECnet/VAX is not running.

User Action: To start the disk server, DECnet/VAX must be running. To start DECnet/VAX, use the command procedure SYS$MANAGER:STARTNET.COM. If you have not included a call to LAD$STARTUP.COM in SYS$MANAGER:STARTNET.COM, start the disk server using the LAD$STARTUP.COM file.

%LAD-E-ZEROFAILED Zero request failed

Severity: Error

Explanation: The PCSA ZERO DISK_SERVER COUNTERS command failed to zero the requested counters.

User Action: Check the other displayed message.

LAD Log File Messages

When generated, the following LAD$KERNEL messages can be found in the log files LAD$LOG_FILES:LAD$KERNEL.LOG and/or LAD$LOG_FILES:LAD$KERNEL_ERROR.LOG.

Cannot remount permanent services

Severity: Error

Explanation: Either of the following occurred:

- The file could not be locked.
- The memory could not be allocated.

User Action: Do either of the following:

- Make sure the LAD$KERNEL process has sufficient ENQ quota for the number of services being mounted.
- Restart LAD$KERNEL with a larger PGFLQUOTA or increase the SYSGEN parameter VIRTUALPAGECNT and reboot the system.

Error creating channel to device

Severity: Error

Explanation: You issued a dismount request, but the service could not be dismounted because the device associated with the file no longer exists.

User Action: See the associated message for more information about what action to take.

Error deleting mailbox

Severity: Error

Explanation: You ran the STOP DISK CONNECTIONS command, but the mailbox could not be deleted.

User Action: See the associated message for more information about what action to take.

Error dismounting service

Severity: Error

Explanation: You issued a dismount request, but the entry for that service in the service database could not be found.

User Action: See the associated message for more information about what action to take.

Error mounting service

Severity: Error

Explanation: Any of the following occurred:

- The record in the service database could not be found.
- The node entry for the record does not exist in the node database
- The service database could not be locked.
- An update to the service database failed.

User Action: Do any of the following:

- For the first two explanations, rebuild LAD$SERVICE_DATABASE using SYS$COMMON:[PCSA]LAD$SERVICE_DATABASE.FDL.
- For the third explanation, make sure the LAD$KERNEL process has sufficient ENQ quota for the number of services being mounted.
- For the fourth explanation, see the associated message for more information about what to do.

Error posting mailbox read

Severity: Error

Explanation: An error occurred between the PCSA Manager and the LAD kernel.

User Action: See the associated message for more information about what action to take.

Error reading input mailbox

Severity: Error

Explanation: The LAD kernel could not read the input mailbox.

User Action: See the associated message for more information about what action to take.

Error reading permanent mailbox

Severity: Error

Explanation: An error occurred reading the permanent mailbox.

User Action: Restart the LAD kernel.

Error writing mailbox

Severity: Error

Explanation: An error occurred between the PCSA Manager and the LAD kernel.

User Action: See the associated message for more information about what action to take.

Invalid database file, please rebuild

Severity: Error

Explanation: There is a version discrepancy between the LAD kernel and the LAD kernel database.

User Action: Reinstall the LAD software.

Invalid protocol

Severity: Error

Explanation: There is a version discrepancy between the PCSA Manager and the LAD kernel.

User Action: See the associated message for more information about what action to take.

LAST-Related Messages on DOS

This section contains messages generated by:

- LAST.EXE
- LADDRV.SYS
- LAD.EXE
- LANSESS.EXE

Many of the user actions indicate making changes to CONFIG.SYS, AUTOEXEC.BAT, and STARTNET.BAT. After making changes to one of those files, you must reboot the computer for the change to have an affect.

Messages Generated by LAST

The following messages are generated by LAST.

/C requires Enable or Disable, leaving disabled

Severity: Warning

Explanation: An invalid checksum switch value was specified on the LAST command line.

User Action: Reissue the command with a valid value following the /C: switch. The valid values are "E" (for enable) and "D" for disable. An example of a valid command is "LAST /C:E".

/M requires Enable or Disable, leaving enabled

Severity: Warning

Explanation: An invalid multicast switch value was specified on the LAST command line.

User Action: Reissue the command with a valid value following the /M: switch. The valid values are "E" (for enable) and "D" for disable. An example of a valid command is "LAST /M:E".

Datalink not installed

Severity: Error

Explanation: The data link was not installed prior to running LAST.EXE.

User Action: Ensure that STARTNET.BAT has not been changed and that it invokes DLLDEPCA.EXE or DLLNDIS.EXE. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Datalink portal failed to open

Severity: Error

Explanation: LAST.EXE tried to open a data link portal (a communications channel) and the operation failed.

User Action: Under normal conditions, this message should not occur. If you are running locally developed TSR programs that use the data link, remove them before starting LAST. If those efforts fail to correct the problem, contact your Digital representative.

Invalid group code specified

Severity: Error

Explanation: An invalid group code was specified on the LAST command line.

User Action: Reissue the command with a valid value following the /G: switch. Valid values are in the range 0 to 255.

Last driver DOS TSR call failed - LAST NOT INSTALLED

Severity: Error

Explanation: LAST.EXE called the DOS Terminate and Stay Resident (TSR) function. The DOS TSR function returned an error.

User Action: Under normal conditions, this message should not occur. It is likely that an application or TSR program has interfered with the correct operation of DOS. Ensure that AUTOEXEC.BAT does not start any TSR programs or applications before running STARTNET.BAT. If those efforts fail to correct the problem, contact your Digital representative.

Loaded into EMS

Severity: Informational

Explanation: LAST was loaded into EMS memory.

User Action: No action is required.

Scheduler not installed

Severity: Error

Explanation: The scheduler was not installed prior to running LAST.EXE.

User Action: Ensure that STARTNET.BAT has not been changed and that it invokes SCH.EXE. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Setting New Group Code

Severity: Informational

Explanation: LAST.EXE was run with a valid /G:'n' switch.

User Action: No action is required.

Unable to determine node name, use /N:name or load DNP

Severity: Error

Explanation: LAST.EXE was started before DNP.EXE was loaded and the node name switch /N: was not entered on the LAST command line.

User Action: Reissue the LAST command line with a node name switch or start DNP before attempting to start LAST. For example, to start LAST before DNP, if the DECnet node name is WKSONE, type "LAST /N:WKSONE".

LADDRV.SYS Messages

The following messages are generated by LADDRV.SYS.

Configured n LAD disks as drives A - A

Severity: Informational

Explanation: When LADDRV.SYS was initialized, n drives letters were allocated for use with virtual disk drives. The "A - A" string indicates the range of the letters that were allocated.

User Action: No action is required.

Invalid LADDRV.SYS switch or value

Severity: Error

Explanation: An invalid switch or switch value was entered on the (DEVICE = LADDRV.SYS /D:n) line in CONFIG.SYS.

User Action: Edit CONFIG.SYS and correct the drive switch /D:n. The valid values for n are a number in the range of 1 to 8. The default value is four.

LAD Messages

The following messages are generated by LAD.

Datalink is not installed

Severity: Error

Explanation: The data link was not installed prior to running LAD.EXE.

User Action: Ensure that STARTNET.BAT has not been changed and that it invokes DLLDEPCA.EXE or DLLNDIS.EXE. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Invalid parameter

Severity: Error

Explanation: An invalid parameter was entered on the LAD command line. When this occurs, LAD displays the allowed switches and usage. The full text of the message is as follows:

```
Invalid parameter

Usage: LAD [/R:n] [/W:n] [/A:x]
Where: /R:n  sets read transaction size from 1 to 15
       /W:n  sets write transaction size from 1 to 15
       /A:x  sets click; E for enabled, D for disabled
```

User Action: Reenter the LAD command line with the correct switches and values.

LAST is not installed

Severity: Error

Explanation: LAST was not installed prior to running LAD.EXE.

User Action: Ensure that STARTNET.BAT has not been changed and that it invokes LAST.EXE. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Loaded into EMS

Severity: Informational

Explanation: LAD was loaded into EMS memory.

User Action: No action is required.

LANSESS Messages

The following messages are generated by LANSESS.EXE.

LANSESS already installed

Severity: Informational

Explanation: LANSESS.EXE was already loaded and started.

User Action: No action is required.

LANSESS installed

Severity: Informational

Explanation: LANSESS.EXE was loaded and started.

User Action: No action is required.

LANSESS not installed

Severity: Error

Explanation: LANSESS.EXE was not installed and was not started.

User Action: For LANSESS to start, LAST.EXE must be running and it is likely that LAST.EXE was not installed. Ensure that LAST.EXE is invoked before LANSESS.EXE. This may require you to edit STARTNET.BAT.

LAST-Related Messages on OS/2

This section contains messages generated by:

- LASTCP.EXE
- LASTDD.SYS
- LADDRV.SYS

LASTCP Messages

The following messages are generated by LASTCP.

Could not open file 'filename'.

Severity: Error

Explanation: LASTCP could not open the indicated file.

User Action: Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Counters have been zeroed.

Severity: Informational

Explanation: You issued the LASTCP command to zero the counters.

User Action: No action is required.

Illegal value 'x' for /x switch.

Severity: Error

Explanation: A LASTCP command was issued with an invalid value for the indicated switch.

User Action: Refer to the user documentation and reissue the command with the correct value.

LAD or LAST driver not loaded, press any key to continue.

Severity: Error

Explanation: A LASTCP command was issued and LADDRV.SYS or LASTDD.SYS was not installed.

User Action: Ensure that LADDRV.SYS and LASTDD.SYS are correctly entered in CONFIG.SYS.

LAST driver initialization error, error code: n.

Severity: Error

Explanation: LASTCP could not initialize LASTDD.SYS or LADDRV.SYS

User Action: Running NETSETUP.EXE will ensure that the components are in the correct location and that the are invoked correctly.

The LAD/LAST drivers have been stopped.

Severity: Informational

Explanation: You issued the LASTCP shutdown command.

User Action: No action is required.

There are active sessions. Continue shutdown? (Yes/No) [NO]:

Severity: User Response

Explanation: When you issued the LASTCP shutdown command, there were one or more active connections to virtual disk drives.

User Action: If you want to disconnect the drives and shut down LAST enter YES. Otherwise, enter NO.

Unable to create shutdown semaphore, error code: n.

Severity: Error

Explanation: An error occurred between OS/2 and LASTCP.

User Action: Reboot OS/2 and then start the network software.

Unable to obtain information about current process.

Severity: Error

Explanation: An error occurred between OS/2 and LASTCP.

User Action: Reboot OS/2 and then start the network software.

Unable to determine DECnet node name.

Severity: Error

Explanation: LASTCP.EXE was started before DNP.EXE was loaded and the node name switch /N: was not entered on the LASTCP command line.

User Action: Reissue the LASTCP command line with a node name switch or start DNP before attempting to start LASTCP. For example, to start LASTCP before DNP, if the DECnet node name is WKSONE, type "LASTCP /N:WKSONE".

Value n for /x switch is out of range [n:n].

Severity: Error

Explanation: You issued a LASTCP command with an invalid value for the indicated switch.

User Action: Refer to the user documentation and reissue the command with the correct value.

LASTDD.SYS Messages

The following messages are generated by LASTDD.SYS. Many of the user actions indicate making changes to CONFIG.SYS. After making changes to CONFIG.SYS, you must reboot the computer.

Data Link driver communication error.

Severity: Error

Explanation: The data link was not loaded and started before LASTDD.SYS.

User Action: Ensure that CONFIG.SYS contains the line DEVICE = DLLMAC.SYS and that the line DEVICE = LASTDD.SYS occurs after the line containing DLLMAC.SYS. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Initialization Failure.

Severity: Error

Explanation: The data link was not loaded and started before LASTDD.SYS or there was an OS/2 problem.

User Action: Ensure that CONFIG.SYS contains the line DEVICE = DLLMAC.SYS and that the line DEVICE = LASTDD.SYS occurs after line containing DLLMAC.SYS. Running NETSETUP.EXE will ensure that the components are in the correct location and that the are invoked correctly.

LADDRV Messages

The following messages are generated by LADDRV.SYS.

Initialization Failure.

Severity: Error

Explanation:

User Action:

Installed n LAD disks as drives A - A.

Severity: :

Explanation: When LADDRV.SYS was initialized, n drives letters were allocated for use with virtual disk drives. The "A - A" string indicates the range of the letters that were allocated.

User Action: No action is required.

Installed 1 LAD disk as drive A.

Severity:

Explanation: When LADDRV.SYS was initialized, one drive letter was allocated for use with virtual disk drives. The "drive A" string indicates the letter that was allocated.

User Action: No action is required.

Switch '/D' value out of range, using default.

Severity: Error

Explanation: An invalid switch value was entered on the DEVICE = LADDRV.SYS /D:n line in CONFIG.SYS.

User Action: Edit CONFIG.SYS and correct the drive switch /D:n. The valid values for n are a number in the range of 1 to 8. The default value is four.

Unable to open LAST device driver.

Severity: Error

Explanation: The LAST device driver was not started.

User Action: Ensure that CONFIG.SYS contains the line DEVICE = LASTDD.SYS and that the line DEVICE = LADDRV.SYS occurs after the line containing LASTDD.SYS. Running NETSETUP.EXE will ensure that the components are in the correct location and that they are invoked correctly.

Unrecognized switch '/x' on command line in config.sys file.

Severity: Error

Explanation: An invalid switch was entered on the DEVICE = LADDRV.SYS /D:n line in CONFIG.SYS.

User Action: Edit CONFIG.SYS and correct the drive switch /D:n. The valid values for n are a number in the range of 1 to 8. The default value is four.

Part 5

Appendixes

A

Routing Layer Events

This appendix provides a list of the DECnet routing layer events (error messages). The following specific event classes and types are supported for the routing layer. Only those events and entire event classes marked with an asterisk (*) are logged by DECnet-VAX components.

*2.0 Aged packet loss**

Routing discarded a packet because it had visited too many nodes. This can be a normal occurrence when the network is reconfiguring its routing database. It can be a failure when the MAXIMUM HOPS value is set too small. This can cause the MAXIMUM VISITS value to be too small for a path that should be usable.

This message displays the name of the line to which the event applies, with one event qualifier - the packet header. This is information from the beginning of the packet. For non-Ethernet packets, it consists of a hexadecimal byte of flags, the decimal destination and source node addresses, and a hexadecimal byte of forwarding data. For Ethernet packets, it also includes the Ethernet address of the destination and source, the service type, and the protocol type.

*2.1 Node unreachable packet loss**

Routing discarded a packet because the local node found that the destination node was unreachable. This event provides a trace of what has happened to packets that are not reaching their destination.

This message displays the name of the line to which the event applies, with one event qualifier: the packet header (as described for event 2.0).

*2.2 Node out-of-range packet loss**

Routing discarded a packet because the destination node number was greater than the maximum node number known to the local node. Typically, this results from the addition of a new node to the network without increasing the MAXIMUM ADDRESS value on the local node, yet expecting the local node to route packets to the new node.

This message displays the name of the line to which the event applies, with one event qualifier: the packet header (as described for event 2.0).

*2.3 Oversized packet loss**

Routing discarded a packet because it was too large to forward to the appropriate adjacent node. Typically, this occurs when the adjacent nodes' buffer size is too small or when the source node sends a packet that is too large.

This message displays the name of the line over which the packet was to be forwarded, with one event qualifier, the packet header (as described for event 2.0).

*2.4 Packet format error**

Routing discarded a packet because of a format error in the packet header. This usually results from a programming error in the packet formatting by the adjacent node, though it could result from a line error that was not detected by the line protocol.

This message displays the name of the line to which the event applies, with one event qualifier: the packet beginning. This consists of the first six bytes of the packet, displayed as hexadecimal.

*2.5 Partial routing update loss**

Routing received a routing message that contained node addresses greater than the maximum addresses known to the local node. Subsequently, information on these nodes was lost. This occurs when the MAXIMUM ADDRESS value on the adjacent node has been increased to accommodate more nodes, but the local node's has not.

This message displays the name of the line over which this message was received, with two event qualifiers: the packet header (as described for event 2.0) and the highest node address in the routing update that was lost.

*2.6 Verification reject**

An attempt to initialize with another node failed. The local node received an invalid password in the verification requested of the adjacent node during routing initialization over the line. Either the local node expected the wrong received password, or the adjacent node sent the wrong transmit password.

This message displays the name of the line to which the event applies, with one event qualifier: the address of the adjacent node that failed to initialize.

*2.7 Circuit down, circuit fault**

An error has occurred for the circuit. This message displays the name of the circuit to which the event applies, along with one event qualifier: the reason for the event. The reason could be one of the following:

- Adjacent node address change

  The adjacent node changed addresses without going through the normal initialization sequence. This is also logged when an adjacent node attempts to initialize with the local node, but the address of the adjacent node is not in the database.

- Adjacent node address out of range

  The adjacent node's address is greater than the maximum address defined for the local node. This may be caused by an incorrectly defined node address or by a failure to update the local node's database when a new node was added.

- Adjacent node block size too small

  The line block size provided by the adjacent node is too small for normal network operations. The block size may be set incorrectly at the adjacent node.

- Adjacent node listener received timeout

  The node has received no message over the data link within the last 30 seconds. This usually means that the remote node is not running.

- Adjacent node listener received invalid data

  A test message sent by the adjacent node contained invalid or corrupted data. This is most likely caused by a hardware problem.

- Call failed

  An outgoing SVC call failed. This is an X.25 event.

- Data errors

  The line was declared down by the line protocol of the local node handler when the line exceeded an error threshold.

- Dropped by adjacent node

  The adjacent node was responsible for breaking the circuit connection.

- Invalid verification seed value

  A routing initialization message sent by an adjacent node is not formatted properly. This is most likely caused by a remote network software problem.

- Line synchronization lost

  The normal line protocol was restarted or terminated by the adjacent node. Either a line exceeded an error threshold, or network management initiated a line state change. DMR/DMC failures that cause a line synchronization error are as follows:

  - Threshold errors, including more than eight attempts to transmit a message, or eight NAKs received in a row.
  - Start message received in the on state (that is, the remote system detected an error and restarted the line).
  - Maintenance requested while in the on state (that is, the remote system tried to perform a maintenance operation, such as LOOP CIRCUIT).
  - Message was lost because no buffer was available in CPU memory.
  - Nonexistent memory error.
  - Procedure error, because of driver failure or hardware failure.
  - Timeout on request to transmit a message in 255 seconds.
  - Power failure.

- Routing update checksum error

  A routing update packet failed its internal integrity test.

- Unexpected packet type

  A packet was received out of the normal protocol sequence. For example, the local node received a normal packet when it expected a verification packet.

- Verification password required from Phase III node

  A required routing verification password was not specified before an attempt was made to initialize the Phase III node in a Phase IV network.

- Verification received timeout

  A required verification password was not received from the adjacent node within the required response time. Either packets were lost on the line or a failure occurred at the adjacent node.

- Version skew

  The routing version of the adjacent node is unacceptable to the local node. The operator may have installed incorrect software at the adjacent node.

*2.8 Circuit down**

An error has occurred for the circuit. This message displays the name of the circuit to which the event applies, with the following event qualifiers: the packet header (as described for event 2.0), the reason (as described for event 2.7), and the address of the adjacent node.

*2.9 Circuit down, operator initiated**

An operator error has occurred for the circuit. This message displays the name of the circuit to which the event applies, with the following event qualifiers: the packet header (as described for event 2.0), the reason (as described for event 2.7), and the addresses of the expected node and the adjacent node.

*2.10 Circuit up**

A remote node has initialized on one of the physical lines connected to the local node. This message displays the name of the line to which the event applies, with one event qualifier: the address of the newly initialized node.

Be sure to note that this event does not imply that the node is reachable. Reachability is determined by the higher-level routing algorithms.

*2.11 Initialization failure, line fault**

A remote node failed to initialize with the local node because of a physical line error. This message displays the name of the line to which the event applies, with one event qualifier: the reason for the event (as described for event 2.7).

*2.12 Initialization failure**

A remote node failed to initialize with the local node because of a software error. This message displays the name of the line to which the event applies, with two event qualifiers: the packet header (as described for event 2.0) and the reason (as described for event 2.7).

*2.13 Initialization failure, operator initiated**

A remote node failed to initialize with the local node because of an operator error. This message displays the name of the line to which the event applies, with three event qualifiers: the packet header (as described for event 2.0), the reason (as described for event 2.7), and the version received from the adjacent node.

*2.14 Node reachability change**

Because of routing operation, the reachability of a remote node has changed. This message displays the name of the node to which the event applies, with one qualifier: the routing status of the node (reachable or unreachable).

*2.15 Adjacency up**

The adjacent node on the circuit is initialized. This message displays the name of the circuit to which the event applies, and one event qualifier: the address of the adjacent node.

*2.16 Adjacency rejected**

The adjacent node on the circuit is not initialized. This message displays the name of the circuit to which the event applies, and two event qualifiers: the address of the adjacent node and the reason for the event (as described for event 2.7).

*2.17 Area reachability change**

Because of routing operation, the reachability of an area has changed. This message displays the name of the area to which the event applies, with one event qualifier: the routing status of the area (reachable or unreachable).

*2.18 Adjacency down**

An error has occurred for an adjacency on the circuit. This message displays the name of the circuit to which the event applies, with the following event qualifiers: the reason (as described for event 2.7), the packet header (as described for event 2.4), and the address of the adjacent node on the circuit.

*2.19 Adjacency down, operator initiated**

An adjacency on the circuit is down because of an operator error. This message displays the name of the circuit to which the event applies, with the following event qualifiers: the reason (as described for event 2.7), the packet header (as described for event 2.0), and the addresses of the expected node and the adjacent node on the circuit.

B

Tuning the DOS Client

This appendix explains how to adjust the DECnet PCSA Client for DOS parameters to match the conditions of your network. Default parameters are adequate for most users. If problems arise, you can adjust some parameters using the Network Control Program (NCP).

Responsiveness to Lost Packets

DECnet software maintains dynamic timers that adjust automatically to track the performance of your entire network connection.

The round-trip delay (RTD) is the primary timer. It estimates how long packets take to travel across the network and receive acknowledgment. Use the NCP SHOW ACTIVE NODES command to see the round trip delay in the Delay column. The default for a new connection is 5 seconds. The RTD timer adjusts according to the success of succeeding transmissions.

The EXECUTOR DELAY WEIGHT parameter determines the timer adjustment. Table B–1 shows the effect on performance.

Table B–1 Delay Weights

Delay Weight Value	Action
Low	Timer speeds up.
High	Timer slows down.

Packets are overdue if they do not comply with the following formula:

```
(RTD)* Delay_Factor/16
```

When the packet timeout occurs, the packet retransmits and the EXECUTOR RESPONSE TIMEOUT is incremented. Table B–2 shows the delay factors possible.

Table B–2 Delay Factors

Connection Type	Delay Factor Value
Ethernet	32
DDCMP	48

Lowering the delay factor causes faster timeouts and unnecessary retransmissions. Raising it decreases response to lost packets and degrades performance.

Note

You can use this technique to improve performance on other DECnet systems.

Connection Persistence

In addition to the information in Responsiveness to Lost Packets, there are two parameters to consider in dealing with transmission errors. The length of time that a link persists depends upon:

- EXECUTOR RETRANSMIT FACTOR parameter
- EXECUTOR CONFIDENCE TIMER parameter

The following sections describe these parameters.

Executor Retransmit Factor Parameter

The first variable in dealing with transmission errors is the EXECUTOR RETRANSMIT FACTOR. A link keeps trying to send a message every time a packet acknowledgment is overdue (RTD)* Delay_Factor/16. The retransmit counter decreases when packets retransmit. The EXECUTOR RETRANSMIT FACTOR parameter sets the counter initial value. Table B–3 shows the default values used.

Table B–3 Default Retransmit Factors

Connection Type	Default Value
Ethernet	12
DDCMP	6

The retransmit counter resets when it receives an acknowledgment. If the retransmit counter reaches zero before receiving an acknowledgment, the confidence factor counts down and the link disconnects.

Executor Confidence Timer Parameter

The second variable in dealing with transmission errors is the EXECUTOR CONFIDENCE FACTOR. When the retransmit counter reaches zero, the confidence timer starts. Retransmission continues for a while before the link disconnects. Continued retransmission allows you to specify a node-wide persistence that is not related to the measured round-trip time. Also, any application can request its own confidence timer value for each connection by using the LINKHOLD socket option. The default is 15 seconds.

C

Ethernet Configuration Guidelines

This appendix provides configuration guidelines for the following:

- Baseband Ethernet
- ThinWire Ethernet
- Fiber-optic cable
- DELNI Local Network Interconnect
- ThinWire multiport repeaters (DEMPRs)
- Ethernet repeaters (DEREPs)
- Bridges

Baseband Ethernet

Configuration guidelines for Baseband Ethernet are as follows:

- 500 meters maximum per length of coaxial cable segment.
- 500 meters maximum per length of coaxial cable segment when connected with a DELNI and a DEMPR.
- 300 meters maximum per length of coaxial cable segment if you cascade a DEMPR or DELNI connected on the Ethernet segment.
- 100 taps maximum per coaxial cable.
- 50 meters maximum per transceiver cable from the board to the coaxial cable.
- 1023 stations maximum per nonextended LAN.
- 1500 meters maximum of coaxial cable between any two stations in a nonextended LAN.
- 2.5 meters minimum separation between stations.
- Use DESTAs to adapt ThinWire to baseband Ethernet devices.

- Use DESPRs and DEMPRs to adapt baseband to ThinWire Ethernet devices.

ThinWire Ethernet

Configuration guidelines for ThinWire Ethernet are as follows:

- 185 meters per ThinWire segment.
- 30 connections maximum per ThinWire cable.
- 0.5 meters minimum separation between stations.
- No cabling is allowed between the T-connector and the DESTA.
- No cabling is allowed between the T-connector and the Ethernet controller.

Fiber-Optic Cable

Configuration guidelines for fiber-optic cable are as follows:

- 1000 meters maximum of fiber-optic cable total within a nonextended LAN
- 1500 meters maximum of fiber-optic cable between a remote bridge and a remote repeater
- 10,000 meters maximum of fiber-optic cable between two remote bridges
- 1000 meters maximum of fiber-optic cable between two stations within a nonextended LAN

DELNI Local Network Interconnect

Configuration guidelines for the DELNI local network interconnect are as follows:

- DELNIs *cannot* be cascaded if connected to an H4000 transceiver in GLOBAL mode.
- DELNIs *can* be cascaded if the top-level DELNI is in LOCAL mode.

DEMPR ThinWire Multiport Repeaters

Configuration guidelines for DEMPR ThinWire Multiport Repeaters are as follows:

- DEMPRs provide grounding and termination on one end for ThinWire segments.
- DEMPRs support a maximum of 29 stations on each segment.
- DEMPRs must be connected to an H4000-ba (no heartbeat) transceiver, or a standalone DELNI in GLOBAL mode with a loopback connector in the global port.

DEREP Ethernet Repeaters

Configuration guidelines for DEREP Ethernet Repeaters are as follows:

- DEREPs must be connected to an H4000-aa (with heartbeat) transceiver.
- Two repeaters (DEREP, DEMPR, DESPR) maximum are allowed between any two stations (this is the *two repeater rule*).
- A pair of remote repeaters connected to either end of a fiber-optic cable count as one repeater.
- A remote repeater and remote bridge combination counts as one repeater and one bridge.
- Parallel (or redundant) repeaters are allowed in LOCAL mode only, set using the standby switch on the repeater.

Bridges

Configuration guidelines for bridges are as follows:

- A maximum of seven bridges are allowed between any two stations.
- A maximum of 8000 stations are allowed on an extended LAN.
- Bridges effectively reset the two repeater rule. Therefore, if you use a bridge between sets of repeaters, you can have more than two repeaters between two stations.
- Parallel (or redundant) bridge configurations are permitted. The spanning tree algorithm automatically disables one bridge to prevent loops. Or, you can use RBMS to disable a bridge and prevent loops.
- A pair of remote bridges on either end of a fiber-optic cable count as two bridges.

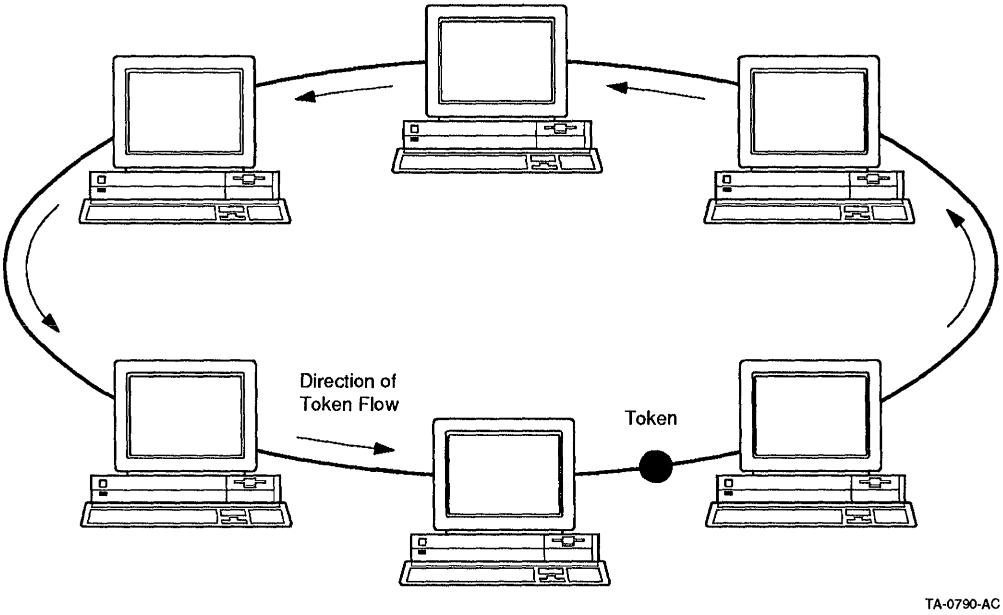
D

Token Ring Concepts and Terms

This appendix provides an overview of Token Ring concepts and terms. For detailed information about Token Ring networks, refer to the IBM documents listed in the Related Documents section at the beginning of this guide.

Token Ring networks use the concept of a single token to control communication between the network devices. An example of a Token Ring network is shown in Figure D–1.

Figure D–1 Example of Token Ring Network



A **token** is a unidirectional bit sequence going from one device to another on the network that provides permission for a device to transmit on the ring network. The token consists of a starting delimiter, an access control field, and an end delimiter.

The **ring network** consists of transmission links between the attaching devices to form a closed path. An **attaching device** is any device, such as a processor, printer, or controller, that is physically connected to the network and can communicate over the network. There can be a maximum of 260 attaching devices per ring.

When an attaching device wants to transmit data, it captures the token, alters the token to show the token has been captured, and appends its data to the token header to form a frame. A **frame** consists of the altered (captured) token header, a receiving address, the sender's address, and the data.

The frame is passed around the ring, with each attaching device examining the frame to see if the receiving address matches its own device address, or one of its enabled group addresses.

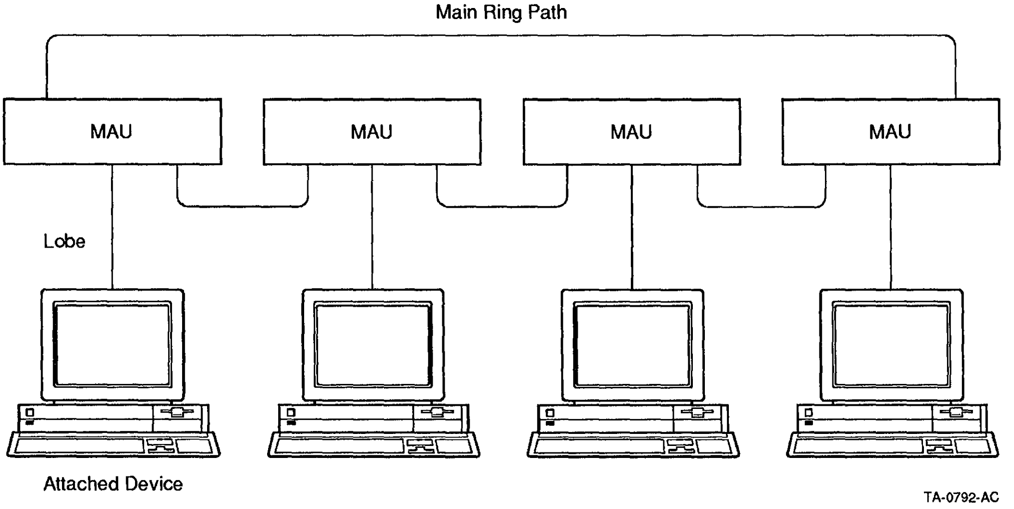
If there is no match, the examining device ignores the frame and sends it to the next device on the ring. If there is a match, the examining device copies the frame for itself, alters the frame to show it was received, and passes the frame onward through the ring.

When the frame is received back at the sending device, the device removes the frame and places a free token on the ring. The free token can then be captured by any device wanting to transmit on the ring.

Each device requires a device adapter to send and receive data on the ring. The cable or cable segments from the device adapter is called a **lobe** and connects to a **Multistation Access Unit (MAU)** that serves as a wiring concentrator for ring connections. This arrangement of multiple lobes connecting to one or more MAUs is called a star-wired ring. The maximum recommended lobe length is 330 feet (100 meters).

An example of attaching devices, lobes and MAUs within a Token Ring network is shown in Figure D–2.

Figure D–2 Example of Token Ring Attaching Device, Lobe, and MAU



The Token Ring is a baseband (unmodulated) system consisting of unshielded or shielded twisted-pair cabling, or fiber-optic cabling. Attaching devices can operate at a transmission rate of 4 or 16 million bits per second (Mbits/s). All devices connected to the ring must operate at the same transmission rate. Token Ring cabling data connectors are self-shorting, so that signals wrap around at disconnected data connectors and travel on a backup path to provide continued ring operation.

Multiple Token Ring networks can be interconnected by bridges. A sending device can place routing information within its data to direct the data across multiple rings using bridges. This is called **source routing**, because the source (the sending device) specifies the actual route the data is to take, rather than using centralized routing tables.

A Token Ring network and Ethernet network can be interconnected by a router, which enables devices on the two networks to exchange messages. The router is attached to each network as a network device, and examines message traffic on each network. When the router identifies a message on one network addressed to a device on the other network, it copies the source message and forwards the message to the receiving device.

Glossary

/etc/hosts

An ULTRIX file that contains network information.

Adaptive routing

Routing that adapts to changing conditions in the network.

Addnode command

An ULTRIX command you use to add a node to your configuration database.

Address mask

A 32-bit mask used to select the network portion of the internet address and one or more local address bits. Also referred to as network mask, netmask, or subnet mask.

Address Resolution Protocol (ARP)

An internet protocol that determines the physical network address of hosts on the same network.

Addressing

The way internet networks define the locations of nodes.

Area leakage

This problem occurs when you allow a Phase III node to have a link to another area.

Area routers

Nodes that perform routing within a specific area.

Area routing

Routing within an area.

Area

A logically configured group of nodes in a network that can run independently as a subnetwork.

ARP

See Address Resolution Protocol.

Asynchronous communications

Communications that are low-speed, low-cost connections over terminal lines switched on for network use either permanently or temporarily.

Attaching device

Any device, such as a processor, printer, or controller, that is physically connected to the Token Ring network and can communicate over the network.

Autobaud

The process by which the terminal software determines the line speed on a dial-up line.

Autonomous system

An internet collection of routers and networks controlled by one central administrative center to promote internet use.

babbling device

A device on the network with a hardware problem, causing it to send out large amounts of data to the local area network.

Backup circuit

A circuit defined in the database which will be used if the primary circuit is currently unavailable.

Baud

The speed at which data is transmitted over a data line; baud rates can be measurements of bits per second, bytes per second, or characters per second.

BIND

Berkeley Internet Name Domain name service.

Boot

To bring a device or system to a defined state where it can operate on its own.

Bridge

A device used to expand a local area network by forwarding frames between data link layers associated with two different kinds of physical links.

Cache

An internet host's temporary storing of its most recent ARP bindings.

Caching mechanism

The process of storing blocks in memory for future use; used to minimize physical transfer of data between mass storage devices and memory.

Carrier Sense Multiple-Access with Collision Detect (CSMA/CD)

A link management method used on Ethernet networks. It allows multiple stations to access a transmission medium (multiple access) by listening until no signals are detected (carrier sense), then transmitting and checking to see if more than one signal is present (collision detection).

Channel

A logical path between a Data Terminal Equipment (DTE) and Data Communications equipment (DCE) over which data is transmitted.

Circuit

The communication data path that carries information from one node to another.

Client

A personal computer or workstation connected to the network, that can access resources on a server. A client can have DOS, OS/2, or Macintosh software. *See also* server.

Cluster

A configuration of VAX processors.

Common carrier

An organization licensed to provide a specific set of services for a specific set of rates, as delineated in an agreed-upon document called a tariff.

Common internet address notation

An internet decimal form of the 32-bit internet address. Also known as dotted decimal notation.

Concentrator

A switching system arranged to connect a large number of inputs to a smaller number of outputs.

Configuration database

On DECnet networks, a database containing files that provide information about network components. Specifically, the files contain information about the local node, and all remote nodes, modules, circuits, lines, logging, and objects in the network.

Congestion-control algorithms

The transport components that manage buffers by limiting the maximum number of packets on a queue for a line. Also called transmit management.

Cost

A number that the network manager assigns to a circuit between two nodes. It is usually proportioned to transmission delay. Each circuit has a separate cost. In terms of the routing algorithm, packets are routed on paths with the least cost. Nodes on either end of a circuit can assign different costs to the same circuit. *See also* path cost.

CTERM

Digital Terminal Services Architecture Command. A network protocol that provides wide area network services to DOS computers for VT terminal emulation. CTERM is one of the possible protocols used in the SETHOST utility.

DAP

Data Access Protocol. A set of standardized formats and procedures that facilitate the creation, deletion, transfer, and access of files between a user process and a file system in a network environment.

Dedicated line

A nonswitched communications channel permanently connected between two or more data stations.

DEFINE

The NCP command used to establish the contents of the permanent database.

DELNI

Digital Ethernet Local Network Interconnect. A device that serves as a concentrator, grouping systems together.

Designated router

A routing node on the Ethernet selected to perform routing services on behalf of end nodes.

DDCMP

Digital Data Communications Message Protocol. A formal set of conventions designed to provide error-free, sequential transmission of data over physical links.

Dialup line

A telephone line connected to a computer for use by terminals.

Digital Network Architecture (DNA)

The name given to the Digital specifications which govern the interrelationship of the components that make up the DECnet software.

Direct routing

An internet process of directing IP datagrams between nodes on the same physical network.

Disk service

A service that offers file sharing by providing clients with high-performance virtual disks, called local area disks (LADs). *See also* local area disks.

Distributed processing

A method that allows systems to be placed where they are needed while still having access to the facilities of other widely dispersed systems.

Domain

The primary category of hosts in the internet domain name system.

Domain name system

The internet system for organizing host names into a tree-structured system.

Dotted decimal notation

An internet decimal form of the 32-bit internet address. Also known as common internet address notation.

Down-line loaded

A process whereby server software, including diagnostics, is transferred to terminal servers from a load host.

Dynamic connection

A temporary connection.

Emulator

An emulator is a combination of hardware and software programs that allows a computer or printer to simulate the characteristics of a terminal or different printer by acting like (emulating) that device. Terminal emulators allow a PC to behave like a specific model terminal, that is, VT320 and printer emulations allow a printer to operate using different control command sets.

End nodes

Nodes that do not forward data.

Equal cost path splitting

When multiple paths to a destination node have the same path cost, the routing layer, by default, splits packet loads for routing on several paths, rather than only one.

Ethernet

A CSMA/CD system using coaxial cable, developed by Xerox Corporation's Palo Alto Research Center, used for local communications networks.

External Gateway Protocol (EGP)

An internet routing protocol enabling individual networks to communicate with the internet backbone.

Fiber-optic cable

A cable made of glass fibers and designed to transmit digital signals in the form of pulses of light. Fiber-optic cable is noted for its properties of electric isolation and resistance to electric contamination.

File service

A service that provides a client a remote file system that appears as a transparent extension of the client system's local computer environment.

File Transfer

A utility used to convert core image formats.

Filtering

The ability of a LAN bridge to evaluate incoming messages and select messages that need to be processed by the bridge.

Flow control

The hardware or software mechanisms employed in data communications to turn off transmission when the receiving station is unable to store data it is receiving.

Forward

The ability of a LAN bridge or router to accept messages from one LAN segment and retransmit (forward) those messages to another LAN segment.

Frame

A Token Ring frame consists of a captured token header, a receiving address, the sender's address, and the data.

Gateway

A connection between two or more networks allowing data to be transferred from a host on one network to a host on a separate network.

Gateway to Gateway Protocol (GGP)

An internet routing protocol used between internet backbone routers for routing and availability information.

Graphic Programming Interface (GPI)

A program that computes data and constructs diagrams for the display of that data on graphic display terminals.

Group code number

A number or set of numbers used by the LAT protocol to identify network resources and to control access to those resources. Group codes can be used to assign LAT resources to a specific set of users and to balance the load between computers offering identical services.

Hop count

The number of hops between two points in an internet. The number of hops equals the number of routers between the source and destination.

Hop

Relative to the transport layer, a hop is the logical distance between two adjacent nodes in a network.

Host

A computer system servicing the needs of its client computer systems.

Host number

The second part of the two-part internet address. The host number identifies the host on the internet.

ICMP

See Internet Control Message Protocol.

Icon

A graphic or picture representative of a function displayed on a terminal screen.

Indirect routing

An internet process of directing IP datagrams between two hosts located on different physical networks.

Interior Gateway Protocol (IGP)

An internet routing protocol for routing information within an autonomous internet system.

Internet

A collection of connected networks using the Internet Protocol (IP).

Internet address

A 32-bit number identifying a host connection on the internet. An internet address contains a network number and host number.

Internet Control Message Protocol (ICMP)

The internet protocol that reports network errors on internetworks. ICMP also informs hosts of route changes on IP routers for alternate routes.

Internet Protocol (IP)

An internet protocol that determines how data is sent from one host to another. IP also specifies the format of packets called Internet Protocol (IP) datagrams.

Internet protocol (IP) datagram

An internet basic unit of information. Each IP datagram contains source and destination addresses and data.

Internet protocol (IP) gateway

See Internet Protocol (IP) router.

Internet protocol (IP) router

An internet host that connects two or more networks. Also called an internet protocol (IP) gateway.

Internetwork

See Internet.

IP

See Internet Protocol (IP).

Job Spawner

A utility that allows your computer to act as a server for multiple service functions. It activates DECnet servers on your node.

LAN Manager

A OS/2 application that transparently extends the file system, device driver I/O system, and selected IPC mechanisms across the network.

LAT

See Local Area Transport.

LAT node

A computer that has LAT software and can offer services, access services, or both. A LAT node can be either a terminal server, a LAT client, or a service node.

LAT service

Any service offered on the LAT; for example, a terminal server and LAT system service are the most common types of LAT services.

LATCP

See LAT Control Program.

lcp

The command that is used on ULTRIX systems to start the LAT Control Program.

LCP command

A command issued within the LAT Control Program to change the characteristics of the LAT protocol functions on an ULTRIX system.

Leaf

An internet host in the domain name system.

Least-cost path

The best or most available path from the source to the destination.

Level 1 router

A node that performs routing between a single area.

Level 2 router

A node that performs routing between areas as well as within their own area.

Lines

Part of the communication system that connects data communications equipment (DCE) together.

Load command

An ULTRIX command you can use to downline load the terminal server software.

Load host

An ULTRIX node which performs the downline loading and upline-dumping of software.

Loaddump_secure

An ULTRIX environmental variable for the load host, which is set to on or off for downline loading.

Lobe

The cable or cable segments from a Token Ring device adapter connecting to a Multistation Access Unit (MAU).

Local area disk (LAD)

Digital's virtual disk software on a DECnet network. LAD provides high performance disk services to DOS and OS/2 clients connecting to a VMS server.

Local area network (LAN)

A network of computers located in close proximity to each other, such as a building, a set of buildings, or a campus.

Local Area Transport (LAT)

A communications protocol that operates on a local area network (LAN) to permit communications between computer systems and other devices such as terminals, printers, and modems.

LAT Control Program (LATCP)

Management software, providing a command interface, that allows the LAT protocol to be used by an operating system to configure and manage the LAT capabilities available on that system.

Local node

The node where you are physically located.

Local printer

A printer directly connected to the server or client.

Local resources

Resources stored on or connected to a client.

Logical links

Connects two processors and carries a stream of communications traffic between the processes over one or more circuits.

Loop node

A node which tests messages between two different nodes.

Loopback tests

The process of systematically testing a link by sending a signal part way down the link and returning it. This method is used to verify the operation of devices along a communications link.

Management agent

Part of the Simple Network Management Protocol (SNMP) residing on network elements. The management agent is used by monitoring stations to perform network management functions.

Maximum cost

The greatest total cost the path to a node may have if the node is to be reachable.

Maximum hops

An operator-controllable transport parameter that defines the point where the routing decision algorithm in a node declares another node unreachable because the length of the shortest path between the two nodes is too long. For correct operation, this parameter must not be less than the network diameter.

Maximum visits

The maximum number of nodes through which a packet can be routed before arriving at the destination node. If the packet exceeds the maximum number of visits, the packet is dropped.

Modem

A device that uses digital data to alter a signal that can be transmitted over an analog transmission facility (modulator) and can also receive an altered signal from an analog transmission facility and determine what digital data the alterations in the receive signal represent (demodulator).

Multicast

A type of network addressing that enables a node to exchange messages with any node on the network that has been configured to recognize a multicast address. Multicast messages are communicated internally and are not visible to users.

Multistation Access Unit (MAU)

A unit serving as a wiring concentrator for Token Ring connections. The arrangement of multiple connections to one or more MAUs is called a star-wired ring.

Naming

An internet method for identifying hosts.

Name server

Software that identifies network entities by performing translations from a name to an address or an address to a name. The software can run on a shared or dedicated processor.

Netacp

A process that contains the procedures that handle the automatic network reconfiguration of a network node.

Netdriver

Where most of the procedures that control network routing are located.

Netmask

See address mask.

Netstat

An ULTRIX network utility command that gives the local hosts' status with respect to the network by symbolically displaying the contents of network-related data structures.

Network Control Program (NCP)

The utility program used to configure and control DECnet networks.

Network Device Utility (NDU)

A utility that allows access to local area disks in a WAN.

Network elements

Internetwork devices such as hosts, gateways and terminal servers. Each device contains SNMP management agents to perform management functions requested by network management stations.

Network File Transfer (NFT)

In DOS, this utility transfers files between your local node and remote nodes.

Network Management Listener (NML)

A utility that executes NCP commands and sends the results back to the source node.

Network management stations

Part of the Simple Network Management Protocol (SNMP) that controls and monitors the network elements.

Network mask

See address mask.

Network number

The portion of the internet address containing the network address and class of a host.

Network Services Protocol (NSP)

A formal set of conventions used in DECnet to perform network management and to exchange messages over logical links.

Network topology

The configuration of wires, cables, and nodes in a network.

Node

A individual computer or device that can communicate with other computers or devices in a network.

Node address

A number uniquely identifying a server node.

Node-id

The unique identifier of a system on the network.

Nonrouting node

A node that can send or receive its information but cannot send information received from another node.

Object

A DECnet-VAX process that receives a logical link request. It performs a specific network function (a nonzero object such as FAL or NML), or is a user-defined image for a special-purpose application (a zero-numbered object).

Octet

An eight-bit byte.

Out-of-order packetcashing

The Network Services Protocol (NSP) maintains a cache of out-of-order packets that are reassembled in order.

Packet

A group of bits, including data and control elements, that are switched and transmitted together. The control elements include a source address and a destination address. The data and control elements, and possibly error-control information, are arranged in a specific format. Packets can also be called segments.

Packet-switching

A data transmission method, utilizing packets, whereby a channel is occupied for only the duration of transmission of the packet. By limiting the length of the packets, the system limits the amount of time that other users will have to wait. Depending upon the length of the message and the system being used, the data may be formatted into a packet or divided and then formatted into a number of packets for transmission and multiplexing purposes.

Parity

The number of 1s in a character or other group of bits. The number may be odd or even. If desired, a 0 or 1 may be added to the group of bits to guarantee that the number of bits is odd (or even). The data is then transmitted and the number of 1s is checked at the receiving station to see that it is still odd (or even). If it is not as expected, one knows that an error has occurred. Unfortunately, the occurrence of multiple errors cannot be accurately detected.

Path

The route the data travels over the circuit in the network.

Path cost

The sum of the circuit cost along a path between two nodes. The path cost never exceeds a maximum cost value the network manager specifies for the network. *See also* Cost.

Path length

The number of hops along the path between two nodes. It is the number of circuits a packet must travel across to reach its destination.

PDU

See Protocol Data Unit.

Physical device

An I/O or peripheral storage device for a computer configuration.

PID

See Process identification.

Point-to-point

A transmission facility that connects only two points. This is in contrast to a multipoint or multidrop facility, which services to many points that share access to the same transmission facility.

Preferred service

A service you configure into the LAT service table on your node, using the LAT Control Program (LATCP).

Presentation Manager

An integral part of the OS/2 software that helps users manage their system by allowing them to select and control applications.

Primary circuit

The preferred path over which data is to travel.

Print queue

The list of documents waiting to be printed.

Printer services

The availability of a printer that is connected to a server. From the client, users run network commands to access a printer service and then print files. A file server makes a printer service available to clients.

Process identification (PID)

A value that uniquely identifies each process. Each process has a PID and a process name.

Protocol

A set of rules for exchanging messages over a communications link.

Protocol Data Unit (PDU)

Usually referred to as a packet or segment, a PDU contains both data and control information.

Protocol Stack

The complete set of protocol layers for a given transport.

Pseudo-device

An I/O device, accessible by the user or system, that is not associated with an actual device.

Reachable node

A reachable node is a destination node to which the routing layer on the local node has a usable path; that is, the path does not exceed the values for the maximum cost or hops between nodes specified in the executor database. For an area network, a reachable node is one to which the path does not exceed the values for maximum cost or hops between areas set in the executor database.

Redirect

The assignment of a logical device name, which is a local representation of a physical device located on the network.

Remote node

Any other node in the network from the local node.

Remote printer

A printer not physically connected to a client; but connected to a server on the network.

Remote resources

Resources available as services from a server.

Requests for Comments (RFC)

A collection of Internet notes containing information about proposed and accepted protocol standards.

Resolver

The software on a client that asks a name server for naming information.

Resource sharing

The common use of one central processor by several users as well as by several peripheral devices.

Response information message

An information message or multicast message from a service node or a terminal server to a client that had queried the availability of a system service.

Reverse path caching

A mechanism whereby the end node uses the acknowledgment messages it receives to build a cache of addresses of target nodes that are either on the same Ethernet or can be reached through a node on the Ethernet.

RFC

See Requests for comments.

Ring network

The transmission links between the attaching devices on a Token Ring network that form a closed path.

Rlogin

An ULTRIX utility that allows you to connect to another system on the network.

Root

The top level internet domain name. The root level has seven categories of domains: COM, EDU, GOV, MIL, NET, ORG, and ARPA.

Root server

The top level name server for the internet domain naming system.

Router

An intervening node that receives data and forwards it to another node.

Routing

The process of directing a data message from a source node to a destination node.

Routing Information Protocol (RIP)

A protocol specifying how routers pass routing information in an autonomous system.

Routing node

A computer on the network that directs a data message from a source node or host to a destination node or host.

Routing table

A host-based table used to select the best routes to other internet networks. Each network table entry has a network number and internet address.

Search

A function of the LAT protocol, implemented in DOS nodes, that allows LAT clients to make inquiries to LAT servers about the availability of a particular service or type of service, for example, printer, modem, system.

Segment

See Packet.

Server

A computer running software that offers file, printer, or disk services to clients. *See also* client.

Service announcement

A multicast message sent from a LAT server to all clients. A service announcement contains information about a LAT service offered by the server. This information is stored in the client's service table.

Service Table

An area in memory that stores information about known services.

Session Control Block (SCB)

A system data structure that must be provided to LAT by an application whenever the application wants to create a session. The SCB contains all the interrupt and exception vectors known to the system.

SET

An NCP command used to establish the contents of the volatile database.

SETHOST

A terminal emulation program that lets you use your personal computer or workstation as if it were directly connected to the host node, giving you access to the host's resources.

Shutdown command

An ULTRIX command that shuts down the network.

Simple Network Management Protocol (SNMP)

SNMP specifies a protocol for monitoring and controlling hosts, routers, and terminal servers on TCP/IP networks with network management applications.

SNA

See Systems Network Architecture.

SNMP

See Simple Network Management Protocol.

Solicit information message

A multicast message from a service node or a terminal server asking whether a specific service is available from another service node or terminal server. *See also* response information message.

Source routing

A Token Ring routing method where the source (the sending device) specifies the actual route the data is to take, rather than using centralized routing tables.

Spool directory

A file that contains specific printer commands for a printer.

Static connection

A permanent connection.

Subdomain

The groups that are part of an internet domain. Also called *branches* or *zones.*

Subnet

Each physical network that shares a network address with other physical networks on an internet. Because a single network address identifies all of the physical networks in a subnet collection, networks outside of the collection see only one network, which in fact are multiple physical networks.

Subnet address

A modified 32-bit internet address that contains a network part and a local part. The network part is the network address and the local part is the physical network and host number.

Subnet mask

A bit mask used to select bits from an internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the internet address and one or more bits of the local portion. Also called a network mask, netmask, or address mask.

Synchronous communications

A communications method of data transmission that allows each event to operate in relation to a timing signal. The timing signal synchronizes the transmitter and the receiver, eliminating the need for stop bits and providing efficiency in data transfer.

Systems Network Architecture (SNA)

An IBM layered communications protocol.

TCP/IP

Transmission Control Protocol/Internet Protocol. Communications software based upon the internet protocol model.

Test port

An ULTRIX command used to verify the configuration of the port.

Terminal server

Connects terminals and other bit-oriented, asynchronous devices to service nodes in an Ethernet LAN.

Timeout

The expiration of the time limit in which a device is to complete an I/O transfer.

Token

A unidirectional bit sequence going from one device to another on the Token Ring network that provides permission for a device to transmit on the ring network. The token consists of a starting delimiter, an access control field, and an end delimiter.

Topology

The arrangement of the nodes and circuits.

Trigger command

An ULTRIX command which directly triggers the bootstrap mechanism of the target node, causing the target to send a program load request to the Ethernet dump/load assistance multicast address.

Upline-dump

A process whereby the server attempts to transfer its memory image to the load host so it can automatically initiate a reload of its software.

VMS Access Control List (ACL)

A file protection service that restricts access to files within services.

Virtual disk

The space the disk server program sets aside on a VMS disk. The virtual disk, actually a VMS container file, functions like a DOS-formatted disk. Users can connect to a virtual disk through a DOS drive and can store, create, and maintain DOS files. *See also* local area disk.

Wide area network (WAN)

A network that provides for communication over a broad geographic area.

Yellow Pages

An internet name server.

Zone

See Subdomain.

Index

Reader's Comments

PATHWORKS
Network Troubleshooting Guide

AA–PAGVC–TK

Your comments and suggestions help us improve the quality of our publications.

Please rate the manual in the following categories:	Excellent	Good	Fair	Poor
Accuracy (product works as described)	□	□	□	□
Completeness (enough information)	□	□	□	□
Clarity (easy to understand)	□	□	□	□
Organization (structure of subject matter)	□	□	□	□
Figures (useful)	□	□	□	□
Examples (useful)	□	□	□	□
Table of contents (ability to find topic)	□	□	□	□
Index (ability to find topic)	□	□	□	□
Page design (overall appearance)	□	□	□	□
Print quality	□	□	□	□

What I like best about this manual:

What I like least about this manual:

Additional comments or suggestions:

I found the following errors in this manual:

Page Description

For which tasks did you use this manual?

□ Installation
□ Maintenance
□ Marketing
□ Operation/Use
□ Programming
□ System Management
□ Training
□ Other (please specify)

Name/Title

Company

Address

Phone

Date

Do Not Tear - Fold Here and Tape

digital

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

DIGITAL EQUIPMENT CORPORATION
CORPORATE USER PUBLICATIONS
PKO3–1/D30
129 PARKER STREET
MAYNARD, MA 01754–9975

Do Not Tear - Fold Here and Tape

digital

Order Number:AA-PAGVC-TK
Printed in the U.S.A.